9.1

IBM MQ ' nun Güvenliğinin sağlanması

Not

Bu bilgileri ve desteklediği ürünü kullanmadan önce, “Özel notlar” sayfa 631 bölümündeki bilgileri okuyun.

Bu basım, yeni basımlarında tersi belirtilmediği sürece, IBM® MQ sürüm 9 yayın düzeyi 1 'i ve sonraki tüm yayın düzeyleri ve değişiklikler için geçerlidir.

İçindekiler

güvenlikIBM MQ

Security is an important consideration for both developers of IBM MQ applications, and for IBM MQ system administrators.

Güvenlik güncellemeleri

Güvenli bölge içindeki ve işletmen iş istasyonlarındaki tüm donanım ve yazılımların destek yaşam çevriminin içinde olduğundan emin olun, zorunlu yazılım güncellemeleriyle büyütülmüş ve en kısa süre içinde güvenlik güncellemeleri edinmiş olmalıdır.

Aşağıdakiler için güvenlik güncelleştirmeleriyle ilgili daha fazla bilgi bulabilirsiniz:

- IBM Security Bulletins' deki tüm platformlar
- Securityüzerindeki güvenlik ve sistem bütünlüğü APAR 'ları IBM Z System Integrity Portal' da yer alan z/OS .

Güvenliğe genel bakış

Bu konu derlemi, IBM MQ güvenlik kavramlarını tanıtır.

Güvenlik kavramları ve mekanizmaları, herhangi bir bilgisayar sistemine uygulandıkça, önce bu güvenlik mekanizmalarının bir tartışması ve ardından IBM MQiçinde uygulandıkça bu güvenlik mekanizmalarının bir tartışmasıyla birlikte sunulur.

Güvenlik kavramları ve mekanizmaları

This collection of topics describes aspects of security to consider in your IBM MQ installation.

Güvenlik konusunda yaygın olarak kabul edilen noktalar aşağıda verilmiştir:

- “Tanımlama ve kimlik doğrulama” sayfa 6
- “Yetkilendirme” sayfa 6
- “Denetleme” sayfa 6
- “Gizlilik” sayfa 7
- “Veri bütünlüğü” sayfa 7

Güvenlik mekanizmaları , güvenlik hizmetlerini uygulamak için kullanılan teknik araçlar ve tekniklerdir. Bir mekanizma, belirli bir hizmeti sağlamak için kendi başına ya da diğerleriyle çalışabilir. Ortak güvenlik mekanizmalarına örnek olarak şunlar verilebilir:

- “Kriptografi” sayfa 7
- “İleti sindirimi ve dijital imzalar” sayfa 9
- “dijital sertifikalar” sayfa 9
- “Genel anahtar altyapısı (PKI)” sayfa 13

Bir IBM MQ uygulamasını planlarken, sizin için önemli olan güvenlik açılarını uygulamak için gereksinim duyduğunuz güvenlik mekanizmalarını göz önünde bulundurun. Bu konuları okuduktan sonra göz önünde bulundurulması gerekenlerle ilgili bilgi için bkz. “Güvenlik gereksinimlerinizin planlanması” sayfa 76.

İlgili kavramlar

“SSL/TLS ile çalışma” sayfa 261
These topics give instructions for performing single tasks related to using TLS with IBM MQ.

İlgili görevler

İki kuyruk yöneticisinin TLS ' yi kullanarak bağlanması

Tanımlama ve kimlik doğrulama

Tanımlama , sistemde çalışmakta olan bir sistemi ya da uygulamayı benzersiz olarak tanımlama yeteneğidir. *Kimlik Doğrulaması* , bir kullanıcının ya da uygulamanın o kişinin ya da uygulamanın ne kadar talep ettiği konusunda gerçekten kim olduğunu kanıtlayabilme yeteneğidir.

Örneğin, bir kullanıcı kimliğini ve parolayı girerek sistemde oturum açan bir kullanıcıyı düşünün. Sistem, kullanıcıyı tanıtmak için kullanıcı kimliğini kullanır. Sistem, oturum açma sırasında kullanıcının kimliğini doğrulayarak, sağlanan parolanın doğru olup olmadığını denetleyerek doğrular.

Itibar edilmeyen

itibar edilmeyen hizmet, kimlik doğrulama ve kimlik doğrulama hizmetine bir uzantı olarak görüntülenebilir. Genel olarak, veri elektronik olarak iletildiğinde itibar edilmeyen bir durum geçerlidir; örneğin, hisse senedi satın almak ya da satmak için bir borsaya sipariş vermek ya da bir bankaya bir hesap için bir sipariş başka bir hesaptan başka bir hesaba aktarıldığında geçerli olur.

Saygınlık dışı hizmetin genel amacı, belirli bir iletinin belirli bir kişi ile ilişkilendirilmiş olduğunu kanıtlayabilmelidir.

Saygınlık dışı hizmet, her bileşenin farklı bir işlev sağladığı birden fazla bileşen içerebilir. Bir iletinin göndericisi göndermeyi reddederse, *kökeninin kanıtı* ile itibarlı olmayan hizmet, alıcıya, iletinin belirli bir kişi tarafından gönderildiğine ilişkin reddedilemez kanıtlarla sağlayabilir. Bir iletinin alıcısı bunu almayı reddederse, *teslim edilme belgesi* ile saygınlık dışı olmayan hizmet, göndereni, iletinin belirli bir kişi tarafından alındığı inkar edilemez kanıtlarla sağlayabilir.

Pratikte, neredeyse %100 kesinlik ya da inkar edilemez kanıtlarla kanıtlanması zor bir hedeftir. Gerçek dünyada, hiçbir şey tamamen güvenli değildir. Güvenliğin yönetilmesi, iş için kabul edilebilir bir düzey için riski yönetmekten daha fazla endişe eder. böyle bir ortamda, itibar edilemeyecek bir hizmetin daha gerçekçi bir beklentisi, kabul edilebilir olan delilleri sağlayabilmek ve sizin davanızı, bir hukuk mahkemesinde destekliyor.

Non-repudiation is a relevant security service in an IBM MQ environment because IBM MQ is a means of transmitting data electronically. Örneğin, belirli bir kişinin belirli bir kişiye ilişkin bir uygulama tarafından gönderildiğini ya da alındığını bildiren bir kanıt bulunmasını zorunlu kılabilir.

Advanced Message Security ileIBM MQ , temel işlevinin bir parçası olarak itibarlı olmayan bir hizmet sağlamaz. Ancak, bu ürün belgelerinde kendi çıkış programlarınızı yazarak bir IBM MQ ortamında kendi itibarını nasıl sağlayabileceğinize ilişkin öneriler yer alır.

İlgili kavramlar

“IBM MQ' ta kimlik doğrulama ve kimlik doğrulama” sayfa 20
IBM MQ' ta, ileti bağlamı bilgilerini ve karşılıklı kimlik doğrulamayı kullanarak kimlik doğrulama ve kimlik doğrulaması uygulayabilirsiniz.

Yetkilendirme

Yetki yalnızca yetkili kullanıcılara ve uygulamalarına erişimi sınırlandırarak kritik öneme sahip kaynakları bir sistemde korur. Bir kaynağın yetkisiz kullanımını ya da kaynak kullanımını yetkisiz bir şekilde önler.

İlgili kavramlar

“IBM MQiçinde yetki” sayfa 21
Belirli kişileri ya da uygulamaları IBM MQ ortamınızda yapabilme yetkisini sınırlandırmak için yetki kullanabilirsiniz.

Denetleme

Denetleme , beklenmeyen ya da yetkisiz bir etkinliğin gerçekleşip gerçekleştirilmediğini ya da bu tür bir etkinliği gerçekleştirme girişiminde bulunulup bulunulmadığını saptamak için olayları kaydetme ve denetleme işletidir.

Yetkilendirmeyi nasıl ayarladığınız hakkında daha fazla bilgi için bkz. “Planlama yetkilendirmesi” sayfa 79 ve ilişkili alt konular.

İlgili kavramlar

“IBM MQiçinde denetim” sayfa 21

IBM MQ , olağan dışı etkinliğin gerçekleşmiş olduğunu kaydetmek için olay iletileri yayınlayabilir.

Gizlilik

Gizlilik hizmeti, hassas bilgileri yetkisiz açıklamalardan korur.

Hassas veriler yerel olarak depolandığında, erişim denetimi mekanizmaları, erişilemiyorsa, verilerin okunamadığı varsayımı üzerinde korumak için yeterli olabilir. Daha yüksek bir güvenlik düzeyi gerekliyse, veriler şifrelenebilir.

Özellikle İnternet gibi güvenli olmayan bir ağ üzerinden iletişim ağı üzerinden aktarıldığında hassas verileri şifreleyin. bir ağ ortamında erişim kontrol mekanizmaları, telefon dinleme gibi verileri önleme girişimlerine karşı etkili değildir.

Veri bütünlüğü

Veri bütünlüğü hizmeti, verilerin yetkisiz olarak değiştirilip değiştirilmediğini belirler.

Verilerin değiştirilebileceği iki yöntem vardır: yanlışlıkla, donanım ve iletim hatalarıyla ya da planlı bir saldırı nedeniyle. Birçok donanım ürünü ve iletim protokolü, donanım ve iletim hatalarını algılamak ve düzeltmek için mekanizmalara sahiptir. Veri bütünlüğü hizmetinin amacı kasıtlı bir saldırıyı algılamak.

Veri bütünlüğü hizmeti, yalnızca verilerin değiştirilip değiştirilmediğini saptamayı hedefliyor. Değiştirildiyse, verileri özgün durumuna geri yüklemeyi hedeflemez.

Erişim reddedilirse, veri değiştirilemeyecek şekilde, erişim denetimi mekanizmaları veri bütünlüğüyle katkıda bulunabilir. Ancak, gizlilik içinde olduğu gibi, erişim denetimi mekanizmaları bir ağ ortamında etkili değildir.

Şifreleme kavramları

Bu konu derlemi, IBM MQiçin geçerli olan şifreleme kavramlarını açıklar.

varlık terimi, bir kuyruk yöneticisine, IBM MQ MQI client' a, tek bir kullanıcıya ya da ileti alışverişi yeteneğine sahip başka bir sisteme gönderme yapmak için kullanılır.

İlgili kavramlar

“IBM MQiçinde şifreleme” sayfa 22

IBM MQ , Transport Security Layer (TLS) iletişim kuralını kullanarak şifreleme sağlar.

Kriptografi

Şifreleme, *düz metin*adlı okunabilir metin ile *şifreli metin*adı verilen okunamayan bir form arasında dönüştürme işletidir.

Bu, aşağıdaki gibi oluşur:

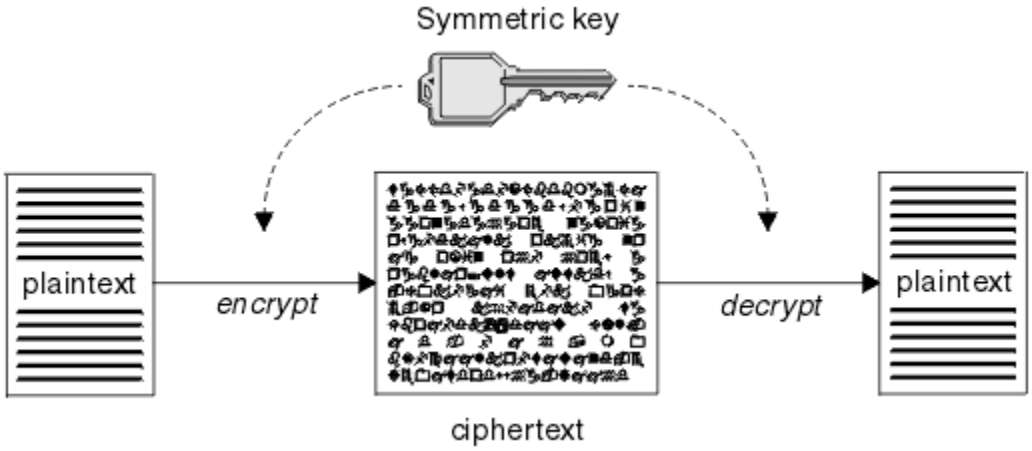
1. Gönderen, düz metin iletisini şifreli metne dönüştürür. İşlemin bu bölümünde *şifreleme* (bazen *şifreleme*) adı verilir.
2. Ciphertext, alıcıya iletilir.
3. Alıcı, ciphertext iletisini düz metin formuna geri çevirir. İşlemin bu kısmına *şifre çözme* denir (bazen *şifre çözer*).

Dönüştürme işlemi, ileti sırasında iletinin görünüşünü değiştiren, ancak içeriği etkilmeyen bir dizi matematiksel işlem içerir. Şifreleme teknikleri, şifreli bir ileti anlaşılabilir olmadığı için, gizliliğin gizliliği ve yetkisiz görüntülere karşı koruma sağlayabilmelerini sağlar. Dijital imzalar, mesaj bütünlüğü konusunda güvence sağlar, şifreleme tekniklerini kullanır. Ek bilgi için “SSL/TLS ' de dijital imzalar” sayfa 18 başlıklı konuya bakın.

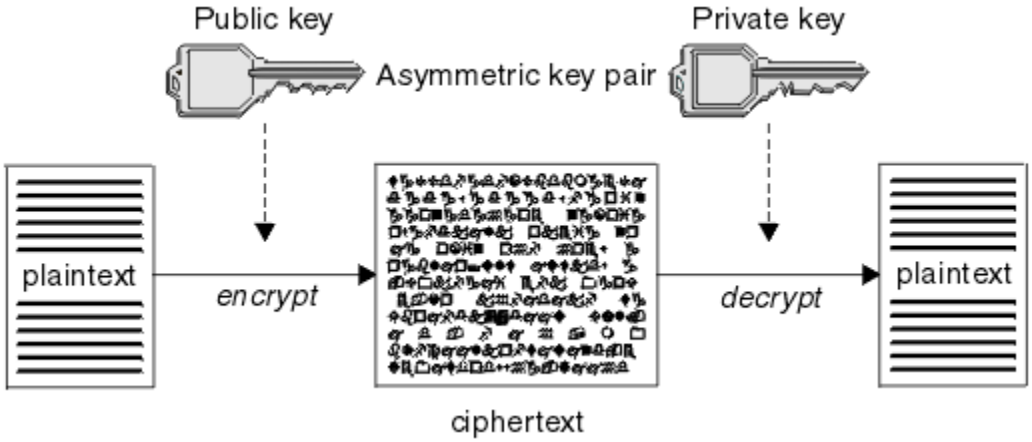
Şifreleme teknikleri, tuşların kullanımıyla özel olarak yapılan genel bir algoritmayı içerir. İki algoritma sınıfı vardır:

- Her iki tarafın da aynı gizli anahtarı kullanmasını gerektirenler. Paylaşılan anahtar kullanan algoritmalar *simetrik* algoritmalar olarak bilinir. Şekil 1 sayfa 8 , simetrik anahtar şifrelemesi gösterir.
- Şifreleme için bir anahtar ve şifre çözme için farklı bir anahtar kullananlar. Bunlardan bir tanesi sır olarak saklanmalıdır, ama diğeri halka açık olabilir. Genel ve özel anahtar çiftlerini kullanan algoritmalar *asimetrik* algoritmalar olarak bilinir. Şekil 2 sayfa 8 , *genel anahtar şifrelemesi*olarak da bilinen asimetrik anahtar şifrelemesi gösterir.

Kullanılan şifreleme ve şifre çözme algoritmaları genel olabilir, ancak paylaşılan gizli anahtar ve özel anahtar gizli tutulmalıdır.



Şekil 1. Simetrik anahtar şifrelemesi



Şekil 2. Asimetrik anahtar şifrelemesi

Şekil 2 sayfa 8 , alıcısının genel anahtarı ile şifrelenmiş düz metni gösterir ve alıcının özel anahtimiyle şifresinin şifresini çözer. Yalnızca amaçlanan günlük nesnesi, şifreli metnin şifresini çözmek için özel anahtarı tutar. Gönderenin, iletileri özel bir anahtarla şifreleyebileceğini, bu da gönderenin genel anahtarını, iletinin göndericiden gelmesi gereken güvenciyle, iletinin şifresini çözmesini sağlayan herkese izin verdiğini unutmayın.

Asimetrik algoritmalarla, iletiler genel ya da özel anahtarla şifrelenir, ancak yalnızca diğer tuşla şifreleri çözülabilir. sadece özel anahtar gizli, halk anahtarı herkes tarafından bilinebiliyor. Simetrik algoritmalarla, paylaşılan anahtarın yalnızca iki kişi tarafından bilinmesi gerekir. Buna, *anahtar dağıtım sorunu*adı verilir. Asimetrik algoritmalar daha yavaşıdır, ancak önemli bir dağıtım sorunu olmamasının avantajına sahiptir.

Şifrelemeyle ilişkili diğer terminoloji aşağıdaki gibi olabilir:

Güvenlik düzeyi
Şifrelemenin gücü, anahtar boyutuna göre belirlenir. Asimetrik algoritmalar büyük anahtarlar gerektirir; örneğin:

1024 bit	Düşük güçlü asimetrik anahtar
2048 bit	Orta kuvvetli asimetrik anahtar
4096 bit	Yüksek güçlü asimetrik anahtar

Simetrik anahtarlar küçüktür: 256 bit anahtarlar güçlü şifreleme sağlar.

Blok şifre algoritması
Bu algoritmalar verileri bloklara göre şifreliyor. Örneğin, RSA Data Security Inc. ' den RC2 algoritması, 8 bayt uzunluğunda bloklar kullanır. Blok algoritmaları, genellikle akış algoritmalarından daha yavaş olur.

Akış şifresi algoritması
Bu algoritmalar her bir veri baytı üzerinde çalışır. Akış algoritmaları genellikle blok algoritmalarından daha hızlılardır.

İleti sindirimi ve dijital imzalar

İleti özeti, bir iletinin içeriğinin sabit boyutlu sayısal gösterimidir. İleti özeti, bir HASH işlevi tarafından hesaplanır ve bir dijital imza oluşturularak şifrelenebilir.

Bir ileti özetinin hesaplanması için kullanılan HASH işlevi iki ölçütü karşılamalıdır:

- Bir yolu olmalı. Tüm olası iletileri test etmek dışında, belirli bir ileti özetine karşılık gelen iletiyi bulmak için işlevin tersine çevrilmesi mümkün değildir.
- Aynı özette hash olan iki ileti bulmak için, bu, hesaplamasal olarak erişilmez olmalıdır.

İleti özeti iletiyle birlikte gönderilir. Alıcı, ileti için bir özet oluşturabilir ve bunu gönderenin özeti ile karşılaştırabilir. İletinin bütünlüğü, iki ileti sindirme işlemi aynı olduğunda doğrulanır. İletişimde yapılan herhangi bir kurcalama, neredeyse kesinlikle farklı bir mesaj özetiyle sonuçlanana kadar.

Gizli simetrik anahtar kullanılarak yaratılan bir ileti özeti, iletinin değiştirilmediği konusunda güvence sağlayabileceği için, bir ileti doğrulama kodu (Message Authentication Code; MAC) olarak bilinir.

Gönderici ayrıca bir ileti özeti oluşturabilir ve daha sonra bir asimetrik anahtar çiftinin özel anahtarını kullanarak özeti şifreleyebilir, dijital imza oluşturur. Daha sonra, bu imzanın şifresini, yerel olarak üretilen bir özet ile karşılaştırmadan önce, alıcı tarafından şifresi çözülmelidir.

İlgili kavramlar

“SSL/TLS ' de dijital imzalar” sayfa 18
Dijital imza, bir iletinin gösterimini şifreleyerek oluşturulur. Şifreleme, imzaya ilişkin özel anahtarı kullanır ve verimlilik için genellikle iletinin kendisinden ziyade bir ileti özeti üzerinde çalışır.

dijital sertifikalar

Dijital sertifikalar, bir genel anahtarın belirtilen bir varlığa ait olduğunu onaylayan kişileştirmeye karşı koruma sağlar. Bunlar bir Sertifika Yetkilisi tarafından verilir.

Dijital sertifikalar, sayısal sertifika sahibinin bir kişi mi, kuyruk yöneticisi mi, yoksa başka bir varlık mı olduğu, bir genel anahtarı sahibine bağlaması nedeniyle, kimliğine bürünmeye karşı koruma sağlar. Dijital sertifikalar genel anahtar sertifikaları olarak da bilinir, çünkü asimetrik anahtar şeması kullandığınızda bir ortak anahtarın sahipliği hakkında size güvence verirler. Sayısal sertifika, bir varlığın genel anahtarını içerir ve genel anahtarın o varlığa ait olduğu bir deyimdir:

- Sertifika tek bir varlık için olduğunda, sertifikana *kişisel sertifika* ya da *kullanıcı sertifikası*adı verilir.
- Sertifika bir Sertifika Yetkilisi için olduğunda, sertifikanın adı *CA sertifikası* ya da *imzalayıcı sertifikası*olarak adlandırılır.

Genel anahtarlar doğrudan sahipleri tarafından başka bir varlığa gönderilirse, iletinin engellenmiş olması ve genel anahtarın başka bir varlığa geri koyması riski vardır. Bu, *orta saldırıdaki adam*olarak bilinir. Bu sorunun çözümü, ortak anahtarları güvenilir bir üçüncü kişi aracılığıyla değiş tokuş etmek, size genel anahtarın gerçekten iletişim kurduğunuz varlığa ait olduğu konusunda güçlü bir güvence vermesidir. Genel anahtarınızı doğrudan göndermek yerine, güvenilir üçüncü kişinin bunu dijital bir sertifika dahil etmesi için

sormanız gerekir. Dijital sertifikaları ele alan güvenilen üçüncü kişi, “Sertifika Yetkilileri” sayfa 11içinde açıklandığı şekilde, Sertifika Yetkilisi (CA) olarak adlandırılır.

Dijital sertifikada ne var?
Sayısal sertifikalar, X.509 standardı tarafından belirlendiği şekilde, belirli bilgi parçalarını içerir.

IBM MQ tarafından kullanılan sayısal sertifikalar, gereken bilgileri ve dosyayı göndermekte kullanılacak biçimi belirten X.509 standartı ile uyumlu olur. X.509 is the Authentication framework part of the X.500 series of standards.

Dijital sertifikalar, sertifikalandırılmakta olan varlıkla ilgili en az aşağıdaki bilgileri içerir:

- Sahibin genel anahtarı
- Sahibin Ayırt Edici Adı
- Sertifikayı veren CA ' nın Ayırt Edici Adı
- Sertifikenin geçerli olduğu tarih
- Sertifikana ilişkin süre bitimi tarihi
- The version number of the certificate data format as defined in X.509. X.509 standardının geçerli sürümü Sürüm 3 ve çoğu sertifikalar bu sürüme uygun olur.
- Bir seri numarası. Bu, sertifikayı veren CA tarafından atanan benzersiz bir tanıtıcıdır. Seri numarası, sertifikayı veren CA içinde benzersizdir: aynı CA sertifikasının imzaladığı iki sertifika aynı seri numarasına sahip değildir.

X.509 Sürüm 2 sertifikası, Sertifika Veren Tanıtıcısı ve Konu Tanıtıcısı da içerir ve X.509 Sürüm 3 sertifikası bir dizi uzantıyı içerebilir. Basic Constraint uzantısı gibi bazı sertifika uzantıları *standart*, ancak diğer kullanıcılar somutla-özeldir. Bir uzantı *kritik*olabilir; bu durumda, bir sistemin alanı tanıyabilmesi gerekir; alanı tanımazsa, sertifikayı reddetmesi gerekir. Bir uzantı kritik değilse, sistem bu uzantıyı tanımazsa bu uzantıyı yoksayabilir.

Kişisel sertifikadaki dijital imza, sertifikayı imzalayan CA ' nın özel anahtarı kullanılarak oluşturulur. Kişisel sertifikanı doğrulamaya gerek duyan herkes, CA ' nın genel anahtarını kullanabilir. CA ' nın sertifikası genel anahtarını içerir.

Dijital sertifikalar özel anahtarınızı içermez. Özel anahtar sırrını saklamış olmalısın.

Kişisel sertifikalara ilişkin gereksinimler
IBM MQ , X.509 standardına uygun dijital sertifikaları destekler. İstemci kimlik denetimi seçeneğini gerektirir.

IBM MQ bir eşdüzey sistem olduğu için, SSL/TLS terminolojisinde istemci kimlik doğrulaması olarak görüntülenir. Bu nedenle, SSL/TLS kimlik doğrulaması için kullanılan kişisel sertifikaların, istemci kimlik doğrulamasının önemli bir kullanımına izin vermesi gerekir. Sunucu sertifikalarının tümü bu seçeneği etkinleştirmez; dolayısıyla, sertifika sağlayıcının güvenli sertifika için kök sertifika kuruluşu (CA) üzerinde istemci kimlik denetimini etkinleştirmesi gerekebilir.

Sayısal sertifika için veri biçimini belirten standartların yanı sıra, sertifikana ilişkin geçerli olup olmadığını belirlemek için de standartlar vardır. Bu standartlar, belirli güvenlik ihlallerinin belirli bir şekilde ihlal edilmemesi için zaman içinde güncellenmiştir. Örneğin, daha eski X.509 sürüm 1 ve 2 sertifikalar, sertifikenin diğer sertifikaları imzalamak için yasal olarak kullanılıp kullanılamayacağını belirtmedi. Bu nedenle, kötü amaçlı bir kullanıcının geçerli bir kaynaktan kişisel bir sertifika alması ve diğer kullanıcıların kimliğine bürünmek üzere tasarlanmış yeni sertifikalar yaratması mümkün oldu.

X.509 sürüm 3 sertifikalarını kullanırken, hangi sertifikaların diğer sertifikaları imzalayabileceğini belirtmek için BasicConstraints ve KeyUsage sertifika uzantıları kullanılır. IETF RFC 5280 standardı, taklitleme saldırılarını önlemek için uyumlu uygulama yazılımların gerçekleştirmesi gereken bir dizi sertifika geçerlilik denetimi kuralı dizisini belirtir. Sertifika kuralları kümesi, sertifika geçerlilik denetimi ilkesi olarak bilinir.

IBM MQ' ta sertifika doğrulama ilkelerine ilişkin daha fazla bilgi için bkz. “IBM MQiçindeki sertifika geçerlilik denetimi ilkeleri” sayfa 41.

Sertifika Yetkilileri
Bir Sertifika Yetkilisi (CA), bir varlığın genel anahtarının gerçekten o varlığa ait olduğu bir güvenceye sahip olmak için dijital sertifikalar veren, güvenilir bir üçüncü taraftır.

Bir CA ' nın rolleri şunlardır:

- Dijital sertifika isteği alınırken, kişisel sertifikayı oluşturmadan, imzalamadan ve döndürmeden önce istekte bulunanın kimliğini doğrulamak için
- CA sertifikasında CA ' nın kendi genel anahtarını sağlamak için
- Bir Sertifika İptal Listesi 'nde (CRL) artık güvenilmeyen sertifikaların listesini yayınlamak için. Daha fazla bilgi için bkz. “İptal edilen sertifikalarla çalışma” sayfa 323
- OCSP yanıtlayıcı sunucusu çalıştırılarak sertifika iptal durumuna erişim sağlamak için

Belirleyici Adlar
The Distinguished Name (DN) uniquely identifies an entity in an X.509 certificate.

Uyarı: Bir SSLPEER süzgecinde yalnızca aşağıdaki tablodaki öznitelikler kullanılabilir. Sertifika DN ' leri diğer öznitelikleri içerebilir, ancak bu özniteliklerde süzgeç uygulamaya izin verilmez.

Çizelge 1. Bir SSLPEER süzgecinde kullanılabilecek ayırt edici ad (DN) içinde bulunan öznitelik tipleri

Öznitelik tipi	**Tanım**
SERIALNUMARı	Sertifika seri numarası
POSTA	E-posta adresi
E	E-posta adresi (POSTA tercihinde kullanımdan kaldırıldı)
UID ya da USERID	Kullanıcı kimliği
CN	Ortak Ad
T	Başlık
OU	Kuruluş Birimi adı
DC	Etki alanı bileşeni
O	Kuruluş adı
Sokak	Adres satırı/adres satırı
L	İlçe adı
ST (ya da SP ya da S)	Eyalet ya da Bölge adı
PC	Posta kodu/posta kodu
C	Ülke
TANıMLAMA ADı	Anasistem adı
YAPıLANDıRMA ADRESI	IP adresi
DNQ	Ayırt edici ad niteleyicisi

X.509 standardı, genellikle DN ' nin bir parçası olmayan, ancak isteğe bağlı uzantılar sağlayabilen diğer öznitelikleri sayısal sertifikadan tanımlar.

X.509 standardı, bir DN ' nin dizgi biçiminde belirtilmesini sağlar. Örneğin:

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

Ortak Ad (CN) tek bir kullanıcıyı ya da başka bir varlığı (örneğin, bir web sunucusu gibi) tanımlayabilir.

Ayırt edici ad, birden çok OU ve DC özniteliği içerebilir. Diğer özniteliklerin her birinin tek bir örneğine izin verilir. OU girişlerinin sırası önemlidir: Order, Organizational Unit (Kuruluş Birimi) adlarının sıradüzenini belirtir, en üst düzey birim ilk sırada olur. DC girişlerinin sırası da önemlidir.

IBM MQ Yanlış biçimlendirilmiş DN ' leri kabul eder. Daha fazla bilgi için bkz. SSLPEER değerleri içinIBM MQ kuralları.

İlgili kavramlar

“Dijital sertifikada ne var?” sayfa 10
Sayısal sertifikalar, X.509 standardı tarafından belirlendiği şekilde, belirli bilgi parçalarını içerir.

Bir sertifika yetkilisinden kişisel sertifikaların alınması
Güvenilir bir dış sertifika yetkilisinden (CA) bir sertifika edinebilirsiniz.

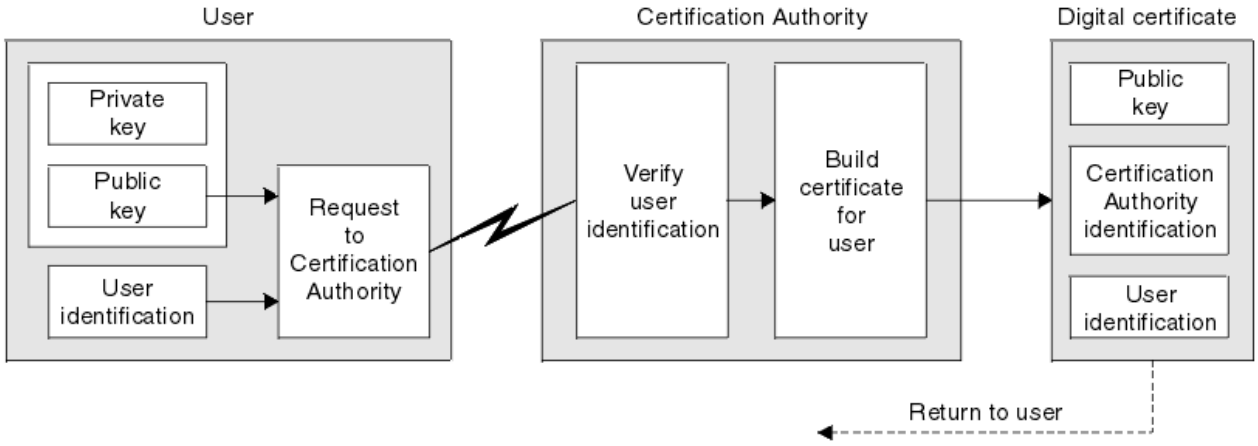
Sertifika isteği biçiminde bir CA ' ya bilgi göndererek sayısal bir sertifika elde edebilirsiniz. X.509 standardı, bu bilgiler için bir biçim tanımlar, ancak bazı CA ' lar kendi biçimlerine sahiptir. Sertifika istekleri genellikle sisteminizin kullandığı sertifika yönetimi aracı tarafından oluşturulur; örneğin:

- Multi Multiplatformsüzerindeki iKeyman aracı.
- z/OS z/OSüzerindeRACF .

Bilgiler, ayırt edici adınızı ve genel anahtarınızı içerir. Sertifika yönetimi aracınız sertifika isteğinizi oluşturduğunda, güvenli tutmanız gereken özel anahtarınızı da oluşturur. Özel anahtarınızı asla dağıtmayın.

CA isteğinizi aldığında, sertifikayı oluşturmadan önce kimliğinizi doğrular ve bunu size kişisel sertifika olarak geri döndürür.

Şekil 3 sayfa 12 , bir CA ' dan sayısal sertifika alma işlemini gösterir.



Şekil 3. Dijital sertifika alma

Şemada:

- Kullanıcı kimliği, Konunun Ayırt Edici Adını içerir.
- Sertifikasyon Yetkisi tanıtıcısı, sertifikayı veren CA ' nın Ayırt Edici Adını içerir.

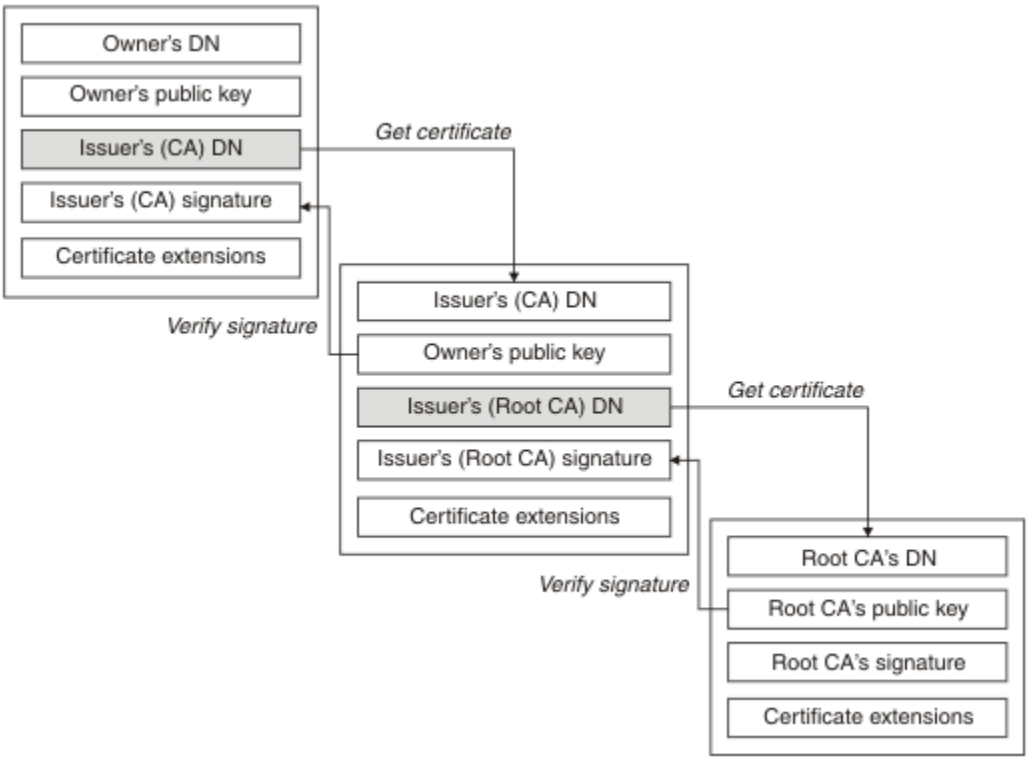
Sayısal sertifikalar, çizgede gösterilenler dışında ek alanlar içerir. Dijital sertifikadaki diğer alanlarla ilgili daha fazla bilgi için bkz. “Dijital sertifikada ne var?” sayfa 10.

Sertifika zincirleri nasıl çalışır
Başka bir varlık için sertifikayı aldığınızda, *kök CA* sertifikasını edinmek için bir *sertifika zinciri* kullanmanız gerekebilir.

The certificate chain, also known as the *sertifikasyon yolu*, is a list of certificates used to authenticate an entity. Zincir ya da yol, o varlığın sertifikasıyla başlar ve zincirdeki her bir sertifika, zincirdeki bir sonraki sertifikayla tanımlanan varlık tarafından imzalanır. Zincir, kök sertifika kuruluşu (CA) sertifikasıyla

sona eriyor. Kök sertifika kuruluşu (CA) sertifikası her zaman sertifika yetkilisi (CA) tarafından imzalanır. Zincirdeki tüm sertifikaların imzaları, kök CA sertifikasına ulaşılıncaya kadar doğrulanmalıdır.

Şekil 4 sayfa 13 , sertifika sahibinden kök CA ' ya bir sertifikasyon yolu gösterir; burada güven zinciri başlar.



Şekil 4. Güven zinciri

Her sertifika bir ya da daha fazla uzantı içerebilir. Bir CA ' ya ait bir sertifika tipik olarak, diğer sertifikaları imzalamaya izin verildiğini belirtmek için isCA işareti ayarlanmış bir BasicConstraints uzantısını içerir.

Sertifikalar artık geçerli olmadığında
Dijital sertifikaların süresi dolabilir ya da iptal edilebilir.

Dijital sertifikalar sabit bir dönem için verilir ve süre bitimi tarihinden sonra geçerli değildir.

Sertifikalar çeşitli nedenlerle iptal edilebilir; bu nedenler şunlar da dahil olmak üzere:

- Sahip, farklı bir kuruluşa taşındı.
- Özel anahtar artık gizli değil.

IBM MQ , bir OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü) yanıtlayıcıya bir istek göndererek sertifikanın iptal edilip edilmediğini denetleyebilir (yalnızca UNIX, Linux®, and Windows üzerinde). Diğer bir seçenek olarak, LDAP sunucusundaki bir Sertifika İptal Listesi 'ne (CRL) erişebilirler. OCSP iptal ve CRL bilgileri bir Sertifika Yetkilisi tarafından yayınlanır. Daha fazla bilgi için “İptal edilen sertifikalarla çalışma” sayfa 323 başlıklı konuya bakın.

Genel anahtar altyapısı (PKI)

Genel Anahtar Altyapısı (Public Key Infrastructure; PKI), bir hareket içinde yer alan tarafların kimlik doğrulaması için ortak anahtar şifrelemesi kullanımını destekleyen bir tesis, ilke ve hizmettir sistemidir.

Bir Genel Anahtar Altyapısının bileşenlerini tanımlayan tek bir standart yoktur, ancak bir PKI genellikle sertifika yetkililerini (CA 'lar) ve Kayıt Yetkililerini (RA' lar) içerir. CAs aşağıdaki hizmetleri sağlar:

- Dijital sertifikaların verilmesi
- Dijital sertifikaların geçerliliği denetleniyor

- Dijital sertifikaları iptal etme
- Ortak anahtarları dağıtma

X.509 standartları, sektör standardı Genel Anahtar Altyapısı için temel sağlar.

Dijital sertifikalar ve sertifika yetkililerine (CA ' lar) ilişkin ek bilgi edinmek için “dijital sertifikalar” sayfa 9 dosyasına bakın. RAs, dijital sertifikalar istendiğinde sağlanan bilgileri doğrular. RA, bu bilgileri doğrularsa, CA, istekte bulunana bir sayısal sertifika verebilir.

Ayrıca, bir PKI, dijital sertifikaları ve genel anahtarları yönetmek için kullanılabilecek araçlar da sağlayabilir. Bir PKI, bazen dijital sertifikaları yönetmek için bir *güven sıradüzeni* olarak tanımlanır, ancak çoğu tanımlama ek hizmetler içerir. Bazı tanımlar şifreleme ve dijital imza hizmetlerini içerir, ancak bu hizmetler PKI ' nın çalışması için gerekli değildir.

Şifreleme güvenlik iletişim kuralları: TLS

Şifreleme iletişim kuralları güvenli bağlantılar sağlar ve iki tarafın gizlilik ve veri bütünlüğü ile iletişim kurmasını sağlar. TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolü, SSL (Secure Sockets Layer; Güvenli Yuva Arabirimi Katmanı) olanağından evrimleşti. IBM MQ TLS ' yi destekler.

Her iki protokolün de birincil hedefleri, gizlilik sağlamak, (bazen *gizlilik* olarak anılır), veri bütünlüğü, tanımlama ve dijital sertifikalar kullanılarak kimlik doğrulaması sağlamaktır.

İki iletişim kuralı benzer olmasına rağmen, farklılıklar SSL 3.0 ve çeşitli TLS sürümlerinin birbiriyle etkileşmediği konusunda yeterince önemli.

İlgili kavramlar

“IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22
IBM MQ , ileti kanalları ve MQI kanalları için bağlantı düzeyinde güvenlik sağlamak üzere TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolünü destekler.

Transport Layer Security (TLS) kavramları

TLS iletişim kuralı, iki tarafın birbirlerinin kimliklerini belirlemesine ve kimliklerini doğrulamasına ve gizlilik ve veri bütünlüğüyle iletişim kurmasına olanak sağlar. TLS iletişim kuralı Netscape SSL 3.0 protokolünden evrimleşti, ancak TLS ve SSL ' ler birbiriyle çalışmaz.

TLS iletişim kuralı, Internet üzerinden iletişim güvenliği sağlar ve istemci/sunucu uygulamalarının gizli ve güvenilir bir şekilde iletişim kurmasını sağlar. Protokollerin iki katmanı vardır: Bir Kayıt İletişim Kuralı ve El Sallama Protokolü ve bunlar, TCP/IP gibi bir iletim protokolünün üst katmanlarıdır. İkisi de asimetrik ve simetrik kriptografi teknikleri kullanıyor.

TLS bağlantısı, TLS istemcisi haline gelen bir uygulama tarafından başlatılır. Bağlantıyı alan uygulama TLS sunucusu olur. Her yeni oturum, TLS iletişim kuralları tarafından tanımlandığı gibi bir tokalaşmayla başlar.

A full list of CipherSpecs supported by IBM MQ is provided at “CipherSpecs' in etkinleştirilmesi” sayfa 402.

SSL protokolleriyle ilgili daha fazla bilgi için https://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt' te sağlanan bilgilere bakın. TLS iletişim kuralı hakkında daha fazla bilgi için, https://www.ietf.orgadresindeki Internet Engineering Task Force web sitesinde TLS Çalışma Grubu tarafından sağlanan bilgilere bakın.

SSL/TLS el sıkışmasına genel bakış

SSL/TLS anlaşması, TLS istemcisinin ve sunucusunun iletişim kurdukları gizli anahtarları oluşturmasına olanak sağlar.

Bu kısım, TLS istemcisinin ve sunucusunun birbiriyle iletişim kurmasını sağlayan adımlara ilişkin bir özet sağlar.

- Kullanılacak protokolün sürümü üzerinde kabul edin.
- Şifreleme algoritmalarını seçin.
- Dijital sertifikaları değiş tokuş ederek ve doğrulayarak birbirlerinin kimliğini doğrulayın.

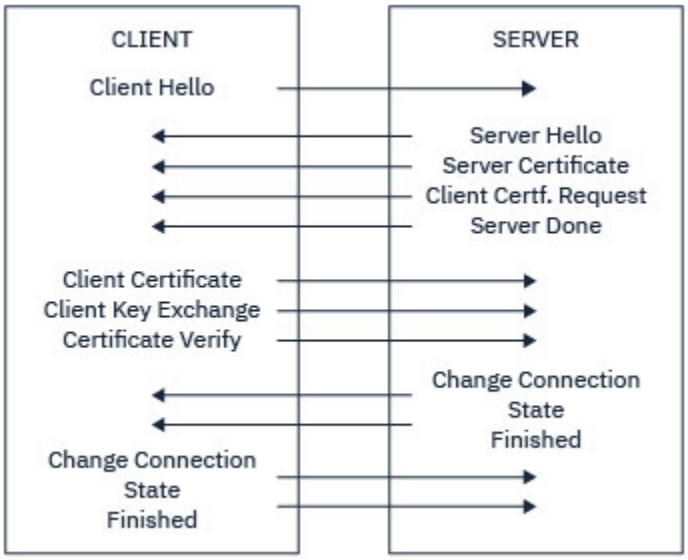
- Anahtar dağıtım sorununu önleyen, paylaşılan bir gizli anahtar oluşturmak için asimetrik şifreleme tekniklerini kullanın. Daha sonra TLS, asimetrik şifrelemeden daha hızlı olan iletilerin simetrik şifrelemesi için paylaşılan anahtarı kullanır.

Şifreleme algoritmaları ve dijital sertifikalar hakkında daha fazla bilgi için, ilgili bilgilere bakın.

Genel bakış, TLS el sıkışmasında yer alan adımlar şunlardır:

1. TLS istemcisi, TLS sürümü gibi şifreleme bilgilerini ve istemcinin tercih sırasını, istemci tarafından desteklenen CipherSuites gibi şifrelemeyle ilgili bilgileri listeleyen bir "istemci merhaba" iletisi gönderir. İleti, sonraki hesaplamalarda kullanılan rasgele byte dizesini de içerir. Bu iletişim kuralı, "istemci merhaba" ' in istemci tarafından desteklenen veri sıkıştırma yöntemlerini içermesine olanak sağlar.
2. TLS sunucusu, istemci tarafından sağlanan listeden, oturum tanıtıcısı ve başka bir rasgele byte dizgisiyle seçilen CipherSuite öğesini içeren bir "sunucu merhaba" iletisiyle yanıt verir. Sunucu, dijital sertifikasını da gönderir. Sunucu, istemci kimlik doğrulaması için bir dijital sertifika gerektiriyorsa, sunucu, desteklenen sertifika tiplerinin listesini ve kabul edilebilir Sertifika Yetkililerinin (CA ' lar) Ayırt Edici Adlarını Içeren bir "istemci sertifikası isteği" gönderir.
3. TLS istemcisi, sunucunun dijital sertifikasını doğrular. Daha fazla bilgi için, bkz. “TLS kimlik doğrulama, kimlik doğrulama, gizlilik ve bütünlük sağlar” sayfa 16.
4. TLS istemcisi, hem istemciyi hem de sunucuyu, sonraki ileti verilerini şifrelemek için kullanılacak gizli anahtarı hesaplayacak şekilde rasgele byte dizesini gönderir. Rasgele byte dizgisinin kendisi, sunucunun genel anahtimiyle şifrelenir.
5. If the TLS server sent a "istemci sertifikası isteği", the client sends a random byte string encrypted with the client's private key, together with the client's digital certificate, or a "dijital sertifika uyarısı yok". Bu uyarı yalnızca bir uyarıdır, ancak bazı somutlamalarda, istemci kimlik doğrulaması zorunlu olduğunda tokalaşma başarısız olur.
6. TLS sunucusu, istemcinin sertifikasını doğrular. Daha fazla bilgi için, bkz. “TLS kimlik doğrulama, kimlik doğrulama, gizlilik ve bütünlük sağlar” sayfa 16.
7. TLS istemcisi sunucuya, el sıkışmasının istemci kısmının tamamlandığını belirten gizli anahtarla şifrelenmiş bir "bitmiş" iletisi gönderir.
8. TLS sunucusu istemciyi, el sıkışmasının sunucu parçasının tamamlandığını belirten gizli anahtarla şifrelenmiş bir "bitmiş" ileti gönderir.
9. TLS oturumunun süresi boyunca, sunucu ve istemci artık ortak gizli anahtarla simetrik olarak şifrelenmiş iletileri değiş tokuş edebilir.

Şekil 5 sayfa 16 , TLS el sıkışmasını gösterir.



Şekil 5. TLS el sıkışmasına genel bakış

TLS kimlik doğrulama, kimlik doğrulama, gizlilik ve bütünlük sağlar

Hem istemci hem de sunucu kimlik doğrulaması sırasında, verilerin asimetrik anahtar çiftindeki anahtarlardan biriyle şifrelenmesini ve çiftin diğer anahtarla şifrelerini çözmesini gerektiren bir adım vardır. Bütünlük sağlamak için bir ileti özeti kullanılır.

TLS el sıkışmasında yer alan adımlara genel bir bakış için bkz. “SSL/TLS el sıkışmasına genel bakış” sayfa 14.

TLS kimlik doğrulamayı nasıl sağlıyor

Sunucu kimlik doğrulaması için, istemci, gizli anahtarı hesaplamak için kullanılan verileri şifrelemek için sunucunun genel anahtarını kullanır. Sunucu, yalnızca doğru özel anahtarla verilerin şifresini çözebilirse gizli anahtarı oluşturabilir.

İstemci kimlik doğrulaması için, sunucu, müşterinin el sıkışmasının “5” sayfa 15 . adımı sırasında gönderdiği verilerin şifresini çözmek için istemci sertifikasında genel anahtarı kullanır. Gizli anahtarla şifrelenmiş olan biten iletilerin (genel bakımda “7” sayfa 15 ve “8” sayfa 15 adımları) kimlik doğrulamasının tamamlandığını onayladığı doğrulanır.

Kimlik doğrulama adımlarından herhangi biri başarısız olursa, tokalaşma başarısız olur ve oturum sonlandırılır.

TLS anlaşması sırasında dijital sertifikaların değişimi, kimlik doğrulama işleminin bir parçasıdır. Sertifikaların, kimliğine bürünmeye karşı koruma sağlama konusunda daha fazla bilgi için, ilgili bilgilere bakın. Gereken sertifikalar aşağıdaki gibidir; burada CA X , TLS istemcisine sertifikayı yayınlar ve CA Y , sertifikayı TLS sunucusuna gönderir:

Yalnızca sunucu kimlik doğrulaması için, TLS sunucusunun gerekli olması gerekir:

- CA Ytarafından sunucuya verilen kişisel sertifika.
- Sunucunun özel anahtarı

ve TLS istemcisi gereksinimleri:

- CA Yiçin CA sertifikası

TLS sunucusu istemci kimlik doğrulaması gerektiriyorsa, sunucu, istemcinin kişisel sertifikasını istemciye veren CA için, bu durumda CA X' te istemcinin dijital sertifikasını doğrulayarak istemcinin kimliğini doğrular. Hem sunucu, hem de istemci kimlik doğrulaması için, sunucu gereklidir:

- CA Ytarafından sunucuya verilen kişisel sertifika.

- Sunucunun özel anahtarı
- CA Xiçin CA sertifikası

ve müşteri gereksinimleri şunlardır:

- CA Xtarafından istemciye verilen kişisel sertifika.
- İstemcinin özel anahtarı
- CA Yiçin CA sertifikası

Hem TLS sunucusu hem de istemci, kök CA sertifikasına bir sertifika zinciri oluşturmak için diğer CA sertifikalarına gereksinim duyabilir. Sertifika zincirleri hakkında daha fazla bilgi için, ilgili bilgilere bakın.

Sertifika doğrulaması sırasında neler oluyor

Genel bakımın “3” sayfa 15 ve “6” sayfa 15 adımlarında belirtildiği gibi, TLS istemcisi sunucunun sertifikasını doğrular ve TLS sunucusu, istemcinin sertifikasını doğrular. Bu doğrulamanın dört yönü vardır:

1. Dijital imza kontrol edilir (bkz. “SSL/TLS ' de dijital imzalar” sayfa 18).
2. Sertifika zinciri imlenmiş; ara CA sertifikalarına sahip olmasınız (bkz. “Sertifika zincirleri nasıl çalışır” sayfa 12).
3. Süre bitimi ve etkinleştirme tarihleri ve geçerlilik süresi denetlenir.
4. Sertifikana ilişkin iptal durumu kontrol edilir (bkz. “İptal edilen sertifikalarla çalışma” sayfa 323).

Gizli anahtar ilk durumuna getirildi

TLS anlaşması sırasında, TLS istemcisi ve sunucusu arasındaki verileri şifrelemek için bir *gizli anahtar* oluşturulur. Gizli anahtar, düz metni okunamayan şifreli metne dönüştürmek için verilere uygulanan bir matematiksel formülde ve düz metne ciphertext formülünde kullanılır.

Gizli anahtar, el sıkışmasının bir parçası olarak gönderilen rasgele metinden oluşturulur ve düz metni şifreli metin olarak şifrelemek için kullanılır. Gizli anahtar, bir iletinin değiştirilip değiştirilmediğini belirlemek için kullanılan MAC (Message Authentication Code; İleti Doğrulama Kodu) algoritmasında da kullanılır. Ek bilgi için “İleti sindirimi ve dijital imzalar” sayfa 9 başlıklı konuya bakın.

Gizli anahtar keşfedildiyse, bir iletinin düz metni şifreli metinden deşifre edilebilir ya da ileti özeti hesaplanabiliyorsa, iletilerin saptanmadan değiştirilebilmesini sağlar. Karmaşık bir algoritma için bile, düz metin, şifreli metne mümkün olan her matematiksel dönüşüm uygulanarak keşfedilebilir. Gizli anahtar bozulursa, deşifre edilebilen ya da değiştirilebilen veri miktarını en aza indirmek için, gizli anahtar periyodik olarak yeniden görüşülebilmektedir. Gizli anahtar yeniden görüşülediğinde, önceki gizli anahtar artık yeni gizli anahtarla şifrelenen verilerin şifresini çözmek için kullanılamaz.

TLS ' nin gizlilik sağladığı

TLS, ileti gizliliğini sağlamak için simetrik ve asimetrik şifreleme bileşimini kullanır. TLS anlaşması sırasında TLS istemcisi ve sunucusu, bir şifreleme algoritmasını ve yalnızca bir oturum için kullanılacak paylaşılan gizli anahtarı kabul eder. TLS istemcisi ile sunucusu arasında iletilen tüm iletiler, bu algoritma ve anahtar kullanılarak şifrelenir ve ileti durdurulsa bile iletinin özel olarak kalmasını sağlar. TLS paylaşılan gizli anahtarı taşırken asimetrik şifreleme kullandığından, anahtar dağıtımı sorunu yoktur. Şifreleme teknikleriyle ilgili daha fazla bilgi için “Kriptografi” sayfa 7' e bakın.

TLS bütünlüğü nasıl sağlar

TLS, bir ileti özetini hesaplayarak veri bütünlüğü sağlar. Daha fazla bilgi için bkz. “İletilerin veri bütünlüğü” sayfa 439.

Use of TLS does ensure data integrity, provided that the CipherSpec in your channel definition uses a hash algorithm as described in the table in “CipherSpecs' in etkinleştirilmesi” sayfa 402.

Özellikle, veri bütünlüğü bir endişesiyse, hash algoritması "None" (Yok) olarak listelenen bir CipherSpec seçilmesini önlemeniz gerekir. MD5 kullanımı, artık çok eski olduğundan ve en pratik amaçlar için artık güvenli olmadığı için güçlü bir şekilde kullanılması önerilidir.

CipherSpecs ve CipherSuites

Şifreleme güvenlik protokolleri, güvenli bir bağlantı tarafından kullanılan algoritmalar üzerinde kabul etmelidir. CipherSpecs ve CipherSuites , algoritmaların belirli bileşimlerini tanımlar.

CipherSpec , şifreleme algoritması ve MAC (Message Authentication Code; İleti Kimlik Doğrulama Kodu) algoritmasının bir birleşimini tanımlar. TLS bağlantısının her iki ucu da, iletişim kurabilmek için aynı CipherSpec üzerinde anlaşmaya varmalıdır.

IBM MQ , TLS 1.2 iletişim kuralını destekler. Ancak, bu işlemi yapmanız gerekiyorsa, kullanımdan kaldırılmış CipherSpecs' ı etkinleştirebilirsiniz.

Aşağıdakiyle ilgili bilgi için bkz. “CipherSpecs' in etkinleştirilmesi” sayfa 402 :

- IBM MQtarafından desteklenenCipherSpecs
- Kullanımdan kaldırılan SSL 3.0 ve TLS 1.0 CipherSpecs' ı nasıl etkinleştirdiğiniz

Önemli: IBM MQ kanallarıyla çalışırken, bir CipherSpeckullanıyorsunuz. Java kanallarıyla, JMS kanallarıyla ya da bir MQTT kanallarıyla çalışırken, CipherSuiteolarak belirtilir.

CipherSpecshakkında daha fazla bilgi için bkz. “CipherSpecs' in etkinleştirilmesi” sayfa 402.

CipherSuite , TLS bağlantısı tarafından kullanılan bir şifreleme algoritmasıdır. Bir süit üç ayrı algoritmadan oluşur:

- El sıkışma sırasında kullanılan anahtar değişimi ve kimlik doğrulama algoritması
- Verileri şifrelemek için kullanılan şifreleme algoritması
- İleti özetini oluşturmak için kullanılan MAC (Message Authentication Code) algoritması

Takımın her bileşeni için birkaç seçenek vardır; ancak, TLS bağlantısı için belirtildiğinde yalnızca belirli birleşimler geçerlidir. Geçerli bir CipherSuite adı, kullanılan algoritmaların bileşimini tanımlar. Örneğin, CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA şunları belirtir:

- RSA anahtar değiş tokası ve doğrulama algoritması
- 128 bit anahtar ve şifre bloğu zincirleme (CBC) kipi kullanılarak AES şifreleme algoritması
- SHA-1 İleti Kimlik Doğrulama Kodu (MAC)

SSL/TLS ' de dijital imzalar

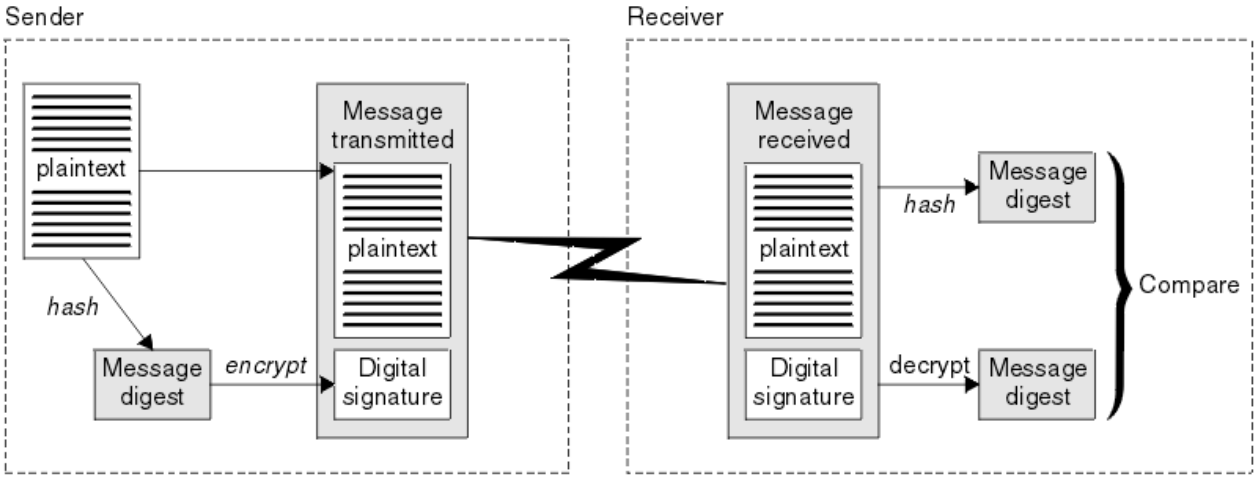
Dijital imza, bir iletinin gösterimini şifreleyerek oluşturulur. Şifreleme, imzaya ilişkin özel anahtarı kullanır ve verimlilik için genellikle iletinin kendisinden ziyade bir ileti özeti üzerinde çalışır.

Dijital imzalar, imzalanmakta olan belgenin içeriğine bağlı olmayan el yazılı imzaların aksine imzalanmakta olan verilere göre değişiklik gösterir. İki farklı ileti aynı varlık tarafından dijital olarak imzalanırsa, iki imza farklı olur, ancak her iki imza da aynı genel anahtarla doğrulanabilir; yani, iletileri imzalayan varlığın genel anahtarı.

Dijital imza işleminin adımları aşağıdaki gibidir:

1. Gönderici bir ileti özetini hesaplar ve daha sonra, gönderenin özel anahtarını kullanarak özeti şifreler, dijital imzayı oluşturur.
2. Gönderen, dijital imzayı mesajla iletir.
3. Alıcı, gönderenin genel anahtarını kullanarak dijital imzanın şifresini çözer ve gönderenin ileti özetini yeniden oluşturur.
4. Alıcı, alınan ileti verilerinden bir ileti özetini hesaplar ve iki sindirenin aynı olduğunu doğrular.

Şekil 6 sayfa 19 bu işlemi gösterir.



Şekil 6. Dijital imza işlemi

Sayısal imza doğrulanırsa, alıcı şunları bilir:

- İleti iletim sırasında değiştirilmedi.
- İleti, iletiyi gönderdiğini iddia eden varlık tarafından gönderildi.

Dijital imzalar bütünlük ve kimlik doğrulama hizmetlerinin bir parçasıdır. Dijital imzalar köken kanıtı da sağlar. Yalnızca gönderen özel anahtarı bilir, bu da gönderenin iletiyi oluşturan kişi olduğuna dair güçlü kanıtlar sağlar.

Not: İletideki bilgilerin gizliliğini koruyan iletiyi de şifreleyebilirsiniz.

Federal Bilgi İşleme Standartları

ABD hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği hakkında teknik danışmanlık yapıyor. National Institute for Standards and Technology (NIST), BT sistemleri ve güvenliği ile ilgili önemli bir organa sahip. NIST, Federal Bilgi İşleme Standartları (FIPS) de dahil olmak üzere öneriler ve standartlar üretir.

Bu standartlardan önemli bir tanesi, güçlü şifreleme algoritmaları kullanılmasını gerektiren FIPS 140-2 'dir. FIPS 140-2 ayrıca, geçiş sırasında yapılan değişikliklere karşı paketleri korumak için kullanılacak karma algoritmalara ilişkin gereksinimleri de belirtir.

IBM MQ , bunu yapmak üzere yapılandırıldığında FIPS 140-2 desteği sağlar.

Zamanla, analistler var olan şifreleme ve hash algoritmalarına karşı saldırılar geliştiriyor. Bu saldırılara karşı koymak için yeni algoritmalar benimsendi. FIPS 140-2, bu değişiklikleri dikkate almak için düzenli aralıklarla güncellenir.

İlgili kavramlar

“Ulusal Güvenlik Ajansı (NSA) Suite B Cryptography” sayfa 19
Amerika Birleşik Devletleri hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği konusunda teknik danışmanlık yapıyor. ABD Ulusal Güvenlik Dairesi (NSA), Suite B standardındaki bir dizi işletilebilir kriptografik algoritmayı önermektedir.

Ulusal Güvenlik Ajansı (NSA) Suite B Cryptography

Amerika Birleşik Devletleri hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği konusunda teknik danışmanlık yapıyor. ABD Ulusal Güvenlik Dairesi (NSA), Suite B standardındaki bir dizi işletilebilir kriptografik algoritmayı önermektedir.

A Suite B standardı, yalnızca belirli bir güvenli şifreleme algoritmaları kümesinin kullanıldığı bir işlem kipini belirtir. A Suite B standard şunları belirtir:

- Şifreleme algoritması (AES)
- Anahtar değişimi algoritması (ECDH olarak da bilinen üç Eliptik Eğri Diffie-Hellman)

- Dijital imza algoritması (ECDSA olarak da bilinen Eliptik Eğri Dijital Imza Algoritması)
- HASH algoritmaları (SHA-256 ya da SHA-384)

Ek olarak, IETF RFC 6460 standardı, Suite B standardıyla uyumlu olması için gerekli olan ayrıntılı uygulama yapılandırmasını ve davranışını tanımlayan Suite B uyumlu profillerini belirtir. İki tanıtım tanımlar:

1. TLS 1.2ile kullanım için bir Suite B uyumlu profil. Suite B uyumlu işlem için yapılandırıldığında, yalnızca listelenmiş olan sınırlı şifreleme algoritmaları kümesi kullanılır.
2. TLS 1.0 ya da TLS 1.1ile kullanım için geçiş profili. Bu profil, Suite olmayan B uyumlu sunucularla birlikte çalışabilirlik sağlar. Suite B geçiş işlemi için yapılandırıldığında, ek şifreleme ve HASH algoritmaları kullanılabilir.

Takım B standardı kavramsal olarak, güvenli bir güvenlik düzeyi sağlamak üzere etkinleştirilmiş şifreleme algoritmaları kümesini kısıtladığı için, kavramsal olarak FIPS 140-2 'ye benzerdir.

Windowssistemlerinde UNIX and Linux sistemleri, IBM MQ, Suite B uyumlu TLS 1.2 profiline uyacak şekilde yapılandırılabilir, ancak Suite B geçişli profilini desteklemez. Daha fazla bilgi için bkz. “NSA Suite B Cryptografi (IBM MQ)” sayfa 38.

İlgili başvurular

“Federal Bilgi İşleme Standartları” sayfa 19
ABD hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği hakkında teknik danışmanlık yapıyor. National Institute for Standards and Technology (NIST), BT sistemleri ve güvenliği ile ilgili önemli bir organa sahip. NIST, Federal Bilgi İşleme Standartları (FIPS) de dahil olmak üzere öneriler ve standartlar üretir.

IBM MQ güvenlik mekanizmaları

Bu konu derlemi, IBM MQiçindeki çeşitli güvenlik kavramlarını nasıl uygulayabileceğiniz ele geçirmektedir.

IBM MQ , “Güvenlik kavramları ve mekanizmaları” sayfa 5' ta tanıtılan tüm güvenlik kavramlarını uygulamak için mekanizmalar sağlar. Bunlar, aşağıdaki bölümlerde daha ayrıntılı bir şekilde ele alınmıştır.

IBM MQ' ta kimlik doğrulama ve kimlik doğrulama

IBM MQ' ta, ileti bağlamı bilgilerini ve karşılıklı kimlik doğrulamayı kullanarak kimlik doğrulama ve kimlik doğrulaması uygulayabilirsiniz.

Aşağıda, bir IBM MQ ortamında tanımlama ve kimlik doğrulamaya ilişkin bazı örnekler bulunmaktadır:

- Her ileti *ileti bağlamı* bilgisi içerebilir. Bu bilgiler ileti tanımlayıcısında tutulur. Kuyruk yöneticisi tarafından, bir ileti bir uygulama tarafından kuyruğa konduğunda, kuyruk yöneticisi tarafından yaratılabilir. Diğer bir seçenek olarak, uygulamayla ilişkili kullanıcı kimliğinin bu işlemi gerçekleştirme yetkisi varsa, uygulama bilgi sağlayabilir.

  Bir iletteki bağlam bilgileri, alma uygulamasının iletiyi yaratan kişi hakkında bilgi bulmasına olanak sağlar. Örneğin, iletiyi ve uygulamayla ilişkili kullanıcı kimliğini içeren uygulamanın adını içerir.
- Bir ileti kanalı başlatıldığında, kanalın her bir ucundaki ileti kanalı aracısı (MCA) iş ortağını doğrulamak için mümkün olur. Bu teknik, *karşılıklı kimlik doğrulama*olarak bilinir. MCA gönderimi için, ileti göndermek üzere olduğu iş ortağının gerçek olduğu güvencisini sağlar. Alıcı MCA için, gerçek bir ortaktan ileti almak üzere olduğu benzer bir güvence vardır.

İlgili kavramlar

“Tanımlama ve kimlik doğrulama” sayfa 6
Tanımlama , sistemde çalışmakta olan bir sistemi ya da uygulamayı benzersiz olarak tanımlama yeteneğidir. *Kimlik Doğrulaması* , bir kullanıcının ya da uygulamanın o kişinin ya da uygulamanın ne kadar talep ettiği konusunda gerçekten kim olduğunu kanıtlayabilme yeteneğidir.

IBM MQiçinde yetki

Belirli kişileri ya da uygulamaları IBM MQ ortamınızda yapabilme yetkisini sınırlandırmak için yetki kullanabilirsiniz.

Aşağıda, bir IBM MQ ortamında yetki verilmesine ilişkin bazı örnekler bulunmaktadır:

- Yalnızca yetkili bir yöneticinin IBM MQ kaynaklarını yönetmek için komutlar yayınlanmasına izin verilir.
- Bir uygulamanın bir kuyruk yöneticisine bağlanmasına izin verilmesi, ancak uygulamayla ilişkili kullanıcı kimliğinin bunu yapma yetkisi olması gerekir.
- Bir uygulamanın, yalnızca işlevi için gerekli olan kuyrukları açmasına izin verilmesi.
- Bir uygulamanın, yalnızca işlevi için gerekli olan konulara abone olması için izin verilmesi.
- Bir uygulamanın, yalnızca kendi işlevi için gerekli olan bir kuyruktaki işlemleri gerçekleştirmesine izin verilmesi. Örneğin, bir uygulamanın yalnızca belirli bir kuyruktaki iletilere göz atmak ve ileti koymak ya da ileti almak için değil olması gerekebilir.

Yetkilendirmeyi nasıl ayarladığınız hakkında daha fazla bilgi için bkz. “Planlama yetkilendirmesi” sayfa 79 ve ilişkili alt konular.

İlgili kavramlar

“Yetkilendirme” sayfa 6

Yetki yalnızca yetkili kullanıcılara ve uygulamalarına erişimi sınırlandırarak kritik öneme sahip kaynakları bir sistemde korur. Bir kaynağın yetkisiz kullanımını ya da kaynak kullanımını yetkisiz bir şekilde önler.

IBM MQiçinde denetim

IBM MQ , olağan dışı etkinliğin gerçekleşmiş olduğunu kaydetmek için olay iletileri yayınlayabilir.

Aşağıda, IBM MQ ortamında denetim örnekleri yer alıyor:

- Uygulama, açma yetkisi olmayan bir kuyruğu açmayı dener. Bir özel işlemden geçirme olayı iletisi yayınlandı. Olay iletisini inceleyerek, bu girişin ortaya çıktığını ve gerekli olan işleme karar verebileceğinin keşfini gerçekleştirdiğinizi fark eder.
- Uygulama bir kanalı açmayı deniyor, ancak SSL bağlantıya izin vermediği için girişim başarısız oldu. Bir özel işlemden geçirme olayı iletisi yayınlandı. Olay iletisini inceleyerek, bu girişin ortaya çıktığını ve gerekli olan işleme karar verebileceğinin keşfini gerçekleştirdiğinizi fark eder.

İlgili kavramlar

“Denetleme” sayfa 6

Denetleme , beklenmeyen ya da yetkisiz bir etkinliğin gerçekleşip gerçekleştirilmediğini ya da bu tür bir etkinliği gerçekleştirme girişiminde bulunulup bulunulmadığını saptamak için olayları kaydetme ve denetleme işletidir.

IBM MQ' da gizlilik

İletileri şifreleyerek IBM MQ ' ta gizliliği uygulayabilirsiniz.

Gizlilik, IBM MQ ortamında aşağıdaki gibi sağlanabilir:

- MCA gönderimi bir iletim kuyruğundan ileti aldıktan sonra, IBM MQ iletiyi ağ üzerinden gönderilen MCA 'ya göndermeden önce şifrelemek için TLS' yi kullanır. Kanalın diğer ucunda, MCA ' nın hedef kuyruğuna yerleştirmeden önce iletinin şifresi çözülür.
- İletiler yerel bir kuyruğun üzerinde saklanırken, IBM MQ tarafından sağlanan erişim denetimi mekanizmaları, içeriklerini yetkisiz bir şekilde açıklamaya karşı korumak için yeterli olabilir. Ancak, daha yüksek bir güvenlik düzeyi için, kuyrukta saklanan iletileri şifrelemek için Advanced Message Security ' u kullanabilirsiniz.
- z/OS V 9.1.4 Messages stored on local queues can be encrypted at rest using z/OS data set encryption.

confidentiality for data at rest on IBM MQ for z/OS with data set encryption.bölümüne bakın. daha fazla bilgi için.

İlgili kavramlar

“Gizlilik” sayfa 7
Gizlilik hizmeti, hassas bilgileri yetkisiz açıklamalardan korur.

IBM MQiçindeki veri bütünlüğü

Bir iletinin değiştirilip değiştirilmediğini saptamak için veri bütünlüğü hizmetini kullanabilirsiniz.

Veri bütünlüğü, IBM MQ ortamında aşağıdaki gibi sağlanabilir:

- Bir iletinin içeriğinin, bir ağ üzerinden iletilirken kasıtlı olarak değiştirilip değiştirilmediğini saptamak için TLS ' yi kullanabilirsiniz. TLS ' de, ileti özetleme algoritması, değiştirilen iletilerin aktarmaya ilişkin algılanmasını sağlar.

  Tüm IBM MQ CipherSpecs , ileti verisi bütünlüğü sağlamayan TLS_RSA_WIT_NULL_NULL dışında bir ileti özeti algoritması sağlar.

  IBM MQ , bunları aldıktan sonra değiştirilen iletileri algılar; değiştirilmiş bir ileti alındığında, IBM MQ bir AMQ9661 hata iletisi atar ve kanal durur.
- İletiler yerel bir kuyruğun üzerinde saklanırken, IBM MQ tarafından sağlanan erişim denetimi mekanizmaları, iletilerin içeriğinin kasıtlı olarak değiştirilmesini önlemek için yeterli olarak düşünülebilebilir.

  However, for a greater level of security, you can use Advanced Message Security to detect whether the contents of a message have been deliberately modified between the time the message was put on the queue and the time it was retrieved from the queue.

  Değiştirilmiş bir ileti algılandıktan sonra, iletiyi almaya çalışan uygulama 2063 dönüş kodunu alır ve MQGET çağrısı kullanılıyorsa, ileti SYSTEM.PROTECTION.ERROR.QUEUE

İlgili kavramlar

“Veri bütünlüğü” sayfa 7
Veri bütünlüğü hizmeti, verilerin yetkisiz olarak değiştirilip değiştirilmediğini belirler.

IBM MQiçinde şifreleme

IBM MQ , Transport Security Layer (TLS) iletişim kuralını kullanarak şifreleme sağlar.

Daha fazla bilgi için bkz. “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22.

İlgili kavramlar

“Şifreleme kavramları” sayfa 7
Bu konu derlemi, IBM MQiçin geçerli olan şifreleme kavramlarını açıklar.

IBM MQiçinde TLS güvenlik iletişim kuralları

IBM MQ , ileti kanalları ve MQI kanalları için bağlantı düzeyinde güvenlik sağlamak üzere TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolünü destekler.

İleti kanalları ve MQI kanalları, bağlantı düzeyinde güvenlik sağlamak için TLS iletişim kuralını kullanabilir. Çağıran MCA bir TLS istemcisinden ve yanıt veren MCA bir TLS sunucudur. IBM MQ , TLS 1.0 ve TLS 1.2' yi destekler. Kanal tanımlamasının bir parçası olarak bir CipherSpec sağlayarak TLS iletişim kuralı tarafından kullanılan şifreleme algoritmalarını belirleyebilirsiniz.

Not: IBM MQ 8.0.0 Fix Pack 2' tan, SSLv3 iletişim kuralı ve bazı IBM MQ CipherSpecs kullanımına ilişkin kullanım önerilmemektedir. Daha fazla bilgi için bkz. Deprecation: SSLv3 iletişim kuralı.

Güvenlik iletişim kuralını görüntülemek için SECPROT ve SSLCIPH parametrelerini, bir kanalda kullanılan CipherSpec ' i kullanabilirsiniz.

Bir ileti kanalının her iki ucunda ve bir MQI kanalının sunucu ucunda, MCA bağlı olduğu kuyruk yöneticisi adına hareket eder. TLS el sıkışması sırasında MCA, kuyruk yöneticisinin dijital sertifikasını, kanalın diğer

ucundaki iş ortağı MCA ' ya gönderir. Bir MQI kanalının istemci ucunda bulunan IBM MQ kodu, IBM MQ istemci uygulamasının kullanıcısı adına hareket eder. TLS el sıkışması sırasında IBM MQ kodu, kullanıcının dijital sertifikasını MQI kanalının sunucu ucundaki MCA ' ya gönderir.

SSLCAUTH (GEREKLI), kanalın sunucu tarafında belirtilmedikçe, kuyruk yöneticileri ve IBM MQ istemci kullanıcılarının, TLS istemcileri olarak işlem yaparken kendileriyle ilişkili kişisel sayısal sertifikalarına sahip olması gerekmez.

Dijital sertifikalar bir *anahtar havuzunda*depolanır. Kuyruk yöneticisi özniteliği **SSLKeyRepository** , kuyruk yöneticisinin sayısal sertifikasını tutan anahtar havuzunun yerini belirtir. Bir IBM MQ istemcisi sisteminde, MQSSLKEYR ortam değişkeni, kullanıcının dijital sertifikasını tutan anahtar havuzunun yerini belirtir. Diğer bir seçenek olarak, bir IBM MQ istemci uygulaması, MQCONNX çağrısında, TLS yapılandırma seçenekleri yapısının **KeyRepository** alanında yerini belirtebilir. Temel havuzlarla ilgili daha fazla bilgi ve konumlarının nasıl belirleneceği hakkında daha fazla bilgi için ilgili konulara bakın.

TLS desteği

IBM MQ , kullanmakta olduğunuz platforma göre TLS 1.0 ve TLS 1.2 için destek sağlar. TLS iletişim kuralı hakkında daha fazla bilgi için alt konulardaki bilgilere bakın.

IBM i
TLS desteği, IBM i işletim sisteminin ayrılmaz bir parçasıdır.

Java ve JMS istemcileri
Bu istemciler, TLS desteği sağlamak için JVM ' yi kullanır.

UNIX, Linux, and Windows sistemleri
TLS desteği, IBM MQile birlikte kurulur.

z/OS
TLS desteği, z/OS işletim sisteminin ayrılmaz bir parçasıdır. The TLS support on z/OS is known as *Sistem SSL*.

IBM MQ TLS desteğine ilişkin önkoşullarla ilgili bilgi için bkz. IBM MQ.

İlgili kavramlar
“Şifreleme güvenlik iletişim kuralları: TLS” sayfa 14
Şifreleme iletişim kuralları güvenli bağlantılar sağlar ve iki tarafın gizlilik ve veri bütünlüğü ile iletişim kurmasını sağlar. TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolü, SSL (Secure Sockets Layer; Güvenli Yuva Arabirimi Katmanı) olanağından evrimleşti. IBM MQ TLS ' yi destekler.

SSL/TLS anahtarı havuzu
Kimliği karşılıklı olarak doğrulanan TLS bağlantısı, bağlantının her bir ucunda bir anahtar havuzu gerektirir. Anahtar havuzu, sayısal sertifikalar ve özel anahtarlar içerir.

Bu bilgiler, dijital sertifikalar ve ilişkili özel anahtarlara ilişkin mağazeyi açıklamak için *anahtar havuzu* genel terimini kullanır. Anahtar havuzu, TLS ' yi destekleyen farklı altyapılarda ve ortamlarda farklı adlarla gönderme yapılan bir havuzdur.

- IBM i IBM iüzerinde: *sertifika deposu*
- Java ve JMSüzerinde: *keystore* ve *truststore*
- ULW UNIX, Linux, and Windowsüzerinde: *anahtar veritabanı dosyası*
- z/OS z/OSüzerinde: *keyring*

Daha fazla bilgi için bkz. “dijital sertifikalar” sayfa 9 ve “Transport Layer Security (TLS) kavramları” sayfa 14.

Kimliği karşılıklı olarak doğrulanan TLS bağlantısı, bağlantının her bir ucunda bir anahtar havuzu gerektirir. Anahtar havuzu aşağıdaki sertifikaları ve istekleri içerebilir:

- Kuyruk yöneticisinin ya da istemcinin, bağlantının uzak ucundaki ortasından aldığı sertifikaları doğrulamasına izin veren çeşitli Sertifika Yetkilileri 'nden CA sertifikalarının sayısı. Tek tek sertifikalar bir sertifika zincirinde olabilir.
- Bir Sertifikasyon Yetkilisinden alınan bir veya daha fazla kişisel sertifika. Ayrı bir kişisel sertifikayı her kuyruk yöneticisi ya da IBM MQ MQI clientile ilişkilendirin. Karşılıklı kimlik doğrulaması gerekirse, TLS istemcisi üzerinde kişisel sertifikalar gereklidir. Karşılıklı kimlik doğrulaması gerekli değilse, istemcide kişisel sertifikalara gerek yoktur. Anahtar havuzu, her kişisel sertifikan karşılık gelen özel anahtarı da içerebilir.
- Güvenilir bir sertifika kuruluşu sertifikası tarafından imzalanmış olarak bekleyen sertifika istekleri.

Anahtar havuzunuzu koruma hakkında daha fazla bilgi için bkz. "IBM MQ anahtar havuzlarının korunması" sayfa 24.

Anahtar havuzunun yeri, kullanmakta olduğunuz altyapıya bağlıdır:

IBM i **IBM i**

Anahtar havuzu bir sertifika deposudur. Varsayılan sistem sertifika deposu, tümleşik dosya sisteminde (IFS) `/QIBM/UserData/ICSS/Cert/Server/Default` konumunda bulunur. IBM MQ , sertifika deposunun parolasını bir *parola saklama dosyası*içinde saklar. Örneğin, `QM1` kuyruk yöneticisine ilişkin parola saklama dosyası `/QIBM/UserData/mqm/qmgrs/QM1/ssl/Stash.sth`' dir.

Diğer bir seçenek olarak, bunun yerine IBM i sistem sertifikası deposunun kullanılacağını da belirtebilirsiniz. Bu işlemi yapmak için, kuyruk yöneticisi **SSLKEYR** özniteliğinin değerini `*SYSTEM`olarak değiştirin. Bu değer, kuyruk yöneticisinin sistem sertifika deposunu kullanması gerektiğini ve kuyruk yöneticisinin Digital Certificate Manager (DCM) ile bir uygulama olarak kullanılmak üzere kaydedildiğini belirtir.

Sertifika deposu, kuyruk yöneticisi için özel anahtarı da içerir.

ULW **UNIX, Linux, and Windows sistemleri**

Anahtar havuzu, anahtar veri tabanı dosyasıdır. Anahtar veritabanı dosyasının adı, `.kdb`dosya uzantısına sahip olmalıdır. For example, on UNIX and Linux, the default key database file for queue manager `QM1` is `/var/mqm/qmgrs/QM1/ssl/key.kdb`. IBM MQ varsayılan konuma kurulduysa, Windows üzerindeki eşdeğer yol `C:\ProgramData\IBM\MQ\Qmgrs\QM1\ssl\key.kdb`olur.

Her anahtar veri tabanı dosyasında, ilişkili bir parola saklama dosyası vardır. Bu dosya, programların anahtar veritabanına erişmelerini sağlayan kodlanmış parolaları içerir. Parola şifreleme dosyası aynı dizinde olmalı ve anahtar veritabanı ile aynı dosya sapına sahip olmalı ve `.sth`sonekiyle bitmelidir (örneğin, `/var/mqm/qmgrs/QM1/ssl/key.sth`).

Not: PKCS #11 şifreleme donanım kartları, anahtar veritabanı dosyasında başka bir şekilde tutulan sertifikaları ve anahtarları içerebilir. PKCS #11 kartlarında sertifikalar ve anahtarlar tutulduğunda, IBM MQ yine de hem anahtar veritabanı dosyasına hem de parola saklama dosyasına erişim gerektirir.

UNIX ve Windows sistemlerinde, anahtar veritabanı, kuyruk yöneticisi ya da IBM MQ MQI clientile ilişkili kişisel sertifikana ilişkin özel anahtarı da içerir.

z/OS **z/OS**

Sertifikalar z/OSiçindeki bir anahtarlık içinde tutulur.

Diğer dış güvenlik yöneticileri (ESM ' ler) de sertifikaları saklamak için anahtaryüzüleri kullanır.

Özel anahtarlar RACFtarafından yönetilir.

IBM MQ anahtar havuzlarının korunması

IBM MQ için anahtar havuzu bir dosyadır. Yalnızca amaçlanan kullanıcının anahtar havuz dosyasına erişebildiğinden emin olun. Bu, izinsiz giriş yapan bir kullanıcının ya da diğer yetkisiz kullanıcıların anahtar havuzu dosyasını başka bir sisteme kopyalamasını önler ve o sistemde aynı kullanıcı kimliğini kullanarak, amaçlanan kullanıcının kimliğini edinir.

Dosyalardaki izinler, kullanıcının umask 'ına ve hangi aracın kullanılsa bağlıdır. On Windows, IBM MQ accounts require permission `BypassTraverseChecking` which means the permissions of the folders in the file path have no effect.

Anahtar havuzu dosyalarının dosya izinlerini denetleyin ve dosyaların ve içeren klasörün dünya tarafından okunabilir olmadığından emin olun, tercihen grup tarafından okunabilir olmadığınızdan emin olun.

Yalnızca yöneticinin bakım gerçekleştirmek için yazma işlemlerini etkinleştirmesine izin verilmesiyle, anahtar deposunun salt okunur olması, hangi sistemde kullanılsa da iyi bir uygulamadır.

Uygulamada, konum ve parola korumalı olsun ya da olmasın, tüm anahtar depolarını korumalısınız; anahtar havuzlarını korumalısınız.

Dijital sertifika etiketleri, gereksinimleri anlama
Dijital sertifikaları kullanmak için TLS ' yi ayarlarken, kullanılan platforma ve bağlanmak için kullandığınız yönteme bağlı olarak, izlememeniz gereken belirli etiket gereksinimleri olabilir.

Sertifika etiketi nedir?

Sertifika etiketi, anahtar havuzunda saklanan sayısal bir sertifikayı temsil eden benzersiz bir tanıtıcıdır ve anahtar yönetimi işlevlerini gerçekleştirirken belirli bir sertifikaya gönderme yapmak için uygun, insan tarafından okunabilir bir ad sağlar. Sertifika etiketini, anahtar havuzuna ilk kez sertifika eklerken atayabilirsiniz.

Sertifika etiketi, sertifikanda **`Subject Distinguished Name`** ya da **`Subject Common Name`** alanlarından ayrıdır. **`Subject Distinguished Name`** ve **`Subject Common Name`** ' in sertifika içindeki alanlarla ilgili olduğunu unutmayın. Bu bilgiler, sertifika yaratıldığında tanımlanır ve değiştirilemez. Ancak gerekirse, dijital sertifikayla ilişkili etiketi değiştirebilirsiniz.

Sertifika etiketi sözdizimi

Bir sertifika etiketi aşağıdaki koşullarla harfler, sayılar ve noktalama işaretleri içerebilir:

- Multi Sertifika etiketi en çok 64 karakter içerebilir.
- z/OS Sertifika etiketi en çok 32 karakter içerebilir.
- Sertifika etiketi boşluk içerebilir.
- Etiketler büyük ve küçük harfe duyarlıdır.
- EBCDIC Katakana kullanan sistemlerde küçük harfli karakterler kullanamazsınız.

Sertifika etiketi değerlerine ilişkin ek gereksinimler aşağıdaki bölümlerde belirtilmiştir.

Sertifika etiketi nasıl kullanılır?

IBM MQ , TLS el sıkışması sırasında gönderilen kişisel bir sertifikayı bulmak için sertifika etiketlerini kullanır. Bu, anahtar havuzunda birden çok kişisel sertifikana sahip olduğunda belirsizlik ortadan kalkar.

Sertifika etiketini seçiminizin bir değerine ayarlayabilirsiniz. Bir değer ayarlamadıysanız, kullandığınız platforma bağlı olarak bir adlandırma kuralını izleyen varsayılan bir etiket kullanılır. Ayrıntılar için, aşağıdaki bölümlere, belirli platformlara ilişkin bölümlere bakın.

Notlar:

1. You cannot set the certificate label yourself on Java or JMS systems.
2. Kanal otomatik tanımlaması (CHAD) çıkışı tarafından oluşturulan otomatik tanımlı kanallar, kanal yaratıldığı zaman TLS anlaşması olduğu için sertifika etiketini ayarlayamaz. Gelen kanallara ilişkin CHAD çıkışta sertifika etiketinin ayarlanması hiçbir etkiye sahip değildir.

Bu bağlamda, TLS istemcisi, bir IBM MQ istemcisi ya da başka bir kuyruk yöneticisi olabilen el sıkışmayı başlatan bağlantı ortağına başvurur.

TLS anlaşması sırasında, TLS istemcisi her zaman, sunucudan sayısal bir sertifikayı doğrular ve doğrular. IBM MQ uygulaması ile, TLS sunucusu her zaman istemciden bir sertifika ister ve istemci her zaman, bulunursa sunucuya bir sertifika verir. İstemci kişisel bir sertifikayı bulamazsa, istemci sunucuya bir no `certificate` yanıtı gönderir.

TLS sunucusu, gönderildiyse istemci sertifikasının her zaman geçerliliğini denetler. İstemci bir sertifika göndermezse, TLS sunucusu olarak hareket eden kanalın sonu, **SSLCAUTH** parametresi *REQUIREND* değerine ayarlanmış ya da bir **SSLPEER** parametre değeri kümesi ile tanımlandıysa kimlik doğrulaması başarısız olur.

Gelen kanalların (alıcı, istek sahibi, küme alıcısı, nitelenmemiş sunucu ve sunucu bağlantısı kanalları dahil) yalnızca uzak eşin IBM MQ sürümü sertifika etiketi yapılanışını tam olarak destekliyorsa ve kanal TLS CipherSpeckullanıyorsa, yapılandırılmış sertifikayı gönderdiğini unutmayın.

Nitelenmemiş bir sunucu kanalı, CONNAME alan kümesine sahip olmayan bir kanaldır.

Diğer tüm durumlarda, kuyruk yöneticisi **CERTLABL** parametresi gönderilen sertifikayı belirler. Aşağıdaki, kanala özgü etiket ayarından bağımsız olarak, yalnızca kuyruk yöneticisinin **CERTLABL** parametresi tarafından yapılandırılan sertifikayı yalnızca aşağıdaki şekilde alır:

- IBM MQ 9.1.1' den önce, tüm geçerli Java ve JMS istemcileri.
- V 9.1.1 From IBM MQ 9.1.1, Java and JMS clients supporting Server Name Indication (SNI), that is, certificates on a channel by channel basis.
- IBM MQ 8.0sürümünden önceki IBM MQ sürümleri.
- Yönetilen .NET istemcileri

Ayrıca, kanal tarafından kullanılan sertifika, kanal CipherSpec için uygun olmalıdır; ek bilgi için “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42 ' e bakın.

IBM MQ 8.0 ve daha sonraki bir sürümü, kanal tanımlamasındaki **CERTLABL** özniteliği kullanılarak belirtilen kanal başına sertifika etiketi kullanılarak aynı kuyruk yöneticisine birden çok sertifika kullanılmasını destekler. Kuyruk yöneticisinden doğru sertifikayı sunmak için kuyruk yöneticisine (örneğin, sunucu bağlantısı ya da alıcı) gelen kanallar, kanal adının TLS Server Name Indication (SNI) işlevini kullanarak saptamasına güvenir.

If a channel connects to the destination queue manager through IBM MQ Internet Pass-Thru (MQIPT), and the MQIPT route has both **SSLServer** and **SSLClient** set, there are two separate TLS sessions between the endpoints, and the SNI data does not flow across the session break. This prevents a per-channel certificate from being used on the destination queue manager, for the TLS connection between MQIPT and the queue manager. Hedef kuyruk yöneticinde kanal başına bir sertifika kullanmak için, MQIPTüzerinden geçen bir TLS bağlantısı için, MQIPT rotasının, SNI adı da dahil olmak üzere tüm TLS denetim akışlarını sağlam bir şekilde ileten TLS yetkili sunucu kipini kullanması gerekir. MQIPT' ta TLS desteği hakkında daha fazla bilgi için bkz. SSL/TLS desteği.

MQIPT tarafından sonlandırılan ya da başlatılan TLS bağlantıları için kullanılan sertifikalar her rota için ayrı olarak yapılandırılabilir; örneğin, **SSLServerSiteLabel** ve **SSLClientSiteLabel** rota özellikleri kullanılarak.

Tek yönlü kimlik doğrulamasını kullanarak bir kuyruk yöneticisini bağlama hakkında daha fazla bilgi için, bu durumda TLS istemcisi bir sertifika göndermezse, Tek yönlü kimlik doğrulaması kullanarak iki kuyruk yöneticisinin bağlanmasıbaşlıklı konuya bakın.

Çoklu Platformlar

Multi

Multiplatformsüzerinde, TLS sunucusu istemciye bir sertifika gönderir.

Sırasıyla kuyruk yöneticileri ve istemciler için, aşağıdaki kaynaklar boş olmayan bir değer için sırayla aranır. İlk boş olmayan değer, sertifika etiketini belirler. Sertifika etiketinin anahtar havuzunda var olması gerekir. Bir etiketle eşleşen doğru durumda ve biçim içinde eşleşen bir sertifika bulunmazsa, bir hata oluşur ve TLS anlaşması başarısız olur.

Kuyruk yöneticileri

1. Kanal sertifikası etiket özniteliği **CERTLABL**.
2. Kuyruk yöneticisi sertifikası etiket özniteliği **CERTLABL**.
3. Varsayılan olarak, şu biçimde olan bir varsayılan değer: `ibmwebspheremq` sonuna kuyruk yöneticisi adı eklenmiş olarak, tümü küçük harfli olarak eklenir. Örneğin, `QM1`adlı bir kuyruk yöneticisi için varsayılan sertifika etiketi `ibmwebspheremqqm1`olur.

IBM MQ müşterileri

1. CLNTCONN kanal tanımlamasındaki **CERTLABL** sertifika etiketi özniteliği.
2. MQSCO yapısı **`CertificateLabel`** özniteliği.
3. Ortam değişkeni **MQCERTLABL**.
4. İstemci `.ini` dosyası (SSL bölümünde) **`CertificateLabel`** özniteliğe
5. Varsayılan bir varsayılan değer: `ibmwebspheremq` , istemci uygulamasının sonuna kadar çalıştırıldığı kullanıcı kimliğiyle, tümü küçük harfli olarak çalıştırılır. Örneğin, `USER1`kullanıcı kimliği için varsayılan sertifika etiketi `ibmwebspheremquser1`olur.

z/OS sistemleri

z/OS

IBM MQ istemcileri, z/OSüzerinde desteklenmez. Ancak, bir z/OS kuyruk yöneticisi bir bağlantı başlatırken TLS istemcisi ya da bir bağlantı isteği kabul edildiğinde TLS sunucusu rolünde işlem yapabilir. z/OS kuyruk yöneticileri için sertifika etiketi gereksinimleri bu rollerin her ikisinde de geçerlidir ve Multiplatformsüzerindeki gereksinimlerden farklı olarak farklılık gösterir.

Sırasıyla kuyruk yöneticileri ve istemciler için, aşağıdaki kaynaklar boş olmayan bir değer için sırayla aranır. İlk boş olmayan değer, sertifika etiketini belirler. Sertifika etiketinin anahtar havuzunda var olması gerekir. Bir etiketle eşleşen doğru durumda ve biçim içinde eşleşen bir sertifika bulunmazsa, bir hata oluşur ve TLS anlaşması başarısız olur.

1. Kanal sertifikası etiket özniteliği, **CERTLABL**.
2. Paylaşılıyorsa, kuyruk paylaşım grubu sertifika etiketi özniteliği (**CERTQSGL**).

   Paylaşılmamışsa, kuyruk yöneticisi sertifikası etiketi özniteliği **CERTLABL**.
3. Kuyruk yöneticisi ya da kuyruk paylaşım grubu adının sonuna eklenen, varsayılan değer olarak `ibmWebSphereMQ` biçiminde olan bir varsayılan değer. Bu dizginin büyük ve küçük harfe duyarlı olduğunu ve gösterildiği gibi yazılmalıdır. Örneğin, `QM1`adlı bir kuyruk yöneticisi için varsayılan sertifika etiketi `ibmWebSphereMQQM1`olur.
4. If there is not a certificate found with the format in option “3” sayfa 27, IBM MQ attempts to use the certificate marked as default in the key ring.

Anahtar havuzunun nasıl görüntüleneceği ile ilgili bilgi için bkz. “z/OSüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzunun bulunması” sayfa 306.

IBM MQ Java ve IBM MQ JMS istemcileri

IBM MQ Java and IBM MQ JMS clients use the facilities of their Java Secure Socket Extension (JSSE) provider to select a personal certificate during the TLS handshake and are not therefore subject to certificate label requirements.

Varsayılan davranış, JSSE istemcisinin anahtar havuzundaki sertifikalar aracılığıyla yinelemesi, bulunan ilk kabul edilebilir kişisel sertifika seçmesi olur. Ancak, bu davranış yalnızca bir varsayılan davranır ve JSSE sağlayıcısının uygulamasına bağlıdır.

Buna ek olarak, JSSE arabirimi, uygulama tarafından çalıştırma zamanında yapılandırma ve doğrudan erişim aracılığıyla yüksek düzeyde özelleştirilebilir. Belirli ayrıntılar için JSSE sağlayıcınız tarafından sağlanan belgelere bakın.

For troubleshooting, or to better understand the handshake performed by the IBM MQ Java client application in combination with your specific JSSE provider, you can enable debugging by setting `javax.net.debug=ssl` in the JVM environment.

Değişkeni uygulama içinde, yapılandırma yoluyla ya da komut satırında `-Djavax.net.debug=ssl` komutunu girerek ayarlayabilirsiniz.

Kuyruk yöneticisinin anahtar havuzu yenileniyor
Bir anahtar havuzunun içeriğini değiştirdiğinizde, kuyruk yöneticisi yeni içeriği hemen açmaz. Kuyruk yöneticisinin yeni anahtar havuzu içeriğini kullanması için, REFRESH SECURITY TYPE (SSL) komutunu vermelisiniz.

Bu işlem kasıtlı bir işlemdir ve birden çok çalışan kanalların bir anahtar havuzunun farklı sürümlerini kullanabilmesinin engellenir. Bir güvenlik denetimi olarak, bir anahtar havuzunun yalnızca bir sürümü kuyruk yöneticisi tarafından herhangi bir zamanda yüklenebilir.

REFRESH SECURITY TYPE (SSL) komutuna ilişkin ek bilgi için REFRESH SECURITY(Güvenlik Yenileme) konusuna bakın.

Bir anahtar havuzunu, PCF komutlarını ya da IBM MQ Explorerkomutunu kullanarak da yenileyebilirsiniz. Daha fazla bilgi için, bu ürün belgelerinin IBM MQ Explorer bölümündeki MQCMD_REFRESH_SECURITY komutu ve *Yenilenmiş TLS Güvenliği* başlıklı konuya bakın.

İlgili kavramlar
“Bir istemcinin SSL/TLS anahtarı havuzu içerikleri ve SSl/TLS ayarları görünümünü yenileme” sayfa 28
İstemci uygulamasını anahtar havuzunun yenilenmiş içeriğiyle güncellemek için istemci uygulamasını durdurmanız ve yeniden başlatmanız gerekir.

Bir istemcinin SSL/TLS anahtarı havuzu içerikleri ve SSl/TLS ayarları görünümünü yenileme
İstemci uygulamasını anahtar havuzunun yenilenmiş içeriğiyle güncellemek için istemci uygulamasını durdurmanız ve yeniden başlatmanız gerekir.

Bir IBM MQ istemcisinde güvenliği yenileyemezsiniz; istemciler için REFRESH SECURITY TYPE (SSL) komutunun eşdeğeri yoktur (REFRESH SECURITY konusuna bakın). daha fazla bilgi için.

Güvenlik sertifikasını değiştirdiğinizde, istemci uygulamasını anahtar havuzunun yenilenmiş içeriğiyle güncellemek için uygulamayı durdurmanız ve yeniden başlatmanız gerekir.

Kanal yeniden başlatılırsa, yapılanışlar yenilenir ve uygulamanızın yeniden bağlantı mantığı varsa, STOP CHL STATUS (DEVREDIŞI) komutunu vererek istemcide güvenliği yenilemeniz mümkün olur.

İlgili kavramlar
“Kuyruk yöneticisinin anahtar havuzu yenileniyor” sayfa 28
Bir anahtar havuzunun içeriğini değiştirdiğinizde, kuyruk yöneticisi yeni içeriği hemen açmaz. Kuyruk yöneticisinin yeni anahtar havuzu içeriğini kullanması için, REFRESH SECURITY TYPE (SSL) komutunu vermelisiniz.

MQCSP parola koruması
From IBM MQ 8.0, you can send passwords that are included in the MQCSP structure either protected, by using IBM MQ functionality, or encrypted, by using TLS encryption.

Önemli: MQCSP parola koruması, sınama ve geliştirme amacıyla, MQCSP parola korumasının kullanılmasının TLS şifrelemesini ayarlamaktan daha basittir, ancak güvenli olarak kullanılmamasını sağlar. Üretim amacıyla, TLS şifrelemesi daha güvenli olduğundan, özellikle istemci ile kuyruk yöneticisi arasındaki ağ güvenilmez olduğunda, IBM MQ parola korumasını tercih ederken TLS şifrelemesini kullanmanız gerekir.

Hangi şifrelemenin kullanılmakta olduğunu ve ne kadar koruma sağladığı konusunda endişeliyseniz, tam TLS şifrelemesi kullanmanız gerekir. Bu durumda, algoritmalar genel olarak bilinmektedir ve **SSLCIPH** kanal özniteliğini kullanarak kuruluşunuza uygun olanı seçebilirsiniz.

MQCSP yapısıyla ilgili ek bilgi için MQCSP yapısıbaşlıklı konuya bakın.

Parola koruması, aşağıdaki koşulların tümü karşılandığında kullanılır:

- Bağlantının her iki ucu da IBM MQ 8.0ya da daha sonraki bir yayın düzeyiyle birlikte kullanılabilir.
- Kanal TLS şifrelemesi kullanmıyor. Kanal boş bir **SSLCIPH** özniteliğine sahipse ya da **SSLCIPH** özniteliği şifreleme sağlamayan bir CipherSpec değerine ayarlıysa, bir kanal TLS şifrelemesi kullanmaz. Boş değerli şifreleme (örneğin, NULL_SHA) şifreleme sağlamıyor.
- **MQCSP**olarak ayarlandınız.**AuthenticationType** -MQCSP_AUTH_USER_ID_AND_PWD. Bu değerin belirlenmesi, parola korumasının yapılıp yapılmadığına karar vermek için daha fazla denetinin değerlendirilmesini sağlar. **MQCSP**varsayılan değeri.**AuthenticationType** , MQCSP_AUTH_NONE olur. Varsayılan ayar ile parola koruması gerçekleştirilmez. Daha fazla bilgi için bkz. **AuthenticationType**.
- İstemci IBM MQ Gezgini (Windows Gezgini) ve kullanıcı kimliği uyumluluğu kipi etkinleştirilmediyse, varsayılan değer bu değildir. Bu koşul yalnızca IBM MQ Gezgini için geçerlidir.

Bu koşullar karşılanmazsa, **PasswordProtection** yapılandırma ayarı tarafından yasaklanmadığı sürece, parola düz metin olarak gönderilir.

PasswordProtection yapılandırma ayarı

İstemcinin ve kuyruk yöneticisi .ini yapılanış kütüklerinin Channelels kısmındaki **PasswordProtection** özniteliği, parolaların düz metin olarak gönderilmesini engelleyebilir. Öznitelik aşağıdaki değerlerden birini alabilir. Varsayılan değer `compatible`değeridir.

Uyumlu
Kuyruk yöneticisi ya da istemci IBM MQ 8.0' den önceki bir IBM MQ sürümünü çalıştırıyorsa, parola düz metin olarak gönderilebilir. Yani, uyumluluk için düz metin parolalarına izin verilir.

Bu nedenle:

- TLS şifrelemesi kullanılıyorsa ve CipherSpec boş değerli değilse, parola TLS CipherSpec tarafından şifrelenir.
- Kuyruk yöneticisi ya da istemci IBM MQ 8.0sürümünden önceki bir IBM MQ sürümü çalıştırıyorsa ve TLS şifrelemesi kullanılmıyorsa, parola düz metin olarak gönderilir. Parola, IBM MQ 8.0 tarihinden önceki IBM MQ sürümleri yalnızca düz metin içinde parola gönderebileceğinden düz metin olarak gönderilir.
- The password is sent protected if both the queue manager and the client are running a version of IBM MQ at IBM MQ 8.0 or later, and either a null CipherSpec is used, or TLS encryption is not used. **MQCSP**.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlanmalıdır.
- The connection fails before the password is sent if both the queue manager and the client are running a version of IBM MQ at IBM MQ 8.0 or later, and **MQCSP**.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlanmamış.

Her zaman
Parola, boş değerli CipherSpecya da **MQCSP**olmayan bir CipherSpec ile şifrelenmelidir.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlanmalıdır. Tersi durumda, bağlantı başarısız olur. Bu, düz metin parolalarına izin verilmez.

Bu nedenle:

- TLS şifrelemesi kullanılıyorsa ve CipherSpec boş değerli değilse, parola TLS CipherSpec tarafından şifrelenir.
- The password is sent protected if both the queue manager and the client are running a version of IBM MQ at IBM MQ 8.0 or later, and either TLS encryption is not used, or a null CipherSpec is used. **MQCSP**.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlanmalıdır.
- Kuyruk yöneticisi ya da istemci IBM MQ 8.0sürümünden önceki bir IBM MQ sürümü çalıştırıyorsa ve TLS şifreleme kullanılmıyorsa, parola gönderilmeden bağlantı başarısız olur. IBM MQ 8.0 sürümünden önceki IBM MQ sürümleri parolaların yalnızca düz metin olarak gönderilebilmesi ve `always` parolasının şifrelenmesini ya da korunmasını gerektirdiğinden, bağlantı başarısız olur.

isteğe bağlı
Parola isteğe bağlı olarak korunuyor olabilir, ancak **MQCSP**ise düz metin olarak gönderilir.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlanmamış. Yani, düz metin parolalarının herhangi bir istemci tarafından gönderilmesine izin verilir.

Bu nedenle:

- TLS şifrelemesi kullanılıyorsa ve CipherSpec boş değerli değilse, parola TLS CipherSpec tarafından şifrelenir.
- Boş değer CipherSpec kullanılırsa ve **MQCSP**ise, parola düz metin olarak gönderilir.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlanmamış.
- Kuyruk yöneticisi ya da istemci IBM MQ 8.0sürümünden önceki bir IBM MQ sürümü çalıştırıyorsa ve TLS şifrelemesi kullanılmıyorsa, parola düz metin olarak gönderilir. Parola, IBM MQ 8.0 tarihinden önceki IBM MQ sürümleri yalnızca düz metin içinde parola gönderebileceğinden düz metin olarak gönderilir.
- The password is sent protected if both the queue manager and the client are running a version of IBM MQ at IBM MQ 8.0 or later, TLS encryption is not used or a null CipherSpec is used, and **MQCSP**.**AuthenticationType** , MQCSP_AUTH_USER_ID_AND_PWD olarak ayarlandı.

uyarı
Düz metin parolalarının herhangi bir istemci tarafından gönderilmesine izin verilir. Düz metin parolası alınırsa, kuyruk yöneticisi hata günlüklerine bir uyarı iletisi (AMQ9297) yazılır.

Java ve JMS istemcileri için, **PasswordProtection** öznitelik değişikliklerinin uyumluluk kipini ya da MQCSP kipini kullanma seçimlerine bağlı olarak değişir:

- Java ve JMS istemcileri uyumluluk kipinde çalışıyorsa, bağlantı işlemesi sırasında bir MQCSP yapısı aktı akıtmaz. Bu nedenle, **PasswordProtection** özniteliğinin davranışı, IBM MQ 8.0sürümünden önceki bir IBM MQ sürümünü çalıştıran istemciler için açıklanan davranışıdır.
- Java ve JMS istemcileri MQCSP kipinde çalışıyorsa, **PasswordProtection** özniteliğinin davranışı anlatıldığı gibi davranışıdır.

Java ve JMS istemcileriyle bağlantı kimlik doğrulamasıyla ilgili daha fazla bilgi için bkz. “Java istemcisi ile bağlantı kimlik doğrulaması” sayfa 74.

Dijital Certificate Manager (DCM)

Use the DCM to manage digital certificates and private keys on IBM i.

Digital Certificate Manager (DCM), dijital sertifikaları yönetmenize ve bunları IBM i sunucusunda güvenli uygulamalarda kullanabilmenizi sağlar. Digital Certificate Manager(Sayısal Sertifika Yöneticisi) ile, Sertifika Yetkilileri (CA ' lar) ya da diğer üçüncü kişiler tarafından sayısal sertifikalar isteyebilir ve işleyebilirsiniz. Kullanıcılarınız için sayısal sertifika yaratmak ve yönetmek için yerel bir Sertifika Yetkilisi işlevi de yapabilirsiniz.

DCM, daha güçlü bir sertifika ve uygulama geçerlilik denetimi süreci sağlamak için Sertifika İptal Listelerinin (CRL ' ler) kullanılmasını da destekler. Belirli bir Sertifika Yetkilisi CRL 'nin bulunduğu konumu bir LDAP sunucusunda tanımlamak için DCM' yi kullanabilirsiniz; böylece, IBM MQ belirli bir sertifikanın iptal edilmediğini doğrulayabilir.

DCM, sertifikaları çeşitli biçimlerde otomatik olarak algılayabilir ve bu biçimlerde otomatik olarak algılayabilir. DCM, PKCSencodedile kodlanmış bir sertifika ya da şifrelenmiş verileri içeren bir PKCS #7 sertifikası algıladığında, otomatik olarak kullanıcıdan sertifikayı şifrelemek için kullanılan parolayı girmesini ister. DCM, şifrelenmiş veriler içermeyen PKCS #7 sertifikaları için bilgi isteminde bulunmaz.

DCM, uygulamalarınız ve kullanıcılarınız için dijital sertifikaları yönetmek üzere kullanabileceğiniz, tarayıcı tabanlı bir kullanıcı arabirimi sağlar. Kullanıcı arabirimi iki ana çerçeveye ayrılır: bir gezinme çerçevesi ve bir görev çerçevesi.

Belgeleri ya da bunları kullanan uygulamaları yönetmek için kullanılacak görevleri seçmek için gezinme çerçevesini kullanabilirsiniz. Bazı bireysel görevler ana gezinme çerçevesinde doğrudan gösterilir, ancak gezinme çerçevesindeki çoğu görev kategorilere göre düzenlenir. Örneğin, Sertifikaları Yönet, Sertifikalar, Renew sertifikası ve Import certificate gibi çeşitli tek kılavuzlu görevleri içeren bir görev kategorisidir.

Gezinme çerçevesindeki bir öğe birden çok görev içeren bir kategoriyse, sayfanın solunda bir ok görüntülenir. Ok, kategori bağlantısını seçtiğinizde, gerçekleştirilecek bir görev listesi görüntülenir ve hangi görevin gerçekleştirileceğini seçmenize olanak tanır.

DCM ile ilgili önemli bilgiler için aşağıdaki IBM Redbooks yayınlarına bakın:

- *IBM i Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements*, SG24-6168. IBM i sisteminizin yerel bir CA olarak ayarlanmasıyla ilgili temel bilgiler için ek bilgi için ek bilgi için ek bilgi (appendixes) bakın.
- *AS/400 Internet Security: Dijital Sertifika Altyapısı Geliştiriyor*, SG24-5659. Özellikle, Bölüm 5 'e bakın. *Digital Certificate Manager for AS/400* , which explains the AS/400 DCM.

Federal Bilgi İşleme Standartları (FIPS)

Bu konuda, US National Institute of Standards and Technology 'nin Federal Bilgi İşleme Standartları (FIPS) Cryptomol Validation Programı ve TLS kanallarında kullanılabilecek şifreleme işlevleri ele alınmıştır.

Bu bilgiler aşağıdaki altyapılar için geçerlidir:

- ULW UNIX, Linux, and Windows
- z/OS z/OS

ULW UNIX, Linux, and Windowsüzerinde bir IBM MQ TLS bağlantısının FIPS 140-2 uyumluluğunu hakkında daha fazla bilgi için bkz. “UNIX, Linux, and Windows için Federal Bilgi İşleme Standartları (FIPS)” sayfa 32.

z/OS z/OSüzerinde bir IBM MQ TLS bağlantısının FIPS 140-2 uyumluluğunu hakkında daha fazla bilgi için bkz. “Federal Information Processing Standards (FIPS) for z/OS” sayfa 34.

Şifreleme donanımı mevcutsa, IBM MQ tarafından kullanılan şifreleme modülleri, donanım üreticisi tarafından sağlananlar için yapılandırılabilir. Bu işlem yapılırsa, bu yapılandırma yalnızca, bu şifreleme modülleri FIPS sertifikalıysa, FIPS uyumludur.

Zaman içinde, Federal Bilgi İşleme Standartları, şifreleme algoritmalarına ve protokollere karşı yeni saldırıları yansıtacak şekilde güncellenir. Örneğin, bazı CipherSpecs , FIPS sertifikasına son verebilir. Bu tür değişiklikler gerçekleştiğinde, IBM MQ en son standardı uygulamak için de güncellenir. Sonuç olarak, bakım uyguladıktan sonra davranışlardaki değişiklikleri görebilirsiniz.

İlgili kavramlar

“MQI istemcisinde çalıştırma zamanında yalnızca FIPS onaylı CipherSpecs kullanılmasının belirtilmesi” sayfa 258
FIPS uyumlu yazılımı kullanarak anahtar havuzlarınızı oluşturun ve daha sonra, kanalın FIPS onaylı CipherSpecsözelliğini kullanması gerektiğini belirtin.

“Dijital sertifikaları yönetmek için runmqckm, runmqakmve strmqikm ' nin kullanılması” sayfa 273
On UNIX, Linux, and Windows systems, manage keys and digital certificates with the **strmqikm** (iKeyman) GUI, or from the command line using **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd).

İlgili görevler

Enabling TLS in IBM MQ classes for Java

Using Transport Layer Security (TLS) with IBM MQ classes for JMS

İlgili başvurular

TLS properties of JMS objects

“Federal Bilgi İşleme Standartları” sayfa 19
ABD hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği hakkında teknik danışmanlık yapıyor. National Institute for Standards and Technology (NIST), BT sistemleri ve güvenliği ile ilgili önemli bir organa sahip. NIST, Federal Bilgi İşleme Standartları (FIPS) de dahil olmak üzere öneriler ve standartlar üretir.

ULW *UNIX, Linux, and Windows için Federal Bilgi İşleme Standartları (FIPS)*

Windows, UNIX and Linux sistemlerinde bir SSL/TLS kanalında şifreleme gerektiğinde IBM MQ , IBM Crypto for C (ICC) adlı bir şifreleme paketi kullanır. Windows, UNIX and Linux platformlarında, ICC yazılımı, ABD Ulusal Standartlar ve Teknoloji Enstitüsü 'nün Federal Bilgi İşleme Standartları (FIPS) Şifreleme Modülü Doğrulama Programı 'nı 140-2 düzeyinde geçmiştir.

Windows, UNIX and Linux sistemlerinde IBM MQ TLS bağlantısının FIPS 140-2 uyumluluğu aşağıdaki gibidir:

- Aşağıdaki koşullar karşılandıysa, tüm IBM MQ ileti kanalları (CLNTCONN kanal tipleri dışında) için bağlantı FIPS uyumludur:
  - Kurulu GSKit ICC sürümü, kurulu işletim sistemi sürümü ve donanım mimarisinde FIPS 140-2 uyumlu olarak onaylanmıştır.
  - Kuyruk yöneticisinin SSLFIPS özniteliği YES olarak ayarlandı.
  - Tüm anahtar havuzları, `-fips` seçeneğiyle **runmqakm** gibi yalnızca FIPS uyumlu yazılımlar kullanılarak oluşturulmuştur ve işlenmiştir.
- Tüm IBM MQ MQI client uygulamaları için bağlantı GSKit kullanır ve aşağıdaki koşullar karşılandığında FIPS uyumludur:
  - Kurulu GSKit ICC sürümü, kurulu işletim sistemi sürümü ve donanım mimarisinde FIPS 140-2 uyumlu olarak onaylanmıştır.
  - MQI istemcisine ilişkin ilgili konuda açıklandığı gibi, yalnızca FIPS sertifikalı şifrelemenin kullanılacağını belirttiniz.
  - Tüm anahtar havuzları, `-fips` seçeneğiyle **runmqakm** gibi yalnızca FIPS uyumlu yazılımlar kullanılarak oluşturulmuştur ve işlenmiştir.
- İstemci kipini kullanan IBM MQ classes for Java uygulamaları için bağlantı, JRE ' nin TLS uygulamalarını kullanır ve aşağıdaki koşullar karşılandığında FIPS uyumludur:
  - Uygulamayı çalıştırmak için kullanılan Java Runtime Environment, kurulu işletim sistemi sürümü ve donanım mimarisinde FIPS uyumludur.
  - Java istemcisi için ilgili konuda açıklandığı gibi, yalnızca FIPS sertifikalı şifrelemenin kullanılacağını belirttiniz.
  - Tüm anahtar havuzları, `-fips` seçeneğiyle **runmqakm** gibi yalnızca FIPS uyumlu yazılımlar kullanılarak oluşturulmuştur ve işlenmiştir.
- İstemci kipini kullanan IBM MQ classes for JMS uygulamaları için bağlantı, JRE ' nin TLS uygulamalarını kullanır ve aşağıdaki koşullar karşılandığında FIPS uyumludur:
  - Uygulamayı çalıştırmak için kullanılan Java Runtime Environment, kurulu işletim sistemi sürümü ve donanım mimarisinde FIPS uyumludur.
  - JMS istemcisi için ilgili konuda açıklandığı gibi, yalnızca FIPS sertifikalı şifrelemenin kullanılacağını belirttiniz.
  - Tüm anahtar havuzları, `-fips` seçeneğiyle **runmqakm** gibi yalnızca FIPS uyumlu yazılımlar kullanılarak oluşturulmuştur ve işlenmiştir.
- Yönetilmeyen .NET istemci uygulamaları için bağlantı GSKit kullanır ve aşağıdaki koşullar karşılandığında FIPS uyumludur:
  - Kurulu GSKit ICC sürümü, kurulu işletim sistemi sürümü ve donanım mimarisinde FIPS 140-2 uyumlu olarak onaylanmıştır.
  - .NET istemcisi için ilgili konuda açıklandığı gibi, yalnızca FIPS sertifikalı şifrelemenin kullanılacağını belirttiniz.
  - Tüm anahtar havuzları, `-fips` seçeneğiyle **runmqakm** gibi yalnızca FIPS uyumlu yazılımlar kullanılarak oluşturulmuştur ve işlenmiştir.
- Yönetilmeyen XMS .NET istemci uygulamaları için bağlantı GSKit 'i kullanır ve aşağıdaki koşullar karşılandığında FIPS uyumludur:

- Kurulu GSKit ICC sürümü, kurulu işletim sistemi sürümü ve donanım mimarisinde FIPS 140-2 uyumlu olarak onaylanmıştır.
- XMS .NET belgelerinde açıklandığı gibi, yalnızca FIPS onaylı şifrelemenin kullanılacağını belirttiniz.
- Tüm anahtar havuzları, `-fips` seçeneğiyle **runmqakm** gibi yalnızca FIPS uyumlu yazılımlar kullanılarak oluşturulmuştur ve işlenmiştir.

Desteklenen tüm platformlar, her düzeltme paketinde ya da yenileme paketinde yer alan benioku dosyasında belirtilenler dışında, FIPS 140-2 sertifikalıdır.

GSKit kullanan TLS bağlantıları için, FIPS 140-2 sertifikalı bileşen *ICC*olarak adlandırılır. Belirli bir platformda GSKit FIPS uyumluluğunu belirleyen bu bileşenin sürümüdür. Kurulu olan ICC sürümünü belirlemek için **dspmqver -p 64 -v** komutunu çalıştırın.

Aşağıda, ICC ile ilgili **dspmqver -p 64 -v** çıktısının bir örneği verilmiştir:

```
icc
============
@ (#)CompanyName: IBM Corporation
@(#)LegalTrademarks: IBM
@ (#)FileDescription: IBM Crypto
@(#)FileVersion:   8.0.0.0
@ (#)LegalCopyright: Lisanslı Malzeme- IBM
@ (#) ICC
@ (#) (C) Copyright IBM Corp. 2002, 2024.
@ (#) Her Hakkı Saklıdır. ABD Hükümeti Kullanıcıları
@ (#) Sınırlı Haklar-Kullanım, çoğaltma ya da açıklama
@ (#), IBM Corp. ile yapılan GSA ADP Schedule Contract adlı sözleşmeyle sınırlanmıştır.
@ (#)ProductName: icc_8.0 (GoldCoast Build) 100415
@(#)ProductVersion:  8.0.0.0
@(#)ProductInfo:   10/04/15.03:32:19.10/04/15.18:41:51
@ (#) CMVCInfo:
```

GSKit ICC 8 (GSKit 8 'e dahil) için NIST sertifikasyon bildirimi şu adreste bulunabilir: Cryptographic Module Validation Program.

Şifreleme donanımı varsa, IBM MQ tarafından kullanılan şifreleme modülleri donanım üreticisi tarafından sağlanacak şekilde yapılandırılabilir. Bu yapıldıysa, yapılandırma yalnızca bu şifreleme modüllerinin FIPS onaylı olması durumunda FIPS uyumludur.

Not: Intel sistemlerinde çalışırken, FIPS 140-2 uyumlu işlem için yapılandırılan 32 bit Solaris x86 SSL ve TLS istemcileri başarısız olur. Bu hata, FIPS 140-2 uyumlu GSKit-Crypto Solaris x86 32 bit kitaplık dosyası Intel yonga setine yüklenmediğinden ortaya çıkar. Etkilenen sistemlerde, istemci hata günlüğünde AMQ9655 hatası bildirildi. Bu sorunu çözmek için, 64 bitlik kod etkilenmediğinden, FIPS 140-2 uyumluluğunu geçersiz kılın ya da istemci uygulamasını 64 bitlik olarak yeniden derleyin.

FIPS 140-2 ile uyumlu olarak çalışırken uygulanan üçlü DES kısıtlamaları

IBM MQ , FIPS 140-2 ile uyumlu çalışacak şekilde yapılandırıldığında, Triple DES (3DES) CipherSpecsile ilgili olarak ek kısıtlamalar uygulanır. Bu kısıtlamalar, ABD NIST SP800-67 önerisiyle uyumluluğu sağlar.

1. Triple DES anahtarının tüm parçaları benzersiz olmalıdır.
2. NIST SP800-67içindeki tanımlara göre Üçlü DES anahtarının hiçbir parçası Zayıf, Yarı Zayıf ya da Zayıf olamaz.
3. Gizli bir anahtar sıfırlaması gerçekleşmeden önce bağlantı üzerinden en fazla 32 GB veri iletilebilir. Varsayılan olarak IBM MQ , gizli oturum anahtarını sıfırlamaz, bu nedenle bu sıfırlama yapılandırılmalıdır. Üçlü DES CipherSpec ve FIPS 140-2 uyumluluğu kullanılırken gizli anahtar sıfırlama etkinleştirilmemesi, bayt sayısı üst sınırı aşıldıktan sonra AMQ9288 hatasıyla bağlantının kapanmasına neden olur. Gizli anahtar sıfırlamasını yapılandırma hakkında bilgi için bkz. “SSL ve TLS gizli anahtarlarını sıfırlama” sayfa 428.

IBM MQ , 1 ve 2 numaralı kurallara zaten uyan Üçlü DES oturum anahtarları oluşturur. Ancak, üçüncü kısıtlamayı karşılamak için FIPS 140-2 yapılandırmasında Üçlü DES CipherSpecs kullanırken gizli anahtar sıfırlamasını etkinleştirmeniz gerekir. Alternatif olarak, Üçlü DES kullanmaktan kaçınabilirsiniz.

İlgili kavramlar

"MQI istemcisinde çalıştırma zamanında yalnızca FIPS onaylı CipherSpecs kullanılmasının belirtilmesi" sayfa 258
FIPS uyumlu yazılımı kullanarak anahtar havuzlarınızı oluşturun ve daha sonra, kanalın FIPS onaylı CipherSpecsözelliğini kullanması gerektiğini belirtin.

"Dijital sertifikaları yönetmek için runmqckm, runmqakmve strmqikm ' nin kullanılması" sayfa 273
On UNIX, Linux, and Windows systems, manage keys and digital certificates with the **strmqikm** (iKeyman) GUI, or from the command line using **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd).

İlgili görevler

IBM MQ classes for Java içinde TLS ' yi etkinleştirme

IBM MQ classes for JMS ile TLS (Transport Layer Security; İletim Katmanı Güvenliği) kullanılması

İlgili başvurular

JMS nesnelerinin TLS özellikleri

"Federal Bilgi İşleme Standartları" sayfa 19
ABD hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği hakkında teknik danışmanlık yapıyor. National Institute for Standards and Technology (NIST), BT sistemleri ve güvenliği ile ilgili önemli bir organa sahip. NIST, Federal Bilgi İşleme Standartları (FIPS) de dahil olmak üzere öneriler ve standartlar üretir.

z/OS *Federal Information Processing Standards (FIPS) for z/OS*

z/OS üzerindeki bir SSL/TLS kanalında şifreleme gerektiğinde, IBM MQ , Sistem SSL adı verilen bir hizmeti kullanır. Sistem SSL ' nin amacı, ABD Ulusal Standartlar ve Teknoloji Enstitülerinin Federal Bilgi İşleme Standartları (FIPS) Cryptomodül Validation Programı 'na bağlı olarak 140-2 düzeyinde güvenli bir şekilde yürütme yeteneği sağlamaktır.

When implementing FIPS 140-2 compliant connections with IBM MQ TLS connections there are a number of points to consider:

- IBM MQ ileti kanallarının FIPS uyumluluğu için geçerli kılınmasını sağlamak için aşağıdaki koşulların karşılandığından emin olun:
  - Sistem SSL Güvenlik Düzeyi 3 FMID kurulu ve yapılandırılmış (bkz. IBM MQ ' u kurmayı planlama).
  - Sistem SSL modüllerinin geçerliliği denetlendi.
  - Kuyruk yöneticisinin SSLFIPS özniteliği **YES**olarak ayarlandı.

FIPS kipinde yürütülürken, kullanılabilir olduğunda Sistem SSL, Şifreleme İşlevi için CP Desteği (CPACF) kullanır. FIPS kipinde çalışırken, ICSF destekli donanım tarafından gerçekleştirilen şifreleme işlevleri, yazılım içinde gerçekleştirilmesi gereken RSA imza oluşturma dışında, FIPS kipinde yürütüldüğünde sömürülmeye devam eder.

Çizelge 2. FIPS kipi ile FIPS dışı kip algoritması desteği arasındaki farklar.

	FIPS dışı		**FIPS**	
Algoritma	**Anahtar büyüklükleri**	**donanım**	**Anahtar büyüklükleri**	**donanım**
RC2	40 ve 128			
RC4	40 ve 128			
DES	56	x		
TDES	168	x	168	x
AES	128 ve 256	x	128 ve 256	x
MD5	48			
SHA-1	160	x	160	x

Çizelge 2. FIPS kipi ile FIPS dışı kip algoritması desteği arasındaki farklar. (devamı var)				
	FIPS dışı		**FIPS**	
Algoritma	**Anahtar büyüklükleri**	**donanım**	**Anahtar büyüklükleri**	**donanım**
SHA-2	224, 256, 384 ve 512	x	224, 256, 384 ve 512	x
RSA	512-4096	x	1024-4096	x
DSA	512-1024		1024	
DH	512-2048		2048	

Sistem SSL, FIPS kipinde yalnızca Tablo 1 'de gösterilen algoritmaları ve anahtar boyutlarını kullanan sertifikaları kullanabilir. FIPS kipiyle uyumsuz bir algoritma saptandığında X.509 sertifikası geçerlilik denetimi sırasında sertifika kullanılamaz ve geçersiz olarak işlem görür.

WebSphere Application Server içindeki istemci kipini kullanan IBM MQ sınıf uygulamaları için Federal Information Processing Standard supportbaşlıklı konuya bakın.

Sistem SSL modülü yapılandırması hakkında bilgi için bkz. System SSL Module Verification Setup.

İlgili başvurular

“Federal Bilgi İşleme Standartları” sayfa 19
ABD hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği hakkında teknik danışmanlık yapıyor. National Institute for Standards and Technology (NIST), BT sistemleri ve güvenliği ile ilgili önemli bir organa sahip. NIST, Federal Bilgi İşleme Standartları (FIPS) de dahil olmak üzere öneriler ve standartlar üretir.

Multi *mqcertck ile kuyruk yöneticinizin TLS yapılandırmasını doğrulama*

MQCERTCK komutu, kuyruk yöneticinizin TLS yapılandırmasında sık kullanılan hataları aramak için kullanılan bir araçtır ve sorunların çözümüne ilişkin bazı öneriler sağlar.

Giriş

mqcertck komutu aşağıdakileri denetler:

- Kuyruk yöneticisi **SSLKEYR** özniteliğinde gönderme yapılan kuyruk yöneticisinin anahtar havuzunun varlığı ve izinleri.
- Kuyruk yöneticisi **CERTLABL** özniteliğinde başvurulan kuyruk yöneticisi sertifikasına ilişkin sertifikanın varlığı ve geçerliliği.
- TLS etkin kanalın **CERTLABL** özniteliklerinde başvurulan sertifikaların varlığı ve geçerliliği.
- Sertifikaların denetlenmesi de içinde olmak üzere, istemci uygulamalarının anahtar havuzu ve sertifikalarının kuyruk yöneticisiyle yetkisi vardır.

Not: mqcertck komutu z/OS ya da IBM iüzerinde kullanılamaz.

Kullanım

mqcertck komutunu kullanmak için `mqcertck`komutunu, gerekli parametreleriyle birlikte ve bir komut satırından gerekli olan isteğe bağlı parametrelerle birlikte çalıştırın.

Komutun ve komutun aldığı değiştirgelerin açıklaması için mqcertck kısmına bakın.

Örnek

Kuyruk yöneticinizin SVRCONN kanalına bağlanan istemcilerden TLS bağlantılarına izin vermek için `QM1` kuyruk yöneticinizi ayarlamayı yeni bitirdiniz.

Birden çok sertifika özelliğini kullanıyorsunuz ve hem kuyruk yöneticinizin hem de kanalınızın **CERTLABL** özniteliklerinde belirtilmiş bir sertifika etiketi var. Kanalı yaratırken, kanalın **CERTLABL** özniteliğinde bir hata yaptınız; bu nedenle, bir istemci bağlanma girişiminde bulunduğunda kuyruk yöneticisi 2393 dönüş kodunu MQRC_SSL_INITIALIZATION_ERROR dönüş kodunu döndürür.

Kuyruk yöneticisini etkinleştirmeden önce, kuyruk yöneticisinin TLS yapılandırmasını doğrulamak için **mqcertck** komutunu kullanın.

`mqcertck QM1` komutunu çalıştırıp aşağıdaki çıkışı alırsınız:

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

Bu çıkış, MQCERTCK.CHANNEL. Burada, yaptığınız hatayı görürsünüz ve sorunu çözümlediğinizi doğrulamak için `mqcertck` komutunu yeniden çalıştırmadan önce hatayı düzeltebilirsiniz.

İstemci bağlantılarının doğrulanması

mqcertck komutu, kuyruk yöneticisinin TLS yapılandırmasının yanı sıra istemci anahtar havuzlarını doğrulama yeteneğine sahiptir. Bunu yapmak için, **mqcertck** ' in kuyruk yöneticisini çalıştıran makineden istemcinin anahtar havuzuna erişebilmesi gerekir.

mqcertck komutunu çalıştırırken, **-clientkeyr** değiştirgesini istemci anahtar havuzunun yeriyle birlikte sağlarsanız (uzantı dışında) **mqcertck** , bu anahtar havuzunu kuyruk yöneticisiyle karşılaştırılarak denetler.

İstemcinin kuyruk yöneticisine bağlanmak için kullanacağı kanalı biliyorsanız, bunu **-clientchannel** işaretiyle belirtebilirsiniz.

İstemci kuyruk yöneticisine bağlanmak için karşılıklı kimlik doğrulaması kullanıyorsa, istemci anahtar havuzunda hangi sertifikanın kullanılacağını **mqcertck** komutuna söylemek için **-clientusername** ya da **-clientlabel** parametresini kullanabilirsiniz.

Varsayılan sertifikayı kullanıyorsanız ve istemci uygulamasına sertifika etiketi sağlamıyorsanız, bu uygulamayı çalıştıran **-clientusername** ve **username** değiştirgelerini kullanabilirsiniz.

mqcertck komutunun çalışması sırasında komut, `ibmwebspheremqXXXX` sertifika etiketini oluşturur; burada XXXX , **-clientusername** değiştirgesinde geçirilen değerdir.

İstemci anahtar havuzunu tam olarak doğrulamak için, **mqcertck** komutu GSKit kullanarak kukla bir bağlantı yaratır. Bunu yapmak için, komutun istemci sınamaları sırasında bağlanabileceği bir kapısı olması gerekir. Kullanılan varsayılan kapı şudur: 5857; ancak, bu zaten kullanılıyorsa, istemci sınamaları sırasında kullanılacak farklı bir kapı belirtebilirsiniz.

Not: **mqcertck** komutu bir kapıya bağlansa da, **mqcertck**tarafından dış iletişim kullanılmaz ve tüm sınamalar yerel olarak gerçekleştirilir.

IBM MQ MQI clientüzerinde SSL/TLS

IBM MQ , istemcilerde TLS ' yi destekler. TLS kullanımını çeşitli şekillerde uyarlayabilirsiniz.

IBM MQ , Windowsüzerinde IBM MQ MQI clients , UNIX and Linux sistemleri için TLS desteği sağlar. If you are using IBM MQ classes for Java, see IBM MQ classes for Javakomutunu kullanma and if you are using IBM MQ classes for JMS, see IBM MQ classes for JMSkomutunu kullanma. Bu bölümün geri kalan kısmı Java ya da JMS ortamları için geçerli değildir.

IBM MQ istemci yapılandırma dosyanızın MQSSLKEYR değeriyle ya da uygulamanızın bir MQCONNX çağrısı yaptığı durumlarda, bir IBM MQ MQI client için anahtar havuzunu belirtebilirsiniz. Bir kanalın TLS ' yi kullanmasını belirtmek için üç seçeneğiniz vardır:

- Kanal tanımlama çizelgesinin kullanılması
- MQCONNX çağrısında SSL yapılandırma seçenekleri yapısının kullanılması, MQSCO
- Active Directory olanağının kullanılması (Windows sistemlerinde)

Bir kanala TLS kullanacağını belirtmek için MQSERVER ortam değişkenini kullanamazsınız.

Aktarım kanalının diğer ucunda TLS belirtilmediği sürece, var olan IBM MQ MQI client uygulamalarınızı TLS olmadan çalıştırmaya devam edebilirsiniz.

Bir istemci makinesinde, TLS Anahtarı Havuzu, TLS Anahtarı Havuzu, Kimlik Doğrulama Bilgileri ya da Şifreleme donanımı parametrelerinin içeriği üzerinde değişiklik yapılırsa, uygulamanın kuyruk yöneticisine bağlanmak için kullandığı istemci-bağlantı kanallarında bu değişiklikleri yansıtmak için tüm TLS bağlantılarını sonalmanız gerekir. Tüm bağlantılar sona erdikten sonra TLS kanallarını yeniden başlatın. Tüm yeni TLS ayarları kullanılır. Bu ayarlar, kuyruk yöneticisi sistemlerinde REFRESH SECURITY TYPE (SSL) komutuna göre yenilenenlere benzer.

When your IBM MQ MQI client runs on a Windows, UNIX and Linux system with cryptographic hardware, you configure that hardware with the MQSSLCRYP environment variable. Bu değişken, ALTER QMGR MQSC komutundaki SSLCRYP parametresine eşdeğerdir. ALTER QMGR MQSC komutundaki SSLCRYP parametresine ilişkin açıklamalar için ALTER QMGR belgesine bakın. SSLCRYP parametresinin GSK_PCS11 sürümünü kullanıyorsanız, PKCS #11 belirteci etiketi tamamen küçük harfle belirtilmelidir.

TLS gizli anahtarı ilk duruma getirme ve FIPS 'ler IBM MQ MQI clients' ta desteklenir. Daha fazla bilgi için bkz. “SSL ve TLS gizli anahtarlarını sıfırlama” sayfa 428 ve “UNIX, Linux, and Windows için Federal Bilgi İşleme Standartları (FIPS)” sayfa 32.

See “IBM MQ MQI client güvenliğini ayarlama” sayfa 257 for more information about the TLS support for IBM MQ MQI clients.

İlgili görevler

Yapılandırma dosyası kullanarak istemci yapılandırılması

Bir MQI kanalının SSL/TLS kullandığını belirtme

Bir MQI kanalının TLS 'yi kullanması için, istemci bağlantı kanalının *SSLCipherSpec* özniteliğinin değeri, istemci altyapısında IBM MQ tarafından desteklenen bir CipherSpec ' in adı olmalıdır.

Bu öznitelik için bir değer içeren bir istemci-bağlantı kanalı tanımlayabilirsiniz. Bunlar, azalan öncelik sırasına göre listelenir.

1. Bir PreConnect çıkışı, kullanılacak bir kanal tanımlama yapısı sağladığında.

   Bir PreConnect çıkışı, bir kanal tanımlama yapısının *SSLCipherSpec* alanında, MQCD ' de CipherSpec adını sağlayabilir. Bu yapı, PreConnect çıkığı tarafından kullanılan MQNXP çıkış parametresi yapısının **ppMQCDArrayPtr** alanında döndürülür.
2. Bir IBM MQ MQI client uygulaması bir MQCONNX çağrısı yayınladığında.

Uygulama, bir kanal tanımlama yapısının, MQCD ' nin *SSLCipherSpec* alanındaki bir CipherSpec adını belirtebilir.Bu yapıya, MQCONNX çağrısında bir parametre olan bağlantı seçenekleri yapısı, MQCNO tarafından başvurulmaktadır.

3. İstemci kanal tanımlama çizelgesi (CCDT) kullanılıyor.

   Bir istemci kanalı tanımlama çizelgesindeki girişlerden biri ya da daha fazlası, bir CipherSpecadının adını belirtebilir.Örneğin, DEFINE CHANNEL MQSC komutunu kullanarak bir girdi oluştururursanız, komutta bir CipherSpecadını belirtmek için SSLCIPH parametresini kullanabilirsiniz.

4. Windowsüzerinde Active Directory seçeneğini kullanma.

   On Windows systems, you can use the **setmqscp** control command to publish the client-connection channel definitions in Active Directory. Bu tanımlardan biri ya da daha fazlası, bir CipherSpecadını belirtebilir.

For example, if a client application provides a client-connection channel definition in an MQCD structure on an MQCONNX call, this definition is used in preference to any entries in a client channel definition table that can be accessed by the IBM MQ client.

TLS kullanan bir MQI kanalının istemci ucunda kanal tanımlaması sağlamak için MQSERVER ortam değişkenini kullanamazsınız.

Bir istemci sertifikasının akıp taşmadığını denetlemek için, bir eşdüzey ad parametresi değerinin varlığına ilişkin bir kanalın sunucu ucunda kanal durumunu görüntüleyin.

İlgili kavramlar

“IBM MQ MQI clientiçin bir CipherSpec belirtme” sayfa 417
IBM MQ MQI clientiçin bir CipherSpec belirtmek için üç seçeneğiniz vardır.

IBM MQiçindeCipherSpecs ve CipherSuites

IBM MQ , TLS 1.2 CipherSpecs, RSA ve Diffie-Hellman algoritmalarını destekler. Ancak, bu işlemi yapmanız gerekiyorsa, kullanımdan kaldırılmış CipherSpecs' ı etkinleştirebilirsiniz.

Aşağıdakiyle ilgili bilgi için bkz. “CipherSpecs' in etkinleştirilmesi” sayfa 402 :

- IBM MQtarafından desteklenenCipherSpecs .
- Kullanımdan kaldırılan SSL 3.0 ve TLS 1.0 CipherSpecs' ı nasıl etkinleştirdiğiniz.

IBM MQ , RSA ve Diffie-Hellman anahtar değişimi ve kimlik doğrulama algoritmalarını destekler. TLS anlaşması sırasında kullanılan anahtarın boyutu, kullandığınız dijital sertifikaya bağlı olabilir, ancak bazı CipherSpecs , el sıkışma anahtarı boyutuna ilişkin bir belirtim içerir. Daha büyük el sıkışma anahtarı boyutları daha güçlü kimlik doğrulaması sağlar Daha küçük anahtar boyutlarıyla, el sıkışma daha hızlı olur.

İlgili kavramlar

“CipherSpecs ve CipherSuites” sayfa 18
Şifreleme güvenlik protokolleri, güvenli bir bağlantı tarafından kullanılan algoritmalar üzerinde kabul etmelidir. CipherSpecs ve CipherSuites , algoritmaların belirli bileşimlerini tanımlar.

NSA Suite B Cryptografi (IBM MQ)

This topic provides information about how to configure IBM MQ on Windows, Linux, and UNIX to conform to the Suite B compliant TLS 1.2 profile.

Zaman içinde NSA Cryptography Suite B Standard, şifreleme algoritmalarına ve protokollere yönelik yeni saldırıları yansıtacak şekilde güncellenmektedir. Örneğin, bazı CipherSpecs , Suite B sertifikalı olmayı durdurabilir. Bu tür değişiklikler gerçekleştiğinde, IBM MQ en son standardı uygulamak için de güncellenir. Sonuç olarak, bakım uyguladıktan sonra davranışlardaki değişiklikleri görebilirsiniz. IBM MQ benioku dosyası, her bir ürün bakım düzeyi tarafından uygulanan Suite B ' nin sürümünü listeler. If you configure IBM MQ to enforce Suite B compliance, always consult the readme file when planning to apply maintenance. Bkz. IBM MQ, WebSphere MQ, ve MQSeries ürün readmes.

Windows, UNIXve Linux sistemlerinde IBM MQ , Tablo 1 'de gösterilen güvenlik düzeylerindeki Suite B uyumlu TLS 1.2 profiline uyacak şekilde yapılandırılabilir.

Çizelge 3. İzin verilen CipherSpecs ve dijital imza algoritmalarına sahip takım B güvenlik düzeyleri		
Güvenlik Düzeyi	**İzin verilen CipherSpecs**	**İzin verilen dijital imza algoritmaları**
128 bit	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA with SHA-256 ECDSA with SHA-384
192 bit	ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA with SHA-384
Her ikisi de [1]	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA with SHA-256 ECDSA with SHA-384

1. Hem 128 bitlik, hem de 192 bit güvenlik düzeylerinin konfigürasyonlarını eşzamanlı olarak tanımlamak mümkündür. Takım B yapılandırması, kabul edilebilir minimum şifreleme algoritmalarını belirlediğinden, hem güvenlik düzeylerinin yapılandırılması, hem de 128 bit güvenlik düzeyinin yapılandırılmasına eşdeğerdir. 192 bit güvenlik düzeyinin şifreleme algoritmaları, 128 bit güvenlik düzeyi için gerekli olan alt sınırdan daha güçlü olduğundan, 192 bit güvenlik düzeyi etkinleştirilmemiş olsa da 128 bitlik güvenlik düzeyi için izin verilir.

Not: Güvenlik düzeyi için kullanılan adlandırma kuralları, her zaman eliptik eğri büyüklüğünü ya da AES şifreleme algoritmasının anahtar büyüklüğünü göstermiyor.

Takım B ' yeCipherSpec kondisyon

IBM MQ ' in varsayılan davranışı Suite B standardına uymamasına rağmen, IBM MQ , Windows, UNIX and Linux sistemlerinde her iki güvenlik düzeyine ya da her iki güvenlik düzeyine uyumlu olacak şekilde yapılandırılabilir. Following the successful configuration of IBM MQ to use Suite B, any attempt to start an outbound channel using a CipherSpec not conforming to Suite B results in the error AMQ9282. Bu etkinlik ayrıca, MQI istemcisinin MQRC_CIPHER_SPEC_NOT_SUITE_Bneden kodunu döndürmesine neden olur. Benzer şekilde, B Suite yapılandırma sonuçlarıyla uyumlu olmayan bir CipherSpec kullanarak bir gelen kanalı başlatmaya çalışmak AMQ9616hatasındaki sonuçlarla sonuçlanır.

IBM MQ CipherSpecshakkında daha fazla bilgi için bkz. “CipherSpecs' in etkinleştirilmesi” sayfa 402

B grubu ve dijital sertifikalar

Suite B, dijital sertifikaları imzalamak için kullanılabilecek dijital imza algoritmalarını kısıtlar. B Grubu, sertifikaların içerebileceği genel anahtar tipini de kısıtlar. Bu nedenle IBM MQ , dijital imza algoritması ve genel anahtar tipine, uzak ortağın yapılandırılan Suite B güvenlik düzeyi tarafından izin verilen sertifikaları kullanacak şekilde yapılandırılmalıdır. Digital certificates which do not comply with the security level requirements are rejected and the connection fails with error AMQ9633 or AMQ9285.

128 bitlik Suite B güvenlik düzeyi için, sertifika konularının genel anahtarı NIST P-256 eliptik eğrisi ya da NIST P-384 eliptik eğrisi ya da NIST P-256 eliptik eğrisi ya da NIST P-384 eliptik eğrisi ile imzalanacak şekilde gereklidir. 192-bit Suite B güvenlik düzeyinde, sertifika konularının genel anahtarı NIST P-384 eliptik eğrisini kullanmak ve NIST P-384 eliptik eğrisi ile imzalanmalıdır.

Suite B uyumlu çalışmaya uygun bir sertifika almak için, **runmqakm** komutunu kullanın ve uygun bir dijital imza algoritması istemek için **-sig_alg** parametresini belirtin. EC_ecdsa_with_SHA256 ve EC_ecdsa_with_SHA384 **-sig_alg** parametre değerleri, izin verilen Suite B dijital imza algoritmaları tarafından imzalanmış eliptik eğri anahtarlarına karşılık gelir.

runmqakm komutuna ilişkin daha fazla bilgi için bkz. runmqckm ve runmqakm seçenekleri.

Not: runmqckm ve **strmqikm** komutları, Suite B uyumlu işlem için dijital sertifikaların oluşturulmasını desteklemez.

Dijital sertifikalar yaratılması ve istenmesi

Suite B testi için kendinden onaylı bir dijital sertifika oluşturmak üzere bkz. “UNIX, Linux, and Windows üzerinde kendinden onaylı kişisel sertifika oluşturma” sayfa 281

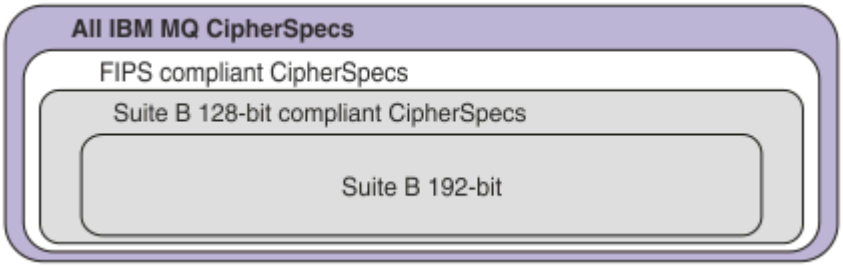
Takım B üretim kullanımı için CA tarafından imzalanmış bir dijital sertifika istemek üzere bkz. “UNIX, Linux, and Windows üzerinde kişisel sertifika isteme” sayfa 284.

Not: Kullanılmakta olan sertifika yetkilisi, IETF RFC 6460 içinde açıklanan gereksinimleri karşılayan sayısal sertifikalar oluşturmalıdır.

FIPS 140-2 ve Suite B

Suite B standardı, güvenli bir güvenlik düzeyi sağlamak üzere etkinleştirilmiş şifreleme algoritmaları kümesini kısıtladığı için, kavramsal olarak FIPS 140-2 'ye benzerdir. The Suite B CipherSpecs currently supported can be used when IBM MQ is configured for FIPS 140-2 compliant operation. Bu nedenle, IBM MQ ' u hem FIPS hem de Suite B uyumluluğu için aynı anda yapılandırmak mümkündür; bu durumda her iki kısıtlama kümesi de geçerlidir.

Aşağıdaki çizge, bu alt kümeler arasındaki ilişkiyi göstermektedir:



Suite B uyumlu işlem için IBM MQ ' nin yapılandırılması

For information about how to configure IBM MQ on Windows, UNIX and Linux for Suite B compliant operation, see “IBM MQ ürününü Suite B için yapılandırma” sayfa 40.

IBM MQ , IBM i ve z/OS platformlarında Suite B uyumlu çalışmasını desteklemez. IBM MQ Java ve JMS istemcileri de Suite B uyumlu çalışmasını desteklemez.

İlgili kavramlar

“MQI istemcisinde çalıştırma zamanında yalnızca FIPS onaylı CipherSpecs kullanılmasının belirtilmesi” sayfa 258
FIPS uyumlu yazılımı kullanarak anahtar havuzlarınızı oluşturun ve daha sonra, kanalın FIPS onaylı CipherSpecsözelliğini kullanması gerektiğini belirtin.

IBM MQ ürününü Suite B için yapılandırma

IBM MQ , Windows, UNIX and Linux platformlarında NSA Suite B standardına uygun olarak çalışacak şekilde yapılandırılabilir.

Suite B, güvenli bir güvenlik düzeyi sağlamak için etkinleştirilmiş şifreleme algoritmaları kümesini sınırlar. IBM MQ , geliştirilmiş bir güvenlik düzeyi sağlamak için Suite B ile uyumlu çalışacak şekilde yapılandırılabilir. Suite B hakkında daha fazla bilgi için bkz. “Ulusal Güvenlik Ajansı (NSA) Suite B Cryptography” sayfa 19. Suite B yapılandırması ve TLS kanalları üzerindeki etkisi hakkında daha fazla bilgi için bkz. “NSA Suite B Cryptografi (IBM MQ)” sayfa 38.

Kuyruk yöneticisi

Bir kuyruk yöneticisinde, gerekli güvenlik düzeyinize uygun değerleri ayarlamak için **SUITEB** parametresiyle birlikte **ALTER QMGR** komutunu kullanın. Daha fazla bilgi için bkz. ALTER QMGR.

Kuyruk yöneticisini Suite B uyumlu işlem için yapılandırmak üzere **MQIA_SUITE_B_STRENGTH** parametresiyle birlikte PCF **MQCMD_CHANGE_Q_MGR** komutunu da kullanabilirsiniz.

Not: Bir kuyruk yöneticisinin Suite B ayarlarını değiştirirseniz, bu ayarların yürürlüğe girmesi için MQXR hizmetini yeniden başlatmanız gerekir.

MQI istemcisi

Varsayılan olarak, MQI istemcileri Suite B uyumluluğunu uygulamaz. Aşağıdaki seçeneklerden birini yürüterek MQI istemcisini Suite B uyumluluğu için etkinleştirebilirsiniz:

1. MQCONNX çağrısında MQSCO yapısında **EncryptionPolicySuiteB** alanını aşağıdaki değerlerden birine ya da daha fazlasına ayarlayarak:
   - MQ_SUITE_B_NONE
   - MQ_SUITE_B_128_BIT
   - MQ_SUITE_B_192_BIT

   MQ_SUITE_B_NONE ' nin başka bir değerle kullanılması geçersiz.
2. MQSUITEB ortam değişkenini aşağıdaki değerlerden birine ya da daha fazlasına ayarlayarak:
   - YOK
   - 128_BIT
   - 192_BIT

   Virgülle ayrılmış bir liste kullanarak birden çok değer belirtebilirsiniz. NONE değerinin başka bir değerle kullanılması geçersiz.
3. MQI istemcisi yapılanış kütüğünün SSL kıtasındaki **EncryptionPolicySuiteB** özniteliğini aşağıdaki değerlerden birine ya da daha fazlasına ayarlayarak:
   - YOK
   - 128_BIT
   - 192_BIT

   Virgülle ayrılmış bir liste kullanarak birden çok değer belirtebilirsiniz. NONE değerinin başka bir değerle kullanılması geçersizdir.

Not: MQI istemcisi ayarları öncelik sırasına göre listelenir. MQCONNX çağrısındaki MSCO yapısı, SSL kısmı içindeki özniteliği geçersiz kılan MQSUITEB ortam değişkenindeki ayarı geçersiz kılar.

MQSCO yapısının tüm ayrıntıları için bkz. MQSCO-SSL yapılandırma seçenekleri.

İstemci yapılandırma dosyasında Suite B kullanımı hakkında daha fazla bilgi için bkz. İstemci yapılandırma dosyasının SSL kısmı.

MQSUITEB ortam değişkeninin kullanımıyla ilgili daha fazla bilgi için Ortam değişkenleri açıklamalarıkonusuna bakın.

.NET

.NET yönetilmeyen istemciler için **MQC.ENCRYPTION_POLICY_SUITE_B** özelliği, gerekli Suite B güvenliğinin tipini gösterir.

IBM MQ classes for .NETiçinde Suite B kullanımı hakkında bilgi için bkz. MQEnvironment .NET sınıfı.

AMQP

Bir kuyruk yöneticisine ilişkin Suite B öznitelik ayarları, o kuyruk yöneticisindeki AMQP kanallarına uygulanır. Kuyruk yöneticisi Suite B ayarlarını değiştirirseniz, değişikliklerin yürürlüğe girmesi için AMQP hizmetini yeniden başlatmanız gerekir.

IBM MQiçindeki sertifika geçerlilik denetimi ilkeleri

Sertifika doğrulama ilkesi, sertifika zinciri geçerlilik denetiminin sektör güvenlik standartlarına ne kadar tam olarak uygun olduğunu belirler.

Sertifika geçerlilik denetimi ilkesi, altyapıya ve ortama bağlıdır:

- Tüm platformlardaki Java ve JMS uygulamaları için, sertifika geçerlilik denetimi ilkesi, Java yürütme ortamının JSSE bileşenine bağlıdır. Sertifika doğrulama ilkesi hakkında daha fazla bilgi için, JRE belgelerinize bakın.
- IBM i sistemleri için, sertifika doğrulama ilkesi, işletim sistemi tarafından sağlanan güvenli yuva kitaplığına bağlıdır. Sertifika doğrulama ilkesi hakkında daha fazla bilgi için işletim sistemine ilişkin belgelere bakın.
- z/OS sistemleri için, sertifika geçerlilik denetimi ilkesi, işletim sistemi tarafından sağlanan Sistem SSL bileşenine bağlıdır. Sertifika doğrulama ilkesi hakkında daha fazla bilgi için işletim sistemine ilişkin belgelere bakın.
- UNIX, Linux, and Windows sistemleri için, sertifika doğrulama ilkesi GSKit tarafından sağlanır ve yapılandırılabilir. İki farklı sertifika geçerlilik denetimi ilkesi desteklenir:
  - Yürürlükteki IETF sertifika geçerlilik denetimi standartlarına uygun olmayan eski sayısal sertifikalarla, geriye doğru uyumluluk ve birlikte çalışabilirlik için kullanılan eski bir sertifika geçerlilik denetimi ilkesi. Bu ilke Temel ilke olarak bilinir.
  - RFC 5280 standardını zorlayan, sıkı, standartlara uygun bir sertifika doğrulama ilkesi. Bu ilke, Standart ilke olarak bilinir.

For information about how to configure the certificate validation policy on UNIX, Linux, and Windows, see “IBM MQ içinde sertifika doğrulama ilkelerini yapılandırma” sayfa 42. Temel ve Standart sertifika doğrulama ilkeleri arasındaki farklar hakkında daha fazla bilgi için bakınız: Certificate validation and trust policy design on UNIX, Linux, and Windows.

IBM MQ içinde sertifika doğrulama ilkelerini yapılandırma

Uzak iş ortağı sistemlerinden alınan sayısal sertifikaları dört şekilde doğrulamak için hangi TLS sertifika doğrulama ilkesinin kullanılacağını belirtebilirsiniz.

Kuyruk yöneticisinde, sertifika geçerlilik denetimi ilkesi aşağıdaki şekillerde ayarlanabilir:

- *CERTVPOL*kuyruk yöneticisi özniteliği kullanılıyor. Bu özniteliğin ayarlanmasıyla ilgili ek bilgi için ALTER QMGRbaşlıklı konuya bakın.

İstemcide, sertifika geçerlilik denetimi ilkesini ayarlamak için kullanılabilecek birkaç yöntem vardır. İlkeyi ayarlamak için birden çok yöntem kullanılırsa, istemci ayarları aşağıdaki öncelik sırasıyla kullanır:

1. İstemci MQSCO yapısında *CertificateValPolicy* alanının kullanılması. Bu alanı kullanma hakkında daha fazla bilgi için bkz. MQSCO-SSL yapılandırma seçenekleri.
2. *MQCERTVPOL*istemci ortam değişkenini kullanarak. Bu değişkeni kullanma hakkında daha fazla bilgi için bkz. MQCERTVPOL.
3. İstemci SSL kısmı ayarlama parametresi ayarını kullanarak, *CertificateValPolicy*. Bu ayarın kullanılmasıyla ilgili ek bilgi için İstemci yapılanış kütüğünün SSL kısmıbaşlıklı konuya bakın.

Sertifika doğrulama ilkeleri hakkında daha fazla bilgi için bkz. “IBM MQiçindeki sertifika geçerlilik denetimi ilkeleri” sayfa 41.

IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu

Bu konuda, IBM MQiçinde CipherSpecs ile dijital sertifikalar arasındaki ilişkiyi özetleyerek güvenlik ilkeniz için uygun CipherSpecs ve dijital sertifikaların nasıl seçileceğine ilişkin bilgiler sağlanır.

Desteklenen tüm sayısal sertifika tipleriyle yalnızca desteklenen CipherSpecs alt kümesi kullanılabilir. Bu nedenle, sayısal sertifikanız için uygun bir CipherSpec seçmeniz gerekir. Benzer şekilde, kuruluşunuzun güvenlik ilkesi belirli bir CipherSpec ' i kullanmanızı gerektiriyorsa, bu CipherSpeciçin uygun bir sayısal sertifika edinmeniz gerekir.

MD5 dijital imza algoritması ve TLS 1.2

MD5 algoritması kullanılarak imzalanan sayısal sertifikalar, TLS 1.2 protokolü kullanıldığında reddedilir. Bunun nedeni, MD5 algoritmasının artık birçok şifreleme analisti tarafından zayıf kabul edilmesi ve

kullanımının genellikle önerilmez olmasıdır. TLS 1.2 iletişim kuralına dayalı daha yeni CipherSpecs kullanmak için dijital sertifikaların dijital imzalarında MD5 algoritmasını kullanmadığından emin olun. TLS 1.0 iletişim kurallarını kullanan daha eski CipherSpecs bu kısıtlamaya tabi değildir ve MD5 dijital imzaları olan sertifikaları kullanmaya devam edebilir.

Belirli bir sertifikaya ilişkin sayısal imza algoritmasını görüntülemek için **runmqakm** komutunu kullanabilirsiniz:

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

Burada *cert_label* , görüntülenecek dijital imza algoritmasının sertifika etiketidir. Ayrıntılar için bkz. Dijital sertifika etiketleri .

Not: runmqckm (iKeycmd) ve **strmqikm** (iKeyman) GUI 'si bir dizi dijital imza algoritmasını görüntülemek için kullanılabilse de, **runmqakm** aracı daha geniş bir aralık sağlar.

runmqakm komutunun çalıştırılması, belirtilen imza algoritmasının kullanımını görüntüleyen bir çıkış üretir:

```
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
```

`Signature Algorithm` satırı, `MD5WithRSASignature` algoritmasının kullanıldığını gösterir. Bu algoritma MD5 ' i temel alır ve bu dijital sertifika TLS 1.2 CipherSpecsile kullanılamaz.

Eliptik Eğri ve RSA CipherSpecs Birlikte Çalışabilirlik

V 9.1.4 Tüm CipherSpecs dijital sertifikalarla birlikte kullanılamaz. CipherSpecs , CipherSpec ad önekiyle gösterilir. Her CipherSpec tipi, kullanılabilecek sayısal sertifika tipi üzerinde farklı kısıtlamalar uygular. Bu kısıtlamalar tüm IBM MQ TLS bağlantıları için geçerlidir, ancak özellikle Eliptik Eğri şifreleme kullanıcıları için geçerlidir.

Aşağıdaki tablo, CipherSpecs ile dijital sertifikalar arasındaki ilişkileri özetler:

Çizelge 4. CipherSpecs ile dijital sertifikalar arasındaki ilişkiler

Tip	CipherSpec Ad Öneki	Açıklama	Gerekli genel anahtar tipi	Dijital imza şifreleme algoritması	Gizli anahtar oluşturma yöntemi
1	ECDHE_ECDSA_	Eliptik Eğri ve genel anahtarları, Eliptik Eğri gizli tuşları ve Eliptik Eğri sayısal imza algoritmalarını kullanan CipherSpecs (Şifre Belirtimleri).	Eliptik Eğri	ECDSA	ECDHE
2	ECDHE_RSA_	RSA ortak anahtarlarını, Eliptik Eğri gizli anahtarlarını ve RSA dijital imza algoritmalarını kullanan CipherSpecs (Şifre Belirtimleri).	RSA	RSA	ECDHE
V 9.1.4 3	(Tüm TLS 1.3 CipherSpecs)	Eliptik Eğri ya da RSA genel anahtarlarını, Eliptik Eğri gizli anahtarlarını ve Eliptik Eğri ya da RSA sayısal imza algoritmalarını kullanan CipherSpecs .	Eliptik Eğri ya da RSA	ECDSA ya da RSA	ECDHE ya da RSA
4	(Diğerleri)	RSA ortak anahtarlarını ve RSA dijital imza algoritmalarını kullanan CipherSpecs (Şifre Belirtimleri).	RSA	RSA	RSA

Not: Tip 1 ve 2 CipherSpecs , IBM i altyapısında IBM MQ kuyruk yöneticileri ve MQI istemcileri tarafından desteklenmez.

Gerekli genel anahtar tipi kolonu, her CipherSpectipi kullanılırken kişisel sertifikanın sahip olması gereken genel anahtarın tipini gösterir. Kişisel sertifika, kuyruk yöneticisini ya da istemciyi uzak ortağına tanıtan son varlık sertifikasıdır.

Bir kanalı, eliptik Eğri (EC) sertifikası ve RSA sertifikası için sertifika etiketi gerektiren bir CipherSpec ile ya da tersi yönde yapılandırabilirsiniz. Sertifika etiketinde adı belirtilen sertifikanın CipherSpeckanalı için uygun olduğundan emin olmanız gerekir.

IBM MQ' in doğru şekilde yapılandırıldığını varsayarak şunları yapabilirsiniz:

- RSA ve EC sertifikalarının karışımını içeren tek bir kuyruk yöneticisi.
- Aynı kuyruk yöneticisinde RSA ya da EC sertifikası kullanan farklı kanallar.

Dijital imza şifreleme algoritması, eşin geçerliliğini denetlemek için kullanılan şifreleme algoritmasına başvurur. Şifreleme algoritması, sayısal imzayı hesaplamak için MD5, SHA-1 ya da SHA-256 gibi bir hash algoritmasıyla birlikte kullanılır. Çeşitli sayısal imza algoritmaları kullanılabilir; örneğin, MD5 ile RSA ya da SHA-256ile ECDSA. Tabloda ECDSA, ECDSA kullanan dijital imza algoritmaları kümesini ifade eder; RSA, RSA kullanan dijital imza algoritmaları kümesini ifade eder. Belirtilen şifreleme algoritmasına dayalı olması koşuluyla, sette desteklenen herhangi bir dijital imza algoritması kullanılabilir.

Tip 1 CipherSpecs , kişisel sertifikanın bir Eliptik Eğri genel anahtarına sahip olmasını gerektirir. Bu CipherSpecs kullanıldığında, bağlantıya ilişkin gizli anahtarı oluşturmak için Elliptic Curve Diffie Hellman Ephemeral anahtar sözleşmesi kullanılır.

Tip 2 CipherSpecs , kişisel sertifikanın bir RSA genel anahtarına sahip olmasını gerektirir. Bu CipherSpecs kullanıldığında, bağlantıya ilişkin gizli anahtarı oluşturmak için Elliptic Curve Diffie Hellman Ephemeral anahtar sözleşmesi kullanılır.

Tip 3 CipherSpecs , kişisel sertifikanın bir RSA genel anahtarına sahip olmasını gerektirir. Bu CipherSpecs kullanıldığında, bağlantıya ilişkin gizli anahtarı oluşturmak için RSA anahtar değişimi kullanılır.

Bu kısıtlama listesi ayrıntılı değildir: Yapılandırmaya bağlı olarak, birlikte çalışma yeteneğini daha fazla etkileyebilecek ek kısıtlamalar olabilir. Örneğin, IBM MQ FIPS 140-2 ya da NSA Suite B standartlarına uyacak şekilde yapılandırıldıysa, bu işlem izin verilen yapılandırma aralığını da sınırlar. Daha fazla bilgi için aşağıdaki bölüme bakın.

Aynı kuyruk yöneticisinde ya da istemci uygulamasında farklı tiplerde CipherSpec kullanmanız gerekirse, istemci tanımlamasında uygun bir sertifika etiketi ve CipherSpec birleşimi yapılandırın.

Üç CipherSpec tipi doğrudan birlikte çalışmaz: Bu, yürürlükteki TLS standartlarının bir sınırlamasıdır. Örneğin, QM1adlı bir kuyruk yöneticisinde TO.QM1 adlı bir alıcı kanalı için ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec ' ı kullanmayı seçtiğinizi varsayın; bu durumda, alıcının Eliptik Eğri anahtarı ve ECDSA tabanlı sayısal imzası olan kişisel bir sertifikası olmalıdır. Alıcı kanal bu gereksinimleri karşılamıyorsa, kanal başlatılamıyor.

QM1 kuyruk yöneticisine bağlanan diğer kanallar, her bir kanalın CipherSpec için doğru tipte bir sertifika kullanması koşuluyla diğer CipherSpecskanallarını kullanabilir. Örneğin, QM1 ' in QM2adlı başka bir kuyruk yöneticisine ileti göndermek için TO.QM2 adlı bir gönderen kanalı kullandığını varsayın. Kanal TO.QM2 Tip 3 CipherSpec TLS_RSA_WITH_AES_256_CBC_SHA256 , RSA genel anahtarlarını içeren kanal kullanım sertifikalarının her iki ucunu da içermesi koşuluyla kullanabilir. Sertifika etiketi kanal özniteliği, her kanal için farklı bir sertifika yapılandırmak için kullanılabilir.

IBM MQ ağlarınızı planlarken hangi kanalların TLS gerektirdiğini dikkatle göz önünde bulundurun ve her kanal için kullanılan sertifika tipinin o kanaldaki CipherSpec ile kullanılmaya uygun olduğundan emin olun.

Dijital sertifikaya ilişkin sayısal imza algoritmasını ve genel anahtar tipini görüntülemek için **runmqakm** komutunu kullanabilirsiniz:

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

Burada *cert_label* , dijital imza algoritmasını görüntülemeniz gereken sertifikanın etiketidir. Ayrıntılar için bkz. Dijital sertifika etiketleri .

runmqakm komutunun yürütülmesi, Genel Anahtar Tipini görüntüleyen çıktı üretecektir:

```
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
```

Bu durumda Genel Anahtar Tipi satırı, sertifikanın bir Eliptik Eğri ortak anahtarı olduğunu gösterir. Bu durumda İmza Algoritması satırı, EC_ecdsa_with_SHA384 algoritmasının kullanımda olduğunu gösterir: Bu, ECDSA algoritmasına dayalıdır. Bu nedenle bu sertifika yalnızca Tip 1 CipherSpecsile kullanıma uygundur.

runmqckm komutunu aynı parametrelerle de kullanabilirsiniz. Anahtar havuzunu açar ve sertifikanın etiketini çift tıklatırsanız, dijital imza algoritmalarını görüntülemek için **strmqikm** GUI de kullanılabilir. Ancak, daha geniş bir algoritma yelpazesini desteklediğinden dijital sertifikaları görüntülemek için **runmqakm** aracını kullanmalısınız.

TLS 1.3 CipherSpecs

V 9.1.4

TLS 1.3 CipherSpecs , hem ECDSA hem de RSA sertifikalarını destekler.

Eliptik Eğri CipherSpecs ve NSA Suite B

IBM MQ , Suite B uyumlu TLS 1.2 profiline uymak üzere yapılandırıldığında, izin verilen CipherSpecs ve dijital imza algoritmaları “NSA Suite B Cryptografi (IBM MQ)” sayfa 38içinde açıklandığı şekilde kısıtlanır. Ayrıca, kabul edilebilir Eliptik Eğri tuşlarının aralığı, yapılandırılan güvenlik düzeylerine göre azaltılır.

128 bit Suite B güvenlik düzeyinde, sertifika konusunun açık anahtarının NIST P-256 ya da NIST P-384 eliptik eğrisini kullanması ve NIST P-256 eliptik eğrisiyle ya da NIST P-384 eliptik eğrisiyle imzalanması gerekir. **runmqakm** komutu, EC_ecdsa_with_SHA256ya da EC_ecdsa_with_SHA384-sig_alg değiştirgesini kullanarak bu güvenlik düzeyine ilişkin sayısal sertifikaları istemek için kullanılabilir.

192 bitlik Suite B güvenlik düzeyinde, sertifika konusunun açık anahtarının NIST P-384 eliptik eğrisini kullanması ve NIST P-384 eliptik eğrisiyle imzalanması gerekir. **runmqakm** komutu, EC_ecdsa_with_SHA384-sig_alg parametresi kullanılarak bu güvenlik düzeyine ilişkin sayısal sertifikaları istemek için kullanılabilir.

Desteklenen NIST eliptik eğrileri şunlardır:

Çizelge 5. Desteklenen NIST eliptik eğrileri

NIST FIPS 186-3 eğri adı	**RFC 4492 eğri adı**	**Eliptik Eğri anahtar boyutu (bit)**
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

Not: NIST P-521 eliptik eğrisi, Suite B uyumlu işlem için kullanılamaz.

İlgili kavramlar

“CipherSpecs' in etkinleştirilmesi” sayfa 402
Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

“MQI istemcisinde çalıştırma zamanında yalnızca FIPS onaylı CipherSpecs kullanılmasının belirtilmesi” sayfa 258
FIPS uyumlu yazılımı kullanarak anahtar havuzlarınızı oluşturun ve daha sonra, kanalın FIPS onaylı CipherSpecsözelliğini kullanması gerektiğini belirtin.

“NSA Suite B Cryptografi (IBM MQ)” sayfa 38
This topic provides information about how to configure IBM MQ on Windows, Linux, and UNIX to conform to the Suite B compliant TLS 1.2 profile.

“Ulusal Güvenlik Ajansı (NSA) Suite B Cryptography” sayfa 19

Amerika Birleşik Devletleri hükümeti, veri şifrelemesi de dahil olmak üzere BT sistemleri ve güvenliği konusunda teknik danışmanlık yapıyor. ABD Ulusal Güvenlik Dairesi (NSA), Suite B standardındaki bir dizi işletilebilir kriptografik algoritmayı önermektedir.

Kanal doğrulama kayıtları

Kanal düzeyinde bağlanan sistemlere verilen erişim üzerinde daha kesin denetim sağlamak için kanal kimlik doğrulama kayıtlarını kullanabilirsiniz.

İstemcilerin kuyruk yöneticinizle boş bir kullanıcı kimliği ya da istemcinin istenmeyen işlemleri gerçekleştirmesini sağlayacak üst düzey bir kullanıcı kimliği kullanarak bağlantı kurmayı denediğini bulabilirsiniz. Kanal kimlik doğrulama kayıtlarını kullanarak bu istemcilere erişimi engelleyebilirsiniz. Diğer bir seçenek olarak, bir istemci istemci altyapısında geçerli olan, ancak bilinmeyen ya da sunucu altyapısında geçersiz biçimdeki bir kullanıcı kimliğini belirleyebilir. Bildirili kullanıcı kimliğini geçerli bir kullanıcı kimliğiyle eşlemek için bir kanal kimlik doğrulama kaydı kullanabilirsiniz.

Kuyruk yöneticinizle bağlantı kuran ve bir şekilde kötü davranan bir istemci uygulaması bulabilirsiniz. Sunucuyu bu uygulamanın neden olduğu sorunlardan korumak için, güvenlik duvarı kuralları güncelleninceye ya da istemci uygulaması düzeltilinceye kadar istemci uygulamasının açık olduğu IP adresi kullanılarak geçici olarak engellenmesi gerekir. İstemci uygulamasının bağlandığı IP adresini engellemek için bir kanal doğrulama kaydı kullanabilirsiniz.

IBM MQ Explorergibi bir yönetim aracı ve bu belirli kullanım için bir kanal ayarladıysanız, bunu yalnızca belirli istemci bilgisayarların kullanabildiğinden emin olmak isteyebilirsiniz. Kanalın yalnızca belirli IP adreslerinden kullanılmasına izin vermek için bir kanal doğrulama kaydı kullanabilirsiniz.

İstemci olarak çalışan bazı örnek uygulamalarla çalışmaya başladıysanız, kanal doğrulama kayıtlarını kullanarak kuyruk yöneticisinin güvenli bir şekilde ayarlanması örneği için Örnek programların hazırlanması ve çalıştırılması konusuna bakın.

Gelen kanalları denetlemek üzere kanal kimlik doğrulama kayıtlarını almak için **ALTER QMGR CHLAUTH(ENABLED)** MQSC komutunu kullanın.

CHLAUTH kuralları, yeni bir gelen bağlantıya yanıt olarak oluşturulan bir kanal MCA için uygulanır. Yerel olarak başlatılmakta olan kanala yanıt olarak oluşturulan bir kanal MCA için **CHLAUTH** kuralları uygulanmaz.

Çizelge 6. CHLAUTH kurallarının farklı kanal çiftleri için uygulandığı yer

Kanal tipi	**CHLAUTH kurallarının uygulandığı MCA**
SDR-RCVR	RCVR
RQSTR-SVR (SVR ' de başlatıldı)	RQSTR
RQSTR-SVR (RQSTR ' de başlatıldı)	SVR
RQSTR-SDR (SDR ' de başlatıldı)	RQSTR
RQSTR-SDR (RQSTR ' de başlatıldı)	İlk bağlantı için SDR. Geri çağırma bağlantısı için RQSTR.

Aşağıdaki işlevleri gerçekleştirmek için kanal doğrulama kayıtları oluşturulabilir:

- Belirli IP adreslerinden bağlantıları engellemek için.
- Belirli kullanıcı kimliklerinden gelen bağlantıları engellemek için.
- Belirli bir IP adresinden bağlanan herhangi bir kanal için kullanılacak bir MCAUSER değeri ayarlamak için.
- Belirli bir kullanıcı kimliği alan herhangi bir kanal için kullanılacak bir MCAUSER değeri ayarlamak için.
- Belirli bir SSL ya da TLS Ayırt Edici Adı (DN) olan herhangi bir kanal için kullanılacak bir MCAUSER değeri ayarlamak için.

- Belirli bir kuyruk yöneticisinden bağlantı kuran herhangi bir kanal için kullanılacak bir MCAUSER değeri ayarlamak için.
- Bağlantı belirli bir IP adresinden değilse, belirli bir kuyruk yöneticisinden olduğunu iddia eden bağlantıları engellemek için.
- Bağlantı belirli bir IP adresinden olmadığı sürece, belirli bir SSL ya da TLS sertifikasını sunan bağlantıları engellemek için.

Bu kullanımlar aşağıdaki bölümlerde daha ayrıntılı olarak açıklanmıştır.

SET CHLAUTH ya da PCF komutunu **Set Channel Authentication Record**kullanarak kanal kimlik doğrulama kayıtları yaratabilir, bunları değiştirebilir ya da kaldırabilirsiniz.

Not: Çok sayıda kanal doğrulama kaydı, kuyruk yöneticisinin performansı üzerinde olumsuz etki yaratabilirler.

Engelleyici IP adresleri

Normalde belirli IP adreslerinden erişimi önlemek için bir güvenlik duvarının rolüdür. Ancak, IBM MQ sisteminize erişimi olmaması gereken bir IP adresinden bağlantı girişimleriyle karşılaşabileceğiniz ve güvenlik duvarının güncellenebilmesi için adresi geçici olarak engellemeniz gereken durumlar olabilir. Bu bağlantı girişimleri IBM MQ kanallarından gelmeyebilir; bu bağlantı girişimleri, IBM MQ dinleyicinizi hedeflemek için yanlış yapılandırılan diğer yuva uygulamalarından geliyor olabilir. BLOCKADDR tipinde bir kanal doğrulama kaydı ayarlayarak IP adreslerini engelleyin. Genel arama karakterleri de içinde olmak üzere bir ya da daha çok tek adres, adres aralığı ya da kalıp belirtebilirsiniz.

IP adresi bu şekilde engellendiği için bir gelen bağlantı reddedildiğinde, kanal olayları etkinleştirildiyse ve kuyruk yöneticisi çalışıyorsa, neden niteleyicisi MQRQ_CHANNEL_BLOCKED_ADDRESS olan bir olay iletisi yayınlanır. Buna ek olarak, dinleyicinin engellenen bağlantı için yinelenen girişimler nedeniyle dinleyicinin su altında kalmadığından emin olmak için, bağlantı, hata döndürmeden önce 30 saniye boyunca açık tutulur.

Yalnızca belirli kanallardaki IP adreslerini engellemek ya da hata bildirilmeden önceki gecikmeyi önlemek için, USERSRC (NOACCESS) parametresiyle ADDRESSMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın.

Bu nedenle bir gelen bağlantı reddedildiğinde, kanal olayları etkinleştirildiyse ve kuyruk yöneticisi çalışıyorsa, neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS olan bir MQRC_CHANNEL_BLOCKED olay iletisi yayınlanır.

Örneğin, “Belirli IP adreslerinin engellenmesi” sayfa 369 başlıklı konuya bakın.

Engelleyici kullanıcı kimlikleri

Belirli kullanıcı kimliklerinin bir istemci kanalı üzerinden bağlanmasını önlemek için, BLOCKUSER tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Bu tip kanal kimlik doğrulama kaydı, ileti kanallarına değil, yalnızca istemci kanallarına uygulanır. Engellenecek bir ya da daha fazla kullanıcı kimliği belirtebilirsiniz, ancak genel arama karakterleri kullanamazsınız.

Bu nedenle bir gelen bağlantı reddedildiğinde, kanal olayları etkinleştirildiyse, neden niteleyicisi MQRQ_CHANNEL_BLOCKED_USERID olan MQRC_CHANNEL_BLOCKED olay iletisi yayınlanır.

Örneğin, “Belirli kullanıcı kimliklerini engelle” sayfa 370 başlıklı konuya bakın.

USERSRC (NOACCESS) parametresiyle USERMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayarak, belirli kanallarda belirtilen kullanıcı kimlikleri için herhangi bir erişimi engelleyebilirsiniz.

Bu nedenle bir gelen bağlantı reddedildiğinde, kanal olayları etkinleştirildiyse ve kuyruk yöneticisi çalışıyorsa, neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS olan bir MQRC_CHANNEL_BLOCKED olay iletisi yayınlanır.

Örneğin, “İstemci kullanıcı kimliği için erişimin engellenmesi” sayfa 373 başlıklı konuya bakın.

Engelleyici kuyruk yöneticisi adları

Belirtilen bir kuyruk yöneticisinden bağlanan herhangi bir kanalın erişimi olmadığını belirtmek için, USERSRC (NOACCESS) parametresiyle QMGRMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Tek bir kuyruk yöneticisi adı ya da genel arama karakterleri de içinde olmak üzere bir kalıp belirtebilirsiniz. Kuyruk yöneticilerinden erişimi engellemek için BLOCKUSER işlevinin eşdeğeri yoktur.

Bu nedenle bir gelen bağlantı reddedildiğinde, kanal olayları etkinleştirildiyse ve kuyruk yöneticisi çalışıyorsa, neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS olan bir MQRC_CHANNEL_BLOCKED olay iletisi yayınlanır.

Örneğin, "Uzak kuyruk yöneticisinden erişimin engellenmesi" sayfa 373 başlıklı konuya bakın.

SSL ya da TLS DN ' leri engelleme

Belirli bir DN içeren bir SSL ya da TLS kişisel sertifikası sunan herhangi bir kullanıcının erişimi olmadığını belirtmek için, USERSRC (NOACCESS) parametresiyle SSLPEERMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Genel arama karakterleri de içinde olmak üzere tek bir ayırt edici ad ya da örüntü belirtebilirsiniz. DN ' lere erişimi engellemek için BLOCKUSER işlevinin eşdeğeri yoktur.

Bu nedenle bir gelen bağlantı reddedildiğinde, kanal olayları etkinleştirildiyse ve kuyruk yöneticisi çalışıyorsa, neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS olan bir MQRC_CHANNEL_BLOCKED olay iletisi yayınlanır.

Örneğin, "SSL ya da TLS Ayırt Edici Adı için erişimin engellenmesi" sayfa 374 başlıklı konuya bakın.

Kullanılacak IP adreslerinin kullanıcı kimlikleriyle eşlenmesi

Belirtilen bir IP adresinden bağlanan herhangi bir kanalın belirli bir MCAUSER ' i kullanmasını belirtmek için, ADDRESSMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Tek bir adres, adres aralığı ya da genel arama karakterleri de içinde olmak üzere bir kalıp belirtebilirsiniz.

Bir kapı ileticisi, DMZ oturumu kesmesi ya da kuyruk yöneticisine sunulan IP adresini değiştiren başka bir ayar kullanırsanız, eşleme IP adresleri kullanımınız için uygun olmayabilir.

Örneğin, "Bir IP adresinin MCAUSER kullanıcı kimliği ile eşlenmesi" sayfa 374 başlıklı konuya bakın.

Kuyruk yöneticisi adlarının kullanılacak kullanıcı kimlikleriyle eşlenmesi

Belirli bir kuyruk yöneticisinden bağlantı kuran herhangi bir kanalın belirli bir MCAUSER ' i kullanacağı belirtmek için, QMGRMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Tek bir kuyruk yöneticisi adı ya da genel arama karakterleri de içinde olmak üzere bir kalıp belirtebilirsiniz.

Örneğin, "Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi" sayfa 371 başlıklı konuya bakın.

Bir istemci tarafından bildirilen kullanıcı kimliklerinin kullanılacak kullanıcı kimlikleriyle eşlenmesi

Belirli bir kullanıcı kimliği IBM MQ MQI istemcisinden gelen bir bağlantı tarafından kullanılıyorsa, farklı, belirtilen bir MCAUSER kullanılacaksa, USERMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Kullanıcı kimliği eşlemesi joker karakter kullanmaz.

Örneğin, "İstemci kullanıcı kimliğinin MCAUSER kullanıcı kimliğiyle eşlenmesi" sayfa 372 başlıklı konuya bakın.

SSL ya da TLS DN ' lerinin kullanılacak kullanıcı kimlikleriyle eşlenmesi

Belirli bir DN içeren bir SSL/TLS kişisel sertifikası sunan herhangi bir kullanıcının belirli bir MCAUSER kullanacağını belirtmek için, SSLPEERMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın. Genel arama karakterleri de içinde olmak üzere tek bir ayırt edici ad ya da örüntü belirtebilirsiniz.

Örneğin, "SSL ya da TLS Ayırt Edici Adının MCAUSER kullanıcı kimliğine eşlenmesi" sayfa 372 başlıklı konuya bakın.

Kuyruk yöneticilerinin, istemcilerin ya da SSL ya da TLS DN ' lerinin IP adresine göre eşlenmesi

Bazı durumlarda, üçüncü bir tarafın bir kuyruk yöneticisi adını sahtecisi olması mümkün olabilir. Bir SSL ya da TLS sertifikası ya da anahtar veritabanı dosyası da çalınabilir ve yeniden kullanılabilir. Bu tehditlere karşı koruma sağlamak için, belirli bir kuyruk yöneticisinden ya da istemciden gelen bir bağlantının ya da belirli bir DN ' nin belirli bir IP adresinden bağlanması gerektiğini belirtebilirsiniz. USERMAP, QMGRMAP ya da SSLPEERMAP tipinde bir kanal kimlik doğrulama kaydı ayarlayın ve ADDRESS parametresini kullanarak izin verilen IP adresini ya da IP adresleri kalıbını belirtin.

Örneğin, “Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi” sayfa 371 başlıklı konuya bakın.

Kanal kimlik doğrulama kayıtları arasındaki etkileşim

Bağlantı kurmaya çalışan bir kanalın birden çok kanal kimlik doğrulama kaydıyla eşleşmesi ve bunların çelişkili etkileri olması olasıdır. Örneğin, bir kanal, BLOCKUSER kanal kimlik doğrulama kaydı tarafından engellenen bir kullanıcı kimliğini, ancak farklı bir kullanıcı kimliği ayarlayan bir SSLPEERMAP kaydıyla eşleşen bir SSL ya da TLS sertifikasını doğrulayabilir. Ayrıca, kanal kimlik doğrulama kayıtları joker karakter kullanıyorsa, tek bir IP adresi, kuyruk yöneticisi adı ya da SSL ya da TLS DN birden çok kalıpla eşleşebilir. Örneğin, 192.0.2.6 IP adresi 192.0.2.0-24, 192.0.2. *, kalıplarıyla eşleşir. ve 192.0. * .6. Yapılan işlem aşağıdaki gibi belirlenir.

- Kullanılan kanal kimlik doğrulama kaydı aşağıdaki gibi seçilir:
  - Kanal adıyla açıkça eşleşen bir kanal kimlik doğrulama kaydı, genel arama karakteri kullanarak kanal adıyla eşleşen bir kanal kimlik doğrulama kaydından önceliklidir.
  - SSL ya da TLS DN kullanan bir kanal kimlik doğrulama kaydı, kullanıcı kimliği, kuyruk yöneticisi adı ya da IP adresi kullanan bir kayıttan önceliklidir.
  - Kullanıcı kimliği ya da kuyruk yöneticisi adı kullanan bir kanal kimlik doğrulama kaydı, IP adresi kullanan bir kayıttan önceliklidir.
- Eşleşen bir kanal kimlik doğrulama kaydı bulunursa ve bir MCAUSER belirtirse, bu MCAUSER kanala atanır.
- Eşleşen bir kanal kimlik doğrulama kaydı bulunursa ve kanalın erişimi olmadığını belirtirse, kanala *NOACCESS MCAUSER değeri atanır. Bu değer daha sonra bir güvenlik çıkış programı tarafından değiştirilebilir.
- Eşleşen bir kanal kimlik doğrulama kaydı bulunamazsa ya da eşleşen bir kanal kimlik doğrulama kaydı bulunursa ve kanalın kullanıcı kimliğinin kullanılacağını belirtirse, MCAUSER alanı incelenir.
  - MCAUSER alanı boşsa, istemci kullanıcı kimliği kanala atanır.
  - MCAUSER alanı boş değilse, kanala atanır.
- Herhangi bir güvenlik çıkış programı çalıştırılır. Bu çıkış programı, kanal kullanıcı kimliğini ayarlayabilir ya da erişimin engelleneceğini belirleyebilir.
- Bağlantı engellenirse ya da MCAUSER için *NOACCESS değeri belirlenmişse, kanal sona erer.
- Bağlantı engellenmezse, bir istemci kanalı dışında herhangi bir kanal için, önceki adımlarda belirlenen kanal kullanıcı kimliği, engellenen kullanıcılar listesiyle karşılaştırılarak denetlenir.
  - Kullanıcı kimliği engellenen kullanıcılar listesindeyse, kanal sona erer.
  - Kullanıcı kimliği engellenen kullanıcılar listesinde yoksa, kanal çalışır.

Kanal kimlik doğrulama kayıtlarının sayısı bir kanal adı, IP adresi, anasistem adı, kuyruk yöneticisi adı ya da SSL ya da TLS ile eşleştiği durumlarda, en özel eşleşme kullanılır. Eşleşme şu şekilde değerlendirilir:

- En özel ad, genel arama karakteri içermeyen bir addır; örneğin:
  - A.B.C
  - 192.0.2.6 IP adresi
  - `hursley.ibm.com` anasistem adı

  - 192.0.2.6 kuyruk yöneticisi adı
- En soysal olanı, aşağıdaki gibi eşleşen tek bir yıldız işaretidir (*):
  - Tüm kanal adları
  - Tüm IP adresleri
  - Tüm anasistem adları
  - Tüm kuyruk yöneticisi adları
- Bir dizginin başında yıldız işareti olan bir kalıp, bir dizginin başında tanımlı bir değerden daha soysaldır:
  - Kanallar için, *.B.C , A ' dan daha genel. *
  - IP adresleri için, *.0.2.6 192 'den daha soysaldır. *
  - Anasistem adları için `*.ibm.com` , `hursley.*` değerinden daha soysal
  - Kuyruk yöneticisi adları için, *QUEUEMANAGER değeri QUEUEMANAGER* değerinden daha soysal
- Bir dizginin belirli bir yerinde yıldız işareti olan bir kalıp, bir dizginin aynı yerinde tanımlı bir değerden daha soysaldır ve benzer şekilde, bir dizginin sonraki her yeri için de geçerlidir:
  - Kanallar için A. * .C, A.B.*
  - IP adresleri için 192. *.2.6 , 192.0. * ' dan daha soysaldır.
  - Anasistem adları için `hursley.*.com` , `hursley.ibm.*` değerinden daha soysal
  - Kuyruk yöneticisi adları için Q* MANAGER, QUEUE* ' den daha soysal
- İki ya da daha çok örüntüde bir dizginin belirli bir yerinde yıldız işareti varsa, yıldız işaretini izleyen daha az sayıda düğüm daha soysaldır:
  - Kanallar için, A. * A * .C ' den daha soysal
  - IP adresleri için, 192. * 192. * .2. * değerinden daha soysal.
  - Anasistem adları için `hurlsey.*` , `hursley.*.com` değerinden daha soysal
  - Kuyruk yöneticisi adları için Q*, Q* MGR ' den daha soysal
- Ayrıca, bir IP adresi için:
  - Kısa çizgi (-) ile gösterilen bir aralık, yıldız işaretinden daha özeldir. Bu nedenle 192.0.2.0-24 , 192.0.2. * ' den daha özeldir.
  - Başka bir alt küme olan bir aralık, daha büyük aralıktan daha özeldir. Bu nedenle 192.0.2.5-15 , 192.0.2.0-24sürümünden daha özeldir.
  - Çakışan aralıklara izin verilmez. Örneğin, hem 192.0.2.0-15 hem de 192.0.2.10-20için kanal kimlik doğrulama kayıtlarına sahip olamazsınız.
  - Örüntü, tek bir sondaki yıldız işaretiyle bitmedikçe, bir örüntünün istenen kısım sayısından az olamaz. Örneğin, 192.0.2 geçersiz, ancak 192.0.2.* geçerli.
  - Sondaki yıldız işareti, adresin geri kalan kısmından uygun parça ayırıcısıyla (IPv4için nokta (.), IPv6için iki nokta (:) ile ayrılmalıdır. Örneğin, 192.0* geçerli değildir, çünkü yıldız işareti kendi içinde yer almıyor.
  - Sondaki yıldız işaretinin yanında yıldız işareti olmaması koşuluyla, bir kalıp ek yıldız işaretleri içerebilir. Örneğin, 192. * .2. * geçerli, ancak 192.0. * .* (çizelge adı) geçersiz.
  - Sonuçtaki adres belirsiz olacağından, IPv6 adres kalıbı çift iki nokta üst üste ve sondaki yıldız işareti içeremez. Örneğin, 2001:: *, 2 0 0 1: 0 0 0: *, 2001:0000:0000: * olarak genişletilebilir
- Bir SSL ya da TLS Ayırt Edici Adı (DN) için, alt dizgilerin öncelik sırası aşağıdaki gibidir:

Çizelge 7. Alt dizgilerin öncelik sırası

Sipariş	**DN alt dizgisi**	**Ad**
1	SERI NUMARASı=	Sertifika seri numarası
2	MAIL=	E-posta adresi

Çizelge 7. Alt dizgilerin öncelik sırası (devamı var)		
Sipariş	**DN alt dizgisi**	**Ad**
3	E=	E-posta adresi (MAIL tercihine göre kullanımdan kaldırıldı)
4	UID=, USERID=	Kullanıcı kimliği
5	CN=	Ortak ad
6	T =	Unvan
7	OU=	Kuruluş Birimi
8	DC=	Etki alanı bileşeni
9	O=	Kuruluş
10	SOKAK =	Açık/İlk adres satırı
11	L=	İlçe
12	ST =, SP=, S=	Eyalet ya da bölge adı
13	PC=	Posta kodu/posta kodu
14	C=	Ülke
15.000	UNSTRUCTUREDNAME=	Anasistem adı
16	UNSTRUCTUREDADDRESS=	IP adresi
17	DNQ=	Ayırt edici ad niteleyicisi

Bu nedenle, bir SSL ya da TLS sertifikası O=IBM ve C=UK alt dizgilerini içeren bir DN ile sunulursa, IBM MQ her ikisi de varsa, C=UK için bir yerine O=IBM için bir kanal kimlik doğrulama kaydı kullanır.

Bir DN birden çok kuruluş birimi içerebilir; bu değer, önce büyük kuruluş birimleri belirtilmiş olarak sıradüzensel sırayla belirtilmelidir. İki DN, kuruluş birimi değerleri dışında her bakımdan eşitse, daha spesifik DN aşağıdaki gibi belirlenir:

1. Farklı sayıda kuruluş birimi özniteliklerine sahiplerse, en fazla kuruluş birimi değerine sahip ayırt edici ad (DN) daha belirleyici olur. Bunun nedeni, daha fazla Kuruluş Birimine sahip DN 'in DN' yi daha ayrıntılı olarak niteleyip daha fazla eşleşme ölçütü sağlamış olmasıdır. Üst düzey kuruluş birimi genel arama karakteri (OU = *) olsa da, daha fazla kuruluş birimine sahip DN genel olarak kabul edilir.
2. Aynı sayıda Kuruluş Birimi özniteliğine sahiplerse, karşılık gelen Kuruluş Birimi değeri çiftleri soldan sağa doğru sırayla karşılaştırılır; burada en soldaki Kuruluş Birimi, aşağıdaki kurallara göre en yüksek düzeydir (en az özel).
   a. Genel arama karakteri değeri olmayan bir kuruluş birimi, yalnızca tek bir dizgiyle eşleşebildiği için en özeldir.
   b. Başında ya da sonunda tek bir genel arama karakteri bulunan bir kuruluş birimi (örneğin, OU=ABC* ya da OU= *ABC) bir sonraki en özel seçenektir.
   c. İki genel arama karakteri içeren bir kuruluş birimi (örneğin, OU= *ABC*) bir sonraki en özeldir.
   d. Yalnızca yıldız işaretinden (OU = *) oluşan bir kuruluş birimi en az özeldir.
3. Dizgi karşılaştırması aynı özelliğe sahip iki öznitelik değeri arasında bağlıysa, daha uzun olan öznitelik dizgisi daha belirgindir.
4. Dizgi karşılaştırması aynı özgüllük ve uzunluğa sahip iki öznitelik değeri arasında bağlıysa, sonuç, DN ' nin herhangi bir genel arama karakteri dışında olan kısmının büyük ve küçük harfe duyarsız bir dizgi karşılaştırmasıyla saptanır.

İki DN, DC değerleri dışında her bakımdan eşitse, DC değerlerinde en soldaki DC 'nin en düşük düzey (en spesifik) olması ve karşılaştırma sıralamasının buna göre farklılık göstermesi dışında, aynı eşleşen kurallar OU' lar için de geçerlidir.

Kanal kimlik doğrulama kayıtlarının görüntülenmesi

Kanal kimlik doğrulama kayıtlarını görüntülemek için **DISPLAY CHLAUTH** ya da PCF komutunu **Inquire Channel Authentication Records**kullanın. Sağlanan kanal adıyla eşleşen tüm kayıtları döndürmeyi seçebilir ya da belirtik bir eşleşme seçebilirsiniz. Belirtik eşleşme, bir kanal belirli bir kuyruk yöneticisinden, belirli bir kuyruk yöneticisinden ya da belirli bir kullanıcı kimliğinden bağlantı kurmaya çalışırsa ve isteğe bağlı olarak, belirli bir DN içeren bir SSL/TLS kişisel sertifikasını sunmaya çalışırsa, hangi kanal kimlik doğrulama kaydının kullanılacağını size bildirir.

İlgili kavramlar

“Uzaktan ileti sistemine ilişkin güvenlik” sayfa 91
Bu bölümde, güvenlik ile uzaktan ileti sistemi konuları ele verilmektedir.

CHLAUTH ve CONNAUTH etkileşimi

Kanal doğrulama kayıtları (CHLAUTH) ve bağlantı kimlik doğrulaması (CONNAUTH), bir kanalda tek bir etkileşim durumunda IBM MQ' de etkileşimde bulunur.

Farklı bağ tanımları tipleri

IBM MQ , bir uygulamanın bağlanabilmesine ilişkin iki yöntemi destekler:

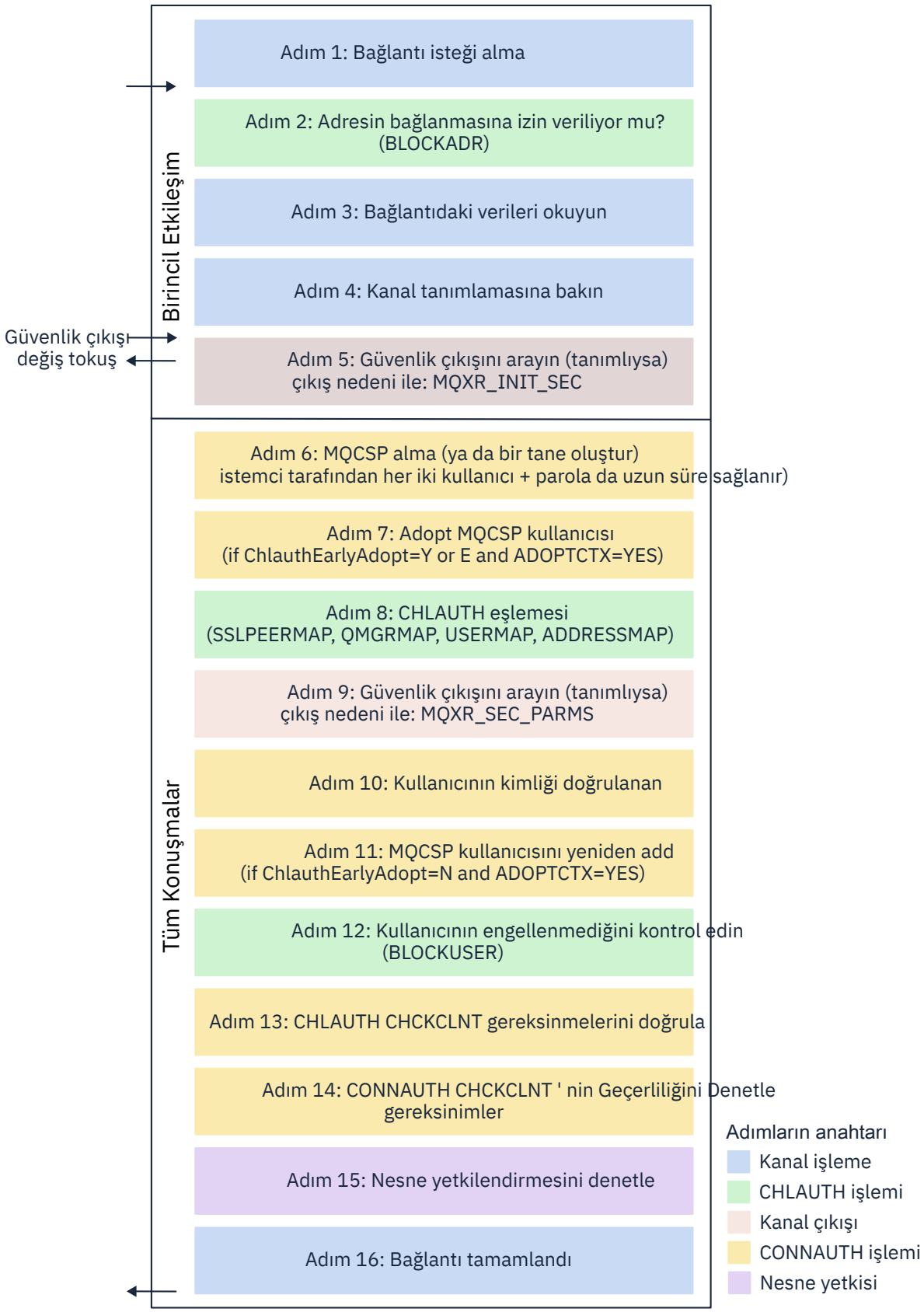
Yerel bağ tanımları
Uygulama ve kuyruk yöneticisi aynı işletim resminde olduğunda geçerlidir. CHLAUTH, bu tip uygulama bağlantılarıyla ilgili değildir.

İstemci bağ tanımları
Uygulama ve kuyruk yöneticisi, iletişim kurmak için ağı kullandığında geçerlidir. Uygulama ve kuyruk yöneticisi aynı makinede çalıştırılabilir ya da farklı makinelerde olabilir. IBM MQ' ta, bir istemci bağlantısı, bir sunucu bağlantısı (SVRCONN) kanalı biçiminde işlenir ve bu durumda, hem CONNAUTH hem de CHLAUTH geçerli olur.

Bir kanala alma uçunun bağlama adımları

Bir uygulama bir kuyruk yöneticisine bağlandığında, kanalın her iki ucunun da diğer ucun desteklendiğini anladığından emin olmak için önemli miktarda denetleme gerçekleştirilir. Kanalın giriş ucu, istemcinin bağlanmasına izin verildiğinden emin olmak için CHLAUTH ve CONNAUTH içeren bazı ek denetimin yanı sıra, bu işlemin sonucu etkileyebileceği gibi bir güvenlik çıkışı da içerebilir. Bu kanal bağlama aşaması, *bağ tanımlama aşaması*olarak da adlandırılır.

Aşağıdaki çizgede, bir SVRCONN kanalının sunucu ucu (kuyruk yöneticisinde) başlatıldığında geçeceği adımlar listelenmektedir:



Adım 1: Bağlantı isteği alma
Kanal başlatıcı ya da dinleyici, ağ üzerindeki bir yerden bir bağlantı isteği alır.

Adım 2: Adresin bağlanmasına izin veriliyor mu?
Herhangi bir veri okunmadan önce, IBM MQ , CHLAUTH kurallarına göre ortağın IP adresini, adresin *BLOCKADDR* kuralında olup olmadığını görmek için denetler. Adres bulunamazsa ve engellenmiş değilse, akış sonraki adıma geçer.

3. Adım: Kanaldan verileri okuyun
IBM MQ şimdi verileri bir arabelleğe okur ve gönderilen bilgileri işlemeye başlar.

4. Adım: Kanal tanımına bakın
İlk veri akışında, IBM MQ , diğer şeylerin yanı sıra, gönderme sonunun başlatılmaya çalıştığı kanalın adıdır. Alma kuyruk yöneticisi, kanal için belirtilen tüm ayarlara sahip olan kanal tanımlamasını arayabilirler.

Adım 5: Güvenlik çıkışını arayın (tanımlıysa)
Kanalın tanımlı bir güvenlik çıkışı (SCYEXIT) varsa, bu, çıkış nedeniyle çağrılır (MQCXP.**ExitReason**) MQXR_INIT_SEC değerine ayarlayın.

Adım 6: MQCSP alma
Gerekirse, kullanıcı kimliği ve parola istemci tarafından sağlandığı sürece, bir yapı oluşturun.

İstemci uyumluluk kipinde çalışan bir Java ya da JMS uygulamasıysa, istemci, kuyruk yöneticisine bir MQCSP yapısını geçirmez. Bunun yerine, uygulama bir kullanıcı kimliği ve parola sağladıysa, burada bir MQCSP yapısı oluşturulur.

Adım 7: Adopt MQCSP kullanıcısı (`ChlauthEarlyAdopt` *Y* ise ve ADOPTCX=YES ise)
İstemcinin doğrulanan kullanıcı kimliği doğrulanır.

CONNAUTH değeri, belirtilen ayırt edici adı kısa bir kullanıcı kimliğiyle eşlemek için LDAP kullanıyorsa, eşleme bu adımda gerçekleşir.

Kimlik doğrulaması başarılı olursa, kullanıcı kimliği kanal tarafından onaylanır ve CHLAUTH eşleme adımı tarafından kullanılır.

Not: From IBM MQ 9.0.4 the **`ChlauthEarlyAdopt=`** *E* parameter is automatically added to the channels stanza of the qm.ini file for new queue managers.

Adım 8: CHLAUTH eşlemesi
CHLAUTH önbelleği, *SSLPEERMAP*, *USERMAP*, *QMGRMAP*ve *AYRıNTıLAR*eşleme kurallarını aramak için yeniden incelendi.

Özellikle gelen kanalla eşleşen kural kullanılır. Kuralda **USERSRC***(KANAL)* ya da *(MAP)*varsa, kanal bağ tanımlamaya devam eder.

CHLAUTH kuralları **USERSRC***(NOACCESS)*ile bir kural değerlediyse, kimlik bilgileri daha sonra 9. adımda geçerli bir kullanıcı kimliği ve parolayla geçersiz kılınmadıkça, uygulama kanala bağlanmaktan engellenir.

Adım 9: Güvenlik çıkışını arayın (tanımlıysa)
Kanalın tanımlı bir güvenlik çıkışı (SCYEXIT) varsa, bu, çıkış nedeniyle çağrılır (MQCXP.**ExitReason**) MQXR_SEC_PARMS değerine ayarlayın.

MQCXP yapısının **`SecurityParms`** alanında MQCSP işaretçisi var olacaktır.

MQCSP yapısında kullanıcı kimliği (MQCSP.**`CSPUserIdPtr`**) için işaretçiler var. ve parola (MQCSP.**`CSPPasswordPtr`**).

Çıkışta kullanıcı kimliği ve parola değiştirilmek mümkündür. Aşağıdaki örnekte, bir güvenlik çıkışısının kullanıcı kimliği ve parola değerlerini denetleme günlüğüne nasıl yazdıracağı gösterilmektedir:

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

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

The exit can tell IBM MQ to close the channel, by returning *MQXCC_CLOSE_CHANNEL* in the MQCXP.**Exitresponse** alanı. Tersi durumda, kanal işleme, bağlantı doğrulama aşamasına devam eder.

Not: Belirtilen kullanıcı güvenlik çıkışı tarafından değiştirilirse, CHLAUTH eşleme kuralları yeni kullanıcıya yeniden uygulanmaz.

Adım 10: Kullanıcının kimliği doğrulanan

Kuyruk yöneticinde CONNAUTH etkinleştirildiyse, kimlik doğrulama aşaması olur.

Bunu denetlemek için, 'DISPLAY QMGR CONNAUTH' MQSC komutunu verin.

z/OS Aşağıdaki örnek, IBM MQ for z/OSüzerinde çalışan bir kuyruk yöneticisinden **DISPLAY QMGR CONNAUTH** komutunun çıktısını gösterir.

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

Multi Aşağıdaki örnekte, IBM MQ for Multiplatformsüzerinde çalışan bir kuyruk yöneticisinden '**DISPLAY QMGR CONNAUTH**' komutunun çıktısı gösterilmektedir.

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

CONNAUTH değeri, bir **AUTHINFO** IBM MQ nesnesinin adıdır.

İşletim sistemi kimlik doğrulaması olarak (**AUTHTYPE**(*IDPWOS*)) hem IBM MQ for Multiplatforms , hem de IBM MQ for z/OSüzerinde geçerlidir; örnekler, işletim sistemi kimlik doğrulamasını kullanır.

z/OS Aşağıdaki örnek, IBM MQ for z/OSüzerinde çalışan bir kuyruk yöneticisinden **AUTHTYPE**(*IDPWOS*) için gönderilen varsayılan nesneyi göstermektedir.

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

Multi Aşağıdaki örnek, IBM MQ for Multiplatformsüzerinde çalışan bir kuyruk yöneticisinden **AUTHTYPE**(*IDPWOS*) için gönderilen varsayılan nesneyi göstermektedir.

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

AUTHTINFO TYPE (IDPWOS), CHCKCLNTadlı bir özniteliğe sahiptir. Değer *REQUIREND* olarak değiştirilirse, tüm istemci uygulamalarının geçerli bir kullanıcı kimliği ve parolası belirtmesi gerekir.

If the user was authenticated in Step 7, the user will not be authenticated again unless the user or password in the SecurityParms field of the MQCXP structure was changed by a security exit in Step 9.

Adım 11: MQCSP kullanıcısının bağlamını seçin (`ChlauthEarlyAdopt=`*N* ve ADOPTCX=YES ise)
You can set the ADOPTCTX attribute, which controls whether the channel runs under MCAUSER, or the user ID the application has supplied.

If the user ID asserted in the MQCSP, or **`SecurityParms`** field of the MQXCP structure, has been successfully authenticated and **ADOPTCTX** is *EVET*, then the context of the user resulting from steps 7 and 8 is adopted as the context to use for this application, unless the user or password in the **`SecurityParms`** field of the MQCXP structure was changed by a security exit in step 9.

Bu değerlendirilen kullanıcı kimliği, IBM MQ kaynaklarını kullanmak için yetki verilen kullanıcı kimliğidir.

Örneğin, SVRCONN kanalında bir MCAUSER ayarınız yok ve istemcinizin Linux makinenizdeki '`johndoe`' altında çalışıyor olması gerekir. Uygulamanız, MQCSP 'de'`fred`'kullanıcısını belirtiyor, böylece kanal etkin MCAUSER olarak'`johndoe`' ile çalışmaya başlıyor. CONNAUTH denetinden sonra, '`fred`' kullanıcısı benimsenir ve kanal etkin MCAUSER olarak '`fred`' ile çalışır.

Adım 12: Kullanıcının engellenmediğini kontrol edin (BLOCKUSER)
CONNAUTH denetimi başarılı olursa, CHLAUTH önbelleği, etkin MCAUSER ' in bir *BLOCKUSER* kuralı tarafından engellenmiş olup olmadığını denetlemek için yeniden incelenir. Kullanıcı engellenirse, kanal sona erer.

Step13: CHLAUTH CHCKCLNT gereksinmelerini doğrula
8 adımında seçilen CHLAUTH kuralı, ek olarak REQUIRES ya da REQDADM için CHCKCLNT değerini belirtiyorsa, gereksinimin karşılanması için geçerli bir CONNAUTH kullanıcı kimliği sağlandığından emin olmak için geçerlilik denetimi yapılır.

- If CHCKCLNT(REQUIRED) is set a user must have been authenticated in step 7 or 10. Tersi durumda, bağlantı reddedilir.
- If CHCKCLNT(REQDADM) is set a user must have been authenticated in step 7 or 10 if this connection is determined to be privileged. Tersi durumda, bağlantı reddedilir.
- CHCKCLNT (ASQMGR) ayarlandıysa, bu adım atlanır.

Notlar:

1. CHCKCLNT (REQUIRES) ya da CHCKCLNT (REQDADM) değeri ayarlandıysa, ancak kuyruk yöneticisinde CONNAUTH etkinleştirilmediyse, yapılanıştaki çakışma nedeniyle bir MQRC_SECURITY_ERROR (2063) dönüş kodu ile bağlantı başarısız olur.
2. Kullanıcı bu adımda yeniden kimlik doğrulaması gerçekleştirmiyor.

Adım 14: CONNAUTH CHCKCLNT gereksinimlerinin geçerliliğini denetleyin.
Kuyruk yöneticinde CONNAUTH etkinleştirildiyse, kimlik doğrulama aşaması olur.

Gelen bağlantılar için hangi gereksinimlerin belirlendiğini belirlemek için CONNAUTH CHCKCLNT değeri denetlenir.

- CHCKCLNT (NONE) ayarlandıysa, bu adım atlanır
- CHCKCLNT (isteğe bağlı) ayarlandıysa, bu adım atlanır.
- If CHCKCLNT(REQUIRED) is set then a user must have been authenticated in step 7 or 10. Tersi durumda, bağlantı reddedilir.
- If CHCKCLNT(REQDADM) is set a user must have been authenticated in step 7 or 10 if this connection is determined to be privileged. Tersi durumda, bağlantı reddedilir.

Not: Kullanıcı bu adımda yeniden kimlik doğrulaması gerçekleştirmiyor.

Multi **Adım 15: Nesne onayının denetlenmesi**
Etkin MCAUSER ' in kuyruk yöneticisine bağlanmak için uygun yetkiye sahip olduğundan emin olmak için bir onay imi yapılır.

ULW Ek bilgi için Object Authority Managerbaşlıklı konuya bakın.

IBM i Daha fazla bilgi için bkz. “IBM iüzerinde nesne yetkisi yöneticisi” sayfa 148.

Adım 16: Bağlantı tamamlanır
Önceki adımlar başarıyla tamamlanırsa, bağlantı tamamlanır.

İlgili kavramlar
CONNAUTH
Bir kuyruk yöneticisi, kullanıcının kaynaklara erişim yetkisinin olup olmadığını denetlemek için, sağlanan bir kullanıcı kimliğini ve parolasını kullanacak şekilde yapılandırılabilir.

İlgili başvurular
CHLAUTH KüMESI
ALTER AUTHINFO

CHLAUTH erişim sorunlarını çözme
Kanal kimlik doğrulama kayıtlarını (CHLAUTH) kullanırken belirli erişim sorunlarını nasıl çözeceğinize ilişkin öneriler.

Varsayılan CHLAUTH kuralları

CHLAUTH işlemesi için üç varsayılan kural vardır:

- `MQ-admin*` kullanıcıları tarafından tüm kanallara ERIşIM YOK
- TüM SISTEMLERE ERIşIM YOK. * tüm kullanıcılar tarafından kanallar
- SYSTEM.ADMIN.SVRCONN kanalı (`MQ-admin` dışı kullanıcılar)

İlk iki kural tüm kanallara erişimi engeller. Üçüncü kural daha spesifiktir ve bu nedenle kanal SYSTEM.ADMIN.SVRCONN kanalı, bu kanalda erişime izin verir.

Ortak bağlantı hataları

CHLAUTH kuralları, bir kanalın başlatılıp başlatılamayacağını belirlemek için kullanılır ve MCAUSER aracılığıyla başka bir kullanıcı kimliğiyle eşlemeye izin verir. Kanal başlatılamazsa, genellikle aşağıdaki hatalar oluşur:

- RC 2035 MQRC_NOT_AUTHORIZED
- RC 2059 MQRC_Q_MGR_NOT_KULLANILAMIYOR
- AMQ4036 Erişimi yok
- AMQ9776: Kanal kullanıcı kimliği tarafından engellendi
- AMQ9777: Kanal engellendi
- MQJE001: Bir MQException oluştu: Tamamlanma Kodu 2, Neden 2035
- MQJE036: Kuyruk yöneticisi bağlantı girişimini reddetti

Erişimi kesin olarak engellemeli ve kanallara kimlerin erişebileceğini ve kanalları başlatabileceğini denetlemek için daha fazla CHLAUTH kuralı eklemelisiniz. Geçici bir önlem olarak ve listelenen hataları gidermek için şunları yapabilirsiniz:

- “CHLAUTH kurallarını devre dışı bırak” sayfa 58
- “CHLAUTH kurallarını değiştir ya da kaldır” sayfa 59

CHLAUTH kurallarını devre dışı bırak

Geçici bir önlem olarak ve yukarıdaki hataları gidermek için CHLAUTH kurallarını devre dışı bırakabilirsiniz. Kurallar herhangi bir zamanda yeniden etkinleştirilebilir ve CHLAUTH kurallarının devre dışı bırakılması bağlantı sorununu çözerse, bunun nedeni olduğunu bilirsiniz.

CHLAUTH kurallarını devre dışı bırakmak için aşağıdaki komutu verin:

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

CHLAUTH ' yi *WARN*olarak ayarlayabileceğinizi unutmayın; bu, kuralın erişimine izin verir ve bunun sonucunu günlüğe kaydeder.

CHLAUTH kurallarını değiştir ya da kaldır

CHLAUTH kuralını ya da kurallarını silebilir ya da değiştirebilirsiniz; bu da sorununuza neden olur.

Bir CHLAUTH kuralını değiştirmek için, SET CHLAUTH komutunu ACTION (REPLACE) ile kullanın. Örneğin, herhangi bir MQ-admin kullanıcısının engellenmek yerine tüm kanallara erişmesine neden olmayan varsayılan kuralı değiştirmek için şu komutu verin:

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

Bir CHLAUTH kuralını silmek için, SET CHLAUTH komutunu ACTION (REMOVE) ile birlikte kullanırsınız. Örneğin, herhangi bir MQ-admin kullanıcısının tüm kanallara erişmesine neden olmayan varsayılan kuralı silmek için aşağıdaki komutu verin:

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

MATCH (RUNCHECK) kullanılarak erişim sınanıyor

CHLAUTH kurallarınızın sonucunu, runmqsc içindeki CHLAUTH kuralının MATCH (*RUNCHECK*) seçeneğini kullanarak sınayabilirsiniz. **MATCH** (*RUNCHECK*) seçeneği, bu kanal bu kuyruk yöneticisine bağlanıyorsa, yürütme sırasında belirli bir gelen kanal tarafından eşleştirilen kaydı döndürür. Aşağıdakileri sağlamanız gerekir:

- Kanal adı
- ADDRESS özniteliği
- SSLPEER özniteliği, yalnızca gelen kanal SSL ya da TLS kullanıyorsa
- QMNAME, gelen kanal bir kuyruk yöneticisi kanalıysa, ya da
- CLNTUSER özniteliği, gelen kanal bir istemci kanalıysa

Aşağıdaki örnek, varsayılan kurallar geçerli olan CHLAUTH kuralını denetler ve MQ-admin kullanıcı johndoe CHAN1adlı bir kanala erişmesiyle sonuçlanır:

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

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

johndoekullanıcısı için kanal çalışmaz, *MQADMIN kullanıcıları için BLOCKUSER kuralı nedeniyle kullanıcı engellenir.

Aşağıdaki örnek, varsayılan kurallarla birlikte hangi CHLAUTH kuralının alice MQ-admin kullanıcısı olmayan bir kullanıcının CHAN1adlı bir kanala erişmesiyle sonuçlandığını denetler:

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

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

alicekullanıcısı için, kanal çalışır ve kanal alice MCAUSER olarak geçer. MCAUSER, IBM MQ nesne yetkilerini denetlemek için kullanılan kullanıcı kimliğidir.

İlgili başvurular
CHLAUTH AYARLA
CHLAUTH 'U GöRüNTüLE

Kullanıcılar için yeni CHLAUTH kuralları yaratılması
Kullanıcılar için bazı genel senaryolar ve bunları gerçekleştirmek için CHLAUTH kuralları verilebilir.

Bu konuda aşağıdaki senaryolar yer alır:

- “Belirli MQ-admin kullanıcıları için erişimi denetleme” sayfa 60
- “Belirli bir kullanıcı ve IBM MQ istemci uygulaması için erişimi denetleme” sayfa 61
- “O kullanıcının sertifika ayırt edici adını (DN) kullanarak belirli bir kullanıcı için erişimi denetleme” sayfa 61
- “Belirli bir kullanıcının mqm kullanıcısıyla eşlenmesi” sayfa 62

Belirli MQ-admin kullanıcıları için erişimi denetleme

For this scenario, setup a server connection channel that is to be exclusively used for an administrative perspective, that is, to connect from IBM MQ Explorer. You have a specific channel for this usage, and defined IP address, or addresses, from where you want connections to be accepted, and access blocked for the `'mqm'` ID, if the connection is not from one of the specified IP addresses.

IBM MQ Explorer için bir SVRCONN kanalı ve `ADMIN.CHAN`adı verilen `MQ-admin` kullanıcıları yapın:

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

Test için, `MQ-admin` grubunda tanımlı bir kullanıcı tanımlı olduğundan ve olmayan bir kullanıcıyla sahip olduğundan emin olun. Bu senaryoda `mqadm` , `MQ-admin` grubunda yer alıyor ve `alice` bu durumda değil.

Varsayılan CHLAUTH kuralları yer alıyor. Belirli bir kullanıcının ADMIN.CHAN belirli IP adreslerinden `MQ-admin` olarak:

- Herhangi bir adresten ACCESS ' i ayarla
- Set BLOCKUSER for this channel to only block user nobody, which overrides the *MQADMIN BLOCKUSER
- ALLOW access to user `mqadm` on a specific subnet of addresses, and MAP to `mqadm` user authority

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

At this point, the user `mqadm` can access and start the ADMIN.CHAN channel, from the specified IP address range.

Aşağıdaki komutların her birinin sonuçlarını görmek için, istediğiniz zaman MATCH (RUNCHECK) komutunu çalıştırabilirsiniz:

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

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

```
CHLAUTH(ADMIN.CHAN) TYPE(ADDRESSMAP)
ADDRESS(*) USERSRC(NOACCESS)
```

Bu noktada, yalnızca CHLAUTH kaydına sahip olan kullanıcıların ADMIN.CHAN' u kullanarak erişmesine izin verilir.

Belirli bir kullanıcı ve IBM MQ istemci uygulaması için erişimi denetleme

Bu senaryoda, varsayılan CHLAUTH kuralları yeterli olur; IBM MQ yetkisinin belirli bir kullanıcı için ayarlanması gerektiği varsayılarak, doğru IBM MQ yetkisi (setmqautkullanılarak) sağlanmalıdır.

Bu senaryoda, yetkiler `MQ-admin` kullanıcısı olmayan bir kullanıcı `mqapp1`için ayarlıdır. Bir SVRCONN kanalı yapın, APP1.CHAN, belirli bir uygulama ve belirli bir kullanıcı tarafından kullanılmak üzere.

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

With the Varsayılan CHLAUTH kuralları in place, user `mqapp1` can start the APP1.CHAN channel.

The user Id coming from the IBM MQ client application is used for IBM MQ object authority checking. Bu durumda, 'mqapp1' kullanıcısının IBM MQ istemci uygulamasını çalıştırıyor olduğunu varsayarsak, bu, IBM MQ nesne yetkisi denetimi için kullanılır. Bu nedenle, `mqapp1` ' in uygulama gereksinimlerinin IBM MQ nesnelerine erişimi varsa, her şey iyi olur; yetki hataları almıyorsa.

`mqapp1` kullanıcı kimliği için belirli CHLAUTH kuralları yaratarak güvenliği daha da artırabilirsiniz; ancak, varsayılan kurallar altında, `MQ-admin` grubunun hiçbir üyesi bu kanala erişemez.

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

O kullanıcının sertifika ayırt edici adını (DN) kullanarak belirli bir kullanıcı için erişimi denetleme

Bu senaryoda, kullanıcının kuyruk yöneticisine akıtılan bir sertifikasına sahip olması gerekir. Daha sonra, DN CHLAUTH kuralının SSLPEER ayarına göre eşleştirilir ve SSLPEER genel arama karakterlerini kullanabilir.

Eşleştirilirse, kullanıcı IBM MQ nesne yetkilerini denetlemek amacıyla farklı bir MCAUSER ile de eşlenebilir. MCAUSER ' un eşlenmesi, IBM MQ nesne yetkisi yöneticisinde (OAM) yönetilmesi gereken kullanıcı sayısını en aza indirebilir.

Kullanımda sertifikalar olan bir TLS kanalınız var ve aşağıdaki kurallara gerek duyuyorsunuz:

- Belirli bir kanala ilişkin tüm kullanıcıları engelle
- Yalnızca belirli bir SSLPEER ' e sahip kullanıcıların IBM MQ OAM erişimi için o kullanıcının istemcisini kullanan kullanıcılara izin verin.

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

Kanala bağlanan istemci kullanıcı kimliği, IBM MQ nesnelerinin IBM MQ OAM yetkisi için kullanılır; bu nedenle, kullanıcı kimliğinin uygun IBM MQ yetkilerine sahip olması gerekir.

Aşağıdakileri kullanarak farklı bir IBM MQ kullanıcı kimliğiyle eşleyebilirsiniz:

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

(USERSRC(CHANNEL)yerine).

Belirli bir kullanıcının mqm kullanıcısıyla eşlenmesi

Bu, “Belirli MQ-admin kullanıcıları için erişimi denetleme” sayfa 60' a eklenen bir ekleme ya da değişikliktir.

Belirli kullanıcıları mqm kullanıcısına ya da IBM MQ OAM olanağında IBM MQ nesne yetkisi kuruluşuna sahip bir MQ-admin kullanıcı kimliği ile eşlemek için aşağıdaki CHLAUTH kuralını ekleyin.

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

This allows and maps the johndoe user over to the mqm user for the particular channel ADMIN.CHAN.

İlgili kavramlar

“CHLAUTH erişim sorunlarını çözme” sayfa 58
Kanal kimlik doğrulama kayıtlarını (CHLAUTH) kullanırken belirli erişim sorunlarını nasıl çözeceğinize ilişkin öneriler.

“Kanallar için yeni CHLAUTH kuralları yaratılması” sayfa 62
Kendi CHLAUTH kurallarınızı yaratmanıza yardımcı olmak için, burada kanallar için bazı ortak senaryolar ve bunları gerçekleştirmek için CHLAUTH kuralları örneği verilebilir.

İlgili başvurular

CHLAUTH KüMESI

CHLAUTH GÖRÜNTÜLE

Kanallar için yeni CHLAUTH kuralları yaratılması
Kendi CHLAUTH kurallarınızı yaratmanıza yardımcı olmak için, burada kanallar için bazı ortak senaryolar ve bunları gerçekleştirmek için CHLAUTH kuralları örneği verilebilir.

Bu konuda aşağıdaki senaryolar yer alır:

- “Belirli bir kanala yalnızca belirli bir IP adresi aralığından erişime izin verin.” sayfa 62
- “Belirli bir kanal için, tüm kullanıcıları engelle, ancak belirli kullanıcıların bağlanmasına izin verin.” sayfa 63
- “Alıcı ve gönderen kanalları için CHLAUTH kullanılması” sayfa 63

Belirli bir kanala yalnızca belirli bir IP adresi aralığından erişime izin verin.

Bu senaryo için şunları yapmak istiyorsunuz:

- Herhangi bir yerden kanala erişim izni yok
- Belirli bir IP adresi ya da adres aralığından erişime izin ver

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

Bu, yalnızca APP2.CHAN kanalı, bağlantı belirlenen belirli bir IP adresi aralığından geldiğinde başlatılacak.

MCAUSER olarak bağlanan kullanıcı mqapp2ile eşlenir ve bu nedenle, o kullanıcı için IBM MQ OAM yetkisi alır.

Belirli bir kanal için, tüm kullanıcıları engelle, ancak belirli kullanıcıların bağlanmasına izin verin.

For this scenario, the access to the channel MY.SVRCONN has the Varsayılan CHLAUTH kuralları in place.

Aşağıdaki bilgileri eklemeniz gerekir:

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

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

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

This first part of the code blocks anyone from connecting on MY.SVRCONN, then the code allows only the MY.SVRCONN channel to be started when the connection comes from the specific user Id `johndoe`.

The user connecting on the channel `johndoe` is used for the IBM MQ OAM authority of IBM MQ objects. Bu nedenle, kullanıcı kimliğinin uygun IBM MQ yetkilerine sahip olması gerekir.

Aşağıdakileri kullanarak farklı bir IBM MQ kullanıcı kimliğiyle eşleyebilirsiniz:

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

(`USERSRC(CHANNEL)` yerine).

Alıcı ve gönderen kanalları için CHLAUTH kullanılması

Alıcı kanalına erişimi kısıtlamak için, alıcı ve gönderen kanallarına ek güvenlik eklemek için CHLAUTH kurallarını kullanabilirsiniz. CHLAUTH kurallarında değişiklik ekliyorsanız ya da değişiklik yapıyorsanız, güncellenen CHLAUTH kuralları yalnızca kanal başlatılırken geçerli olur; bu nedenle, kanallar zaten çalışıyorsa, CHLAUTH güncellemelerinin geçerli olması için bunları durdurmanız ve yeniden başlatmanız gerekir.

CHLAUTH kuralları herhangi bir kanalda kullanılabilir, ancak bazı kısıtlamalar vardır. Örneğin, USERMAP kuralları yalnızca SVRCONN kanalları için geçerlidir.

Bu örnek, yalnızca belirli bir IP adresinden, TO.MYSVR1 kanalı:

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

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

Bu örnek, yalnızca belirli bir kuyruk yöneticisinden bağlantıya izin verir:

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

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

İlgili kavramlar

“CHLAUTH erişim sorunlarını çözme” sayfa 58

Kanal kimlik doğrulama kayıtlarını (CHLAUTH) kullanırken belirli erişim sorunlarını nasıl çözeceğinize ilişkin öneriler.

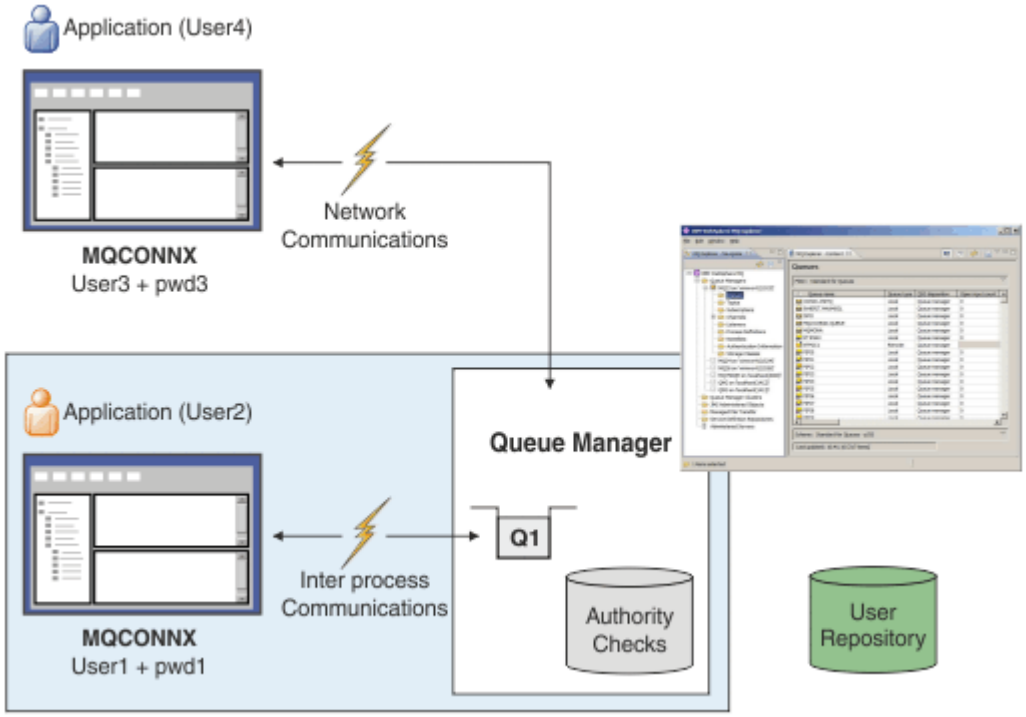
"Kullanıcılar için yeni CHLAUTH kuralları yaratılması" sayfa 60
Kullanıcılar için bazı genel senaryolar ve bunları gerçekleştirmek için CHLAUTH kuralları verilebilir.

İlgili başvurular
CHLAUTH KüMESI
CHLAUTH GÖRÜNTÜLE

Bağlantı kimlik doğrulaması

Bağlantı kimlik doğrulaması çeşitli şekillerde gerçekleştirilebilir:

- Bir uygulama, bir kullanıcı kimliği ve parola sağlayabilir. Uygulama bir istemci olabilir ya da yerel bağ tanımlarını kullanabilir.
- Bir kuyruk yöneticisi, sağlanan bir kullanıcı kimliği ve parola üzerinde işlem yapmak üzere yapılandırılabilir.
- Bir havuz, bir kullanıcı kimliği ve parola birleşiminin geçerli olup olmadığını belirlemek için kullanılabilir.



Çizgede, iki uygulama bir kuyruk yöneticisiyle bağlantılar, bir uygulama istemci olarak ve biri yerel bağ tanımları kullanılarak bağlantı sağlar. Uygulamalar, kuyruk yöneticisine bağlanmak için çeşitli API ' ler kullanabilir, ancak tümü bir kullanıcı kimliği ve parola sağlayabilme yeteneğine sahiptir. The user ID that the application is running under, `User2` and `User4` in the diagram, which is the usual operating system user ID presented to IBM MQ, might be different from the user ID provided by the application, `User1` and `User3`.

Kuyruk yöneticisi yapılanış komutlarını alır (çizgede, IBM MQ Explorer kullanılıyor) ve kaynakların açıldığını yönetir ve bu kaynaklara erişim yetkisi verir. IBM MQ ' da bir uygulamanın erişim yetkisi gerektiren birçok farklı kaynak vardır. Çizge, çıkış için bir kuyruk açılmasını gösterir, ancak aynı ilkeler diğer kaynaklar için de geçerlidir.

Kullanıcı kimliklerini ve parolaları denetlemek için kullanılan havuzla ilgili ayrıntılar için Kullanıcı havuzları başlıklı konuya bakın.

İlgili kavramlar

“Bağlantı kimlik doğrulaması: Yapılandırma” sayfa 65
Bir kuyruk yöneticisi, kullanıcının kaynaklara erişim yetkisinin olup olmadığını denetlemek için, sağlanan bir kullanıcı kimliğini ve parolasını kullanacak şekilde yapılandırılabilir.

“Bağlantı kimlik doğrulaması: Uygulama değişiklikleri” sayfa 69

“Bağlantı kimlik doğrulaması: Kullanıcı havuzları” sayfa 70
Kuyruk yöneticilerinizin her biri için, kullanıcı kimliklerini ve parolaları doğrulamak üzere farklı tiplerde kimlik doğrulama bilgileri nesnesi seçebilirsiniz.

Bağlantı kimlik doğrulaması: Yapılandırma

Bir kuyruk yöneticisi, kullanıcının kaynaklara erişim yetkisinin olup olmadığını denetlemek için, sağlanan bir kullanıcı kimliğini ve parolasını kullanacak şekilde yapılandırılabilir.

Kuyruk yöneticiliklerinde bağlantı doğrulamasının açılması

Bir kuyruk yöneticisi nesnesinde, **CONNAUTH** özniteliği bir kimlik doğrulama bilgisi (AUTHINFO) nesnesi adı olarak ayarlanabilir. Bu nesne iki tipten biri olabilir (AUTHTYPE özniteliği):

IDPWOS
Kuyruk yöneticisinin kullanıcı kimliği ve parolanın kimliğini doğrulamak için yerel işletim sistemini kullandığını gösterir.

IDPWLDAP
Kuyruk yöneticisinin kullanıcı kimliği ve parolayı doğrulamak için bir LDAP sunucusu kullandığını gösterir.

Not: CONNAUTH alanında başka bir kimlik doğrulama bilgisi nesnesi türünü kullanamazsınız.

IDPWOS ve IDPWLDAP , burada açıklanan özniteliklerine benzer bir sayıyla benzerdir. Diğer öznitelikler daha sonra dikkate alınır.

Yerel bağlantıları denetlemek için, **CHCKLOCL** AUTHINFO özniteliğini kullanın (yerel bağlantıları denetleyin). İstemci bağlantılarını denetlemek için, **CHCKCLNT** AUTHINFO özniteliğini kullanın (istemci bağlantılarını denetleyin). Kuyruk yöneticisinin değişiklikleri tanıması için yapılandırmanın yenilenmesi gerekir.

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

Burada USE . PW , AUTHOINFO tanımlamasıyla eşleşen bir dizgidir.

Hem **CHCKLOCL** hem de **CHCKCLNT** , denetimlerin geçersiz kılınmasına izin veren olası değerler kümesini de içerir:

YOK
Anahtarlar denetleyerek kapatılıyor.

İsteğe Bağlı
Bir uygulama tarafından bir kullanıcı kimliği ve parola sağlansa, bunlar geçerli bir çifttir, ancak bunları sağlamanın zorunlu olmadığını doğrular. Bu seçenek, geçiş sırasında yararlı olabilir. Örneğin,

Önemli: İSTIKLE , daha sıkı CHLAUTH kurallarını kullanmak için ayarlanabileceğiniz en düşük değerdir.

YOK seçeneğini belirlerseniz ve istemci bağlantısı CHCKCLNT GEREKLI (ya da z/OSdışındaki altyapılarda REQDADM) ile CHLAUTH kayıtlarıyla eşleşirse, bağlantı başarısız olur. You receive message AMQ9793 on platforms other than z/OS, and message CSQX793E on z/OS.

ZORUNLU
Tüm uygulamaların geçerli bir kullanıcı kimliği ve parola belirtmesini gerektirir. Aşağıdaki nota da bakın.

REQDADM
Ayrıcalıklı kullanıcılar geçerli bir kullanıcı kimliği ve parola sağlamalı, ancak ayrıcalıklı olmayan kullanıcılara OPTIONAL (İsteğe bağlı) ayarında olduğu gibi davranılır. Aşağıdaki nota da bakın.

z/OS (Bu ayarın z/OS sistemlerinde kullanılmasına izin verilmez.)

Not:

Setting **CHCKLOCL** to GEREKLI or REQDADM means that you cannot locally administer the queue manager by using **runmqsc** (error AMQ8135: Not authorized) unless the user specifies the -u UserId parameter on the **runmqsc** command line. Bu kümeyle, **runmqsc** , konsolda kullanıcının parolasını ister.

Similarly, a user running IBM MQ Explorer on the local system will see error AMQ4036 when attempting to connect to the queue manager. Bir kullanıcı adı ve parola belirtmek için, yerel kuyruk yöneticisi nesnesini farenin sağ düğmesiyle tıklatın ve **Bağlantı Ayrıntıları** > **Özellikler ...**öğelerini seçin. öğesini seçin. **Kullanıcı Kimliği** bölümünde, kullanılacak kullanıcı adını ve parolayı girin ve ardından **Tamam**seçeneğini tıklatın.

Benzer konular, **CHCKCLNT**ile uzak bağlantılar için de geçerlidir.

CONNAUTH is blank for migrated queue managers but set to *SYSTEM.DEFAULT.AUTHINFO.IDPWOS* for new queue managers. Önceki **AUTHINFO** tanımında **CHCKCLNT** varsayılan olarak *REQDADM* değerine ayarlanmış olmalıdır.

Bu nedenle, bağlantı kurmak için ayrıcalıklı bir kullanıcı kimliği kullanarak, var olan tüm istemciler için doğru işletim sistemi parolasını sağlamanız gerekir.

Uyarı: Bazı durumlarda, istemci uygulaması için bir MQCSP yapısındaki parola, düz metindeki bir ağ üzerinden gönderilir. İstemci uygulaması parolalarının uygun şekilde korunmasını sağlamak için bkz. “MQCSP parola koruması” sayfa 28.

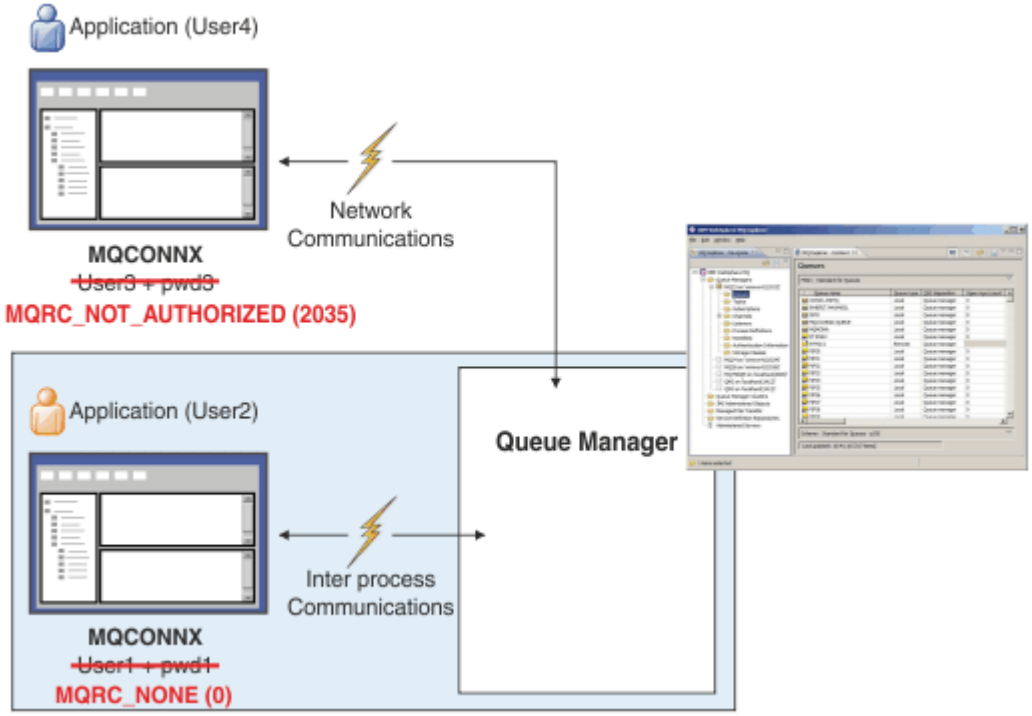
Yapılandırma ayrıntı düzeyi

In addition to **CHCKLOCL** and **CHCKCLNT** that are used to turn on user ID and password checking, there are enhancements to the CHLAUTH rules so that more specific configuration can be made using **CHCKCLNT**.

Genel **CHCKCLNT** değerini OPTIONALolarak ayarlayabilir ve daha sonra, CHLAUTH kuralıyla **CHCKCLNT** ayarını REQUIREMENT ya da REQDADM olarak ayarlayarak belirli kanallar için daha sıkı bir değer belirleyebilirsiniz. Varsayılan olarak, CHLAUTH kuralları CHCKCLNT(ASQMGR) ile çalıştırılır; böylece bu ayrıntı düzeyi kullanılmayacak. Örneğin:

```
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)
```

Hata bildirimi



Bir uygulama gerektiğinde kullanıcı kimliği ve parola sağlamıyorsa ya da isteğe bağlı olduğunda da yanlış bir birleşim sağladıysa hata kaydedilir.

Not: Parola denetimi kapatıldığında, **CHCKLOCL** ya da **CHCKCLNT**üzerinde NONE seçeneği kullanılarak geçersiz parolalar saptanmaz.

Başarısız kimlik doğrulamaları, hata uygulamaya geri döndürülmeden önce **FAILDLAY** özniteliği tarafından belirtilen saniye sayısı için tutulur. Bu, bir uygulamadan sürekli olarak bağlanmaya çalışılan bir uygulamadan koruma sağlar.

Bu hata çeşitli yollarla kaydedilir:

Uygulama
Uygulama standart IBM MQ güvenlik hatası döndürdü: RC2035 -MQRC_NOT_YETKILI.

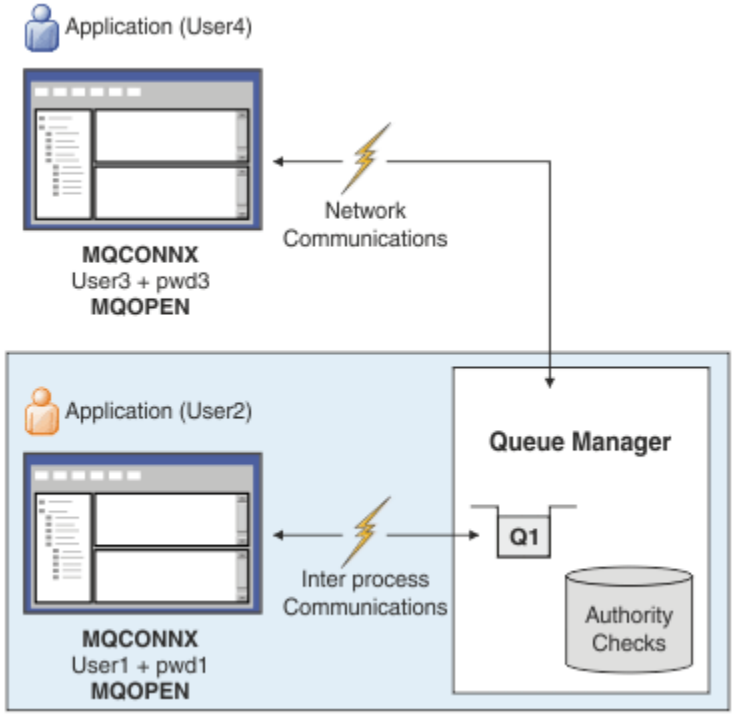
Sistem yöneticisi
Bir IBM MQ yöneticisi, hata günlüğünde bildirilen olayı görür ve bu nedenle, kullanıcı kimliği ve parola denetlemeyi başarısız olduğundan uygulamanın reddedildiğini görebilir; örneğin, bağlantı yetkisi yok.

İzleme aracı
A monitoring tool can also be notified of the failure, if you turn on authority events by sending an event message to the SYSTEM.ADMIN.QMGR.EVENT queue:

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

Bu "Yetkili Değil" olayı, bir Tip 1 bağlantı olayıdır ve diğer Tip 1 olaylarıyla, ek bir alana, sağlanan MQCSP kullanıcı kimliğine aynı alanları sağlar. Olay iletisinde parola verilmemiş. Bu, olay iletisinde iki kullanıcı kimliği olduğu anlamına gelir: Uygulamanın altında çalıştığı kimlik ve uygulamanın kullanıcı kimliği ve parola denetimi için sunduğu tanıtıcı.

Yetkilendirme ile ilişki



Bir kuyruk yöneticisini, uygulamanın çalışmakta olduğu kullanıcı kimliği olarak, kullanıcı kimliklerinin ve parolaların belirli uygulamalar tarafından sağlandığını zorunlu kılacak bir kuyruk yöneticisi yapılandırabilirsiniz; örneğin, uygulama çıkış kuyruğu açtığında, uygulama tarafından sunulan kullanıcı kimliği aynı olmayabilir; örneğin:

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

Kullanıcı kimliklerinin ve parolaların nasıl işlendiği, kimlik doğrulama bilgileri nesnesindeki **ADOPTCTX** özniteliği tarafından denetlenir.

ADOPTCTX (EVET)
Bir uygulamaya ilişkin tüm yetki denetimleri, bağladığınız kullanıcı kimliğiyle, bağlantının ömrünün sonuna kadar bağlamı uygulama bağlamı olarak kabul etmek için seçilerek, parola ile doğrulamandığınız kullanıcı kimliğiyle yapılır.

Uyarı: ADOPTCTX (YES) ve OS kullanıcı Ids 'i kullanırken, benimsenmekte olan kullanıcı kimliğinin kullanıcı kimliklerinin uzunluk üst sınırını aşmadığından emin olmanız gerekir. Ek bilgi için “Kullanıcı Kimlikleri” sayfa 79 başlıklı konuya bakın.

ADOPTCTX (NO)
Bir uygulama, bağlantı sırasında kimlik doğrulaması yapmak amacıyla bir kullanıcı kimliği ve parola sağlar, ancak daha sonra, uygulamanın gelecekteki yetkilendirme denetimleri için altında çalıştığı kullanıcı kimliği kullanılarak devam eder. Geçiş sırasında bu seçeneği yararlı bulabilir ya da kanal doğrulama kayıtları gibi başka mekanizmaları kullanmayı planlıyorsanız, ileti kanalı aracısı kullanıcı kimliği (MCAUSER)atamak için kullanılır.

Uyarı:

Bir kimlik doğrulama bilgileri nesnesinde **ADOPTCTX(YES)** parametresini kullandığınızda, `qm.ini` dosyasının kanal kısmında **ChlauthEarlyAdopt** parametresini ayarlamadığınız sürece başka bir güvenlik bağlamı benimsenemez.

For example, the default authentication information object is set to **ADOPTCTX(YES)**, and the user `fred` is logged in. Aşağıdaki iki CHLAUTH kuralı yapılandırılıyor:

```
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)
```

The following command is issued, with the intention of authenticating the command as the adopted security context of the user `bob`:

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

In fact, the queue manager uses the security context of `fred`, not `bob`, and the connection fails.

ChlauthEarlyAdoptile ilgili daha fazla bilgi için bkz. Kanal stanza öznitelikleri.

İlgili kavramlar

“Bağlantı kimlik doğrulaması” sayfa 64

“Bağlantı kimlik doğrulaması: Uygulama değişiklikleri” sayfa 69

“Bağlantı kimlik doğrulaması: Kullanıcı havuzları” sayfa 70
Kuyruk yöneticilerinizin her biri için, kullanıcı kimliklerini ve parolaları doğrulamak üzere farklı tiplerde kimlik doğrulama bilgileri nesnesi seçebilirsiniz.

Bağlantı kimlik doğrulaması: Uygulama değişiklikleri

Bir uygulama, MQCONNX çağrıldığında, bağlantı güvenliği değiştirgeleri (MQCSP) yapısı içinde bir kullanıcı kimliği ve parola sağlayabilir. Kullanıcı kimliği ve parola, kuyruk yöneticisiyle birlikte sağlanan nesne yetkisi yöneticisi (OAM) ' ı denetleyerek ya da z/OS sistemlerinde kuyruk yöneticisiyle birlikte sağlanan yetki hizmeti bileşeniyle birlikte geçirilir. Kendi özel arabiriminizi yazmanıza gerek yoktur.

Uygulama istemci olarak çalışıyorsa, işlem için istemci tarafı ve sunucu tarafı güvenlik çıkışlarına kullanıcı kimliği ve parola da iletilir. Ayrıca, bir kanal yönetim ortamının ileti kanalı aracısı kullanıcı kimliği (MCAUSER) özniteliği ayarı için de kullanılabilir. Bu işleme ilişkin çıkış nedeni MQXR_SEC_PARMS çıkış nedeni ile güvenlik çıkışıdır. İstemci tarafı güvenlik çıkışları ve bağlantı öncesi çıkış, kuyruk yöneticisine gönderilmeden önce MQCONN ' da değişiklik yapabilir.

Uyarı: Bazı durumlarda, istemci uygulaması için bir MQCSP yapısındaki parola, düz metindeki bir ağ üzerinden gönderilir. İstemci uygulaması parolalarının uygun şekilde korunmasını sağlamak için bkz. “MQCSP parola koruması” sayfa 28.

Bir kullanıcı kimliği ve parola sağlamak için XAOPEN dizesini kullanarak, uygulama kodunda değişiklik yapmak zorunda kalmaktan kaçınabilirsiniz.

Not:

From IBM WebSphere MQ 6.0, the security exit has allowed the MQCSP to be set. Bu nedenle, bu düzeydeki ya da daha sonra bu düzeydeki istemcilerin yükseltilmesine gerek yoktur.

Ancak, IBM MQ 8.0öncesindeki IBM MQ sürümlerinde, MQCSP, uygulama tarafından sağlanan kullanıcı kimliği ve parolaya ilişkin hiçbir kısıtlama getirmedi. IBM MQ tarafından sağlanan özelliklerle bu değerleri kullanırken, bu özelliklerin kullanılması için geçerli olan sınırlar vardır; ancak bunları yalnızca kendi çıkışlarınıza geçiriyorsanız, bu sınırlar geçerli değildir.

İlgili kavramlar

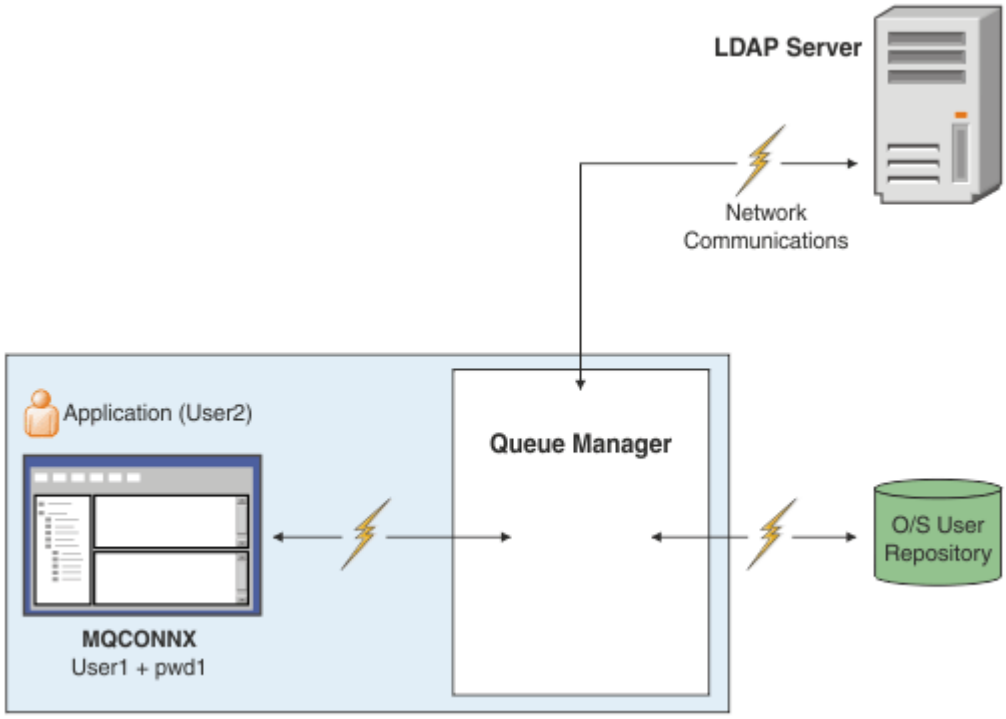
“Bağlantı kimlik doğrulaması” sayfa 64

“Bağlantı kimlik doğrulaması: Yapılandırma” sayfa 65
Bir kuyruk yöneticisi, kullanıcının kaynaklara erişim yetkisinin olup olmadığını denetlemek için, sağlanan bir kullanıcı kimliğini ve parolasını kullanacak şekilde yapılandırılabilir.

“Bağlantı kimlik doğrulaması: Kullanıcı havuzları” sayfa 70
Kuyruk yöneticilerinizin her biri için, kullanıcı kimliklerini ve parolaları doğrulamak üzere farklı tiplerde kimlik doğrulama bilgileri nesnesi seçebilirsiniz.

Bağlantı kimlik doğrulaması: Kullanıcı havuzları

Kuyruk yöneticilerinizin her biri için, kullanıcı kimliklerini ve parolaları doğrulamak üzere farklı tiplerde kimlik doğrulama bilgileri nesnesi seçebilirsiniz.



Şekil 7. Kimlik doğrulama bilgisi nesnelerinin tipleri

```
DEFINE AUTHINFO(USE.OS) AUTHTYPE(IDPWOS)
DEFINE AUTHINFO(USE.LDAP) +
AUTHTYPE(IDPWLDAP) +
CONNAME('ldap1(389),ldap2(389)') +
LDAPUSER('CN=QMGR1') +
LDAPPWD('passw0rd') SECCOMM(YES)
```

Çizgede gösterildiği gibi, iki tip kimlik doğrulama bilgisi nesnesi vardır:

- `IDPWOS` , kuyruk yöneticisinin kullanıcı kimliğini ve parolayı doğrulamak için yerel işletim sistemini kullandığını belirtmek için kullanılır. Yerel işletim sistemini kullanmayı seçerseniz, önceki konularda açıklandığı gibi ortak öznitelikleri ayarlamanız gerekir.
- `IDPWLDAP` , kuyruk yöneticisinin kullanıcı kimliğini ve parolayı doğrulamak için bir LDAP sunucusu kullandığını belirtmek için kullanılır. LDAP sunucusu kullanmayı seçerseniz, bu konuda daha fazla bilgi sağlanır.

Kuyruk yöneticisinin **CONNAUTH** özniteliğinde uygun nesne adlandırılarak, her kuyruk yöneticisinin kullanması için tek bir kimlik doğrulama bilgisi nesnesi seçilebilir.

Kimlik doğrulaması için LDAP sunucusu kullanılıyor.

CONNAME alanını, kuyruk yöneticisine ilişkin LDAP sunucusunun adresine ayarlayın. LDAP sunucusu için virgülle ayrılmış bir listede daha fazla adres sağlayabilirsiniz; bu, LDAP sunucusu bu olanağı sağlamazsa yedekliliğinize yardımcı olabilir.

Kuyruk yöneticisinin LDAP sunucusuna erişebilmesi ve kullanıcı kayıtlarıyla ilgili bilgileri arayabilmesi için **LDAPUSER** ve **LDAPPWD** alanlarında gerekli LDAP sunucusu kimliğini ve parolasını ayarlayın.

LDAP Sunucusuna Güvenli Bağlantı

Kanallardan farklı olarak, LDAP sunucusuyla iletişim için TLS kullanımını açmak için **SSLCIPH** parametresi yoktur. Bu durumda IBM MQ , LDAP sunucusu için istemci işlevi görür ve yapılandırmanın çoğu LDAP sunucusunda yapılır. IBM MQ içinde var olan bazı parametreler, bağlantının nasıl çalıştığını yapılandırmak için kullanılır.

LDAP sunucusuna bağlanırlığın TLS kullanıp kullanmayacağını denetlemek için **SECCOMM** alanını ayarlayın.

Bu özniteliğe ek olarak, kuyruk yöneticisi öznitelikleri **SSLFIPS** ve **SUITEB** , seçilen şifreleme belirtimleri kümesini kısıtlar. Kuyruk yöneticisini LDAP sunucusuna tanıtmak için kullanılan sertifika, `ibmwebspheremq` *`qmgr-name`* kuyruk yöneticisi sertifikasıdır ya da **CERTLABL** özniteliğinin değeridir. Ayrıntılar için bkz. Dijital sertifika etiketleri .

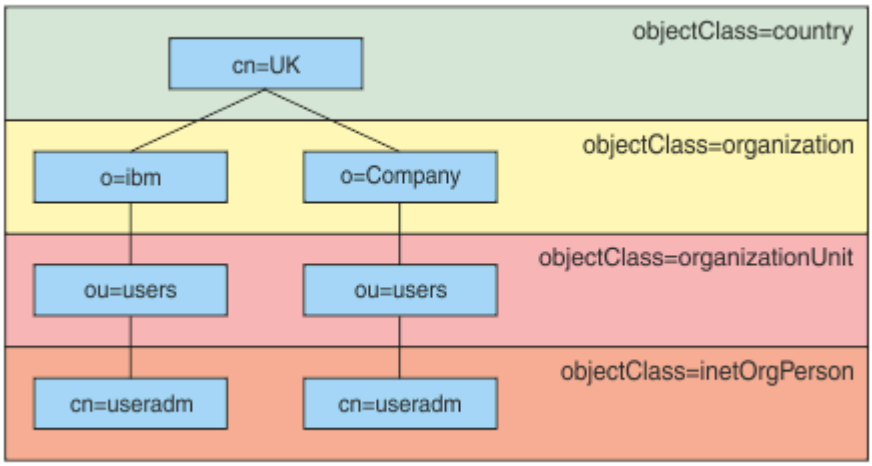
LDAP Kullanıcı Havuzu

Bir LDAP kullanıcı havuzu kullanılırken, kuyruk yöneticisine LDAP sunucusunu nerede bulacağını söylemek dışında, kuyruk yöneticisinde yapılması gereken başka bir yapılanış vardır.

LDAP sunucusunda tanımlanan kullanıcı kimlikleri, bunları benzersiz olarak tanımlayan sıradüzenli bir yapıya sahiptir. Bu nedenle, bir uygulama kuyruk yöneticisine bağlanabilir ve kullanıcı kimliğini tam olarak nitelenmiş sıradüzenli kullanıcı kimliği olarak sunabilir.

Ancak, bir uygulamanın sağlaması gereken bilgileri basitleştirmek için, kuyruk yöneticisini, sıradüzenin ilk kısmının tüm tanıtıcılar için ortak olduğunu varsaymak ve uygulama tarafından sağlanan kısaltılmış tanıtıcıdan önce bunu otomatik olarak eklemek üzere yapılandırmak mümkündür. Kuyruk yöneticisi daha sonra LDAP sunucusuna tam bir kimlik sunabilir.

BASEDNU değerini, LDAP aramasının LDAP sıradüzeninde kimliği aradığı ilk noktaya ayarlayın. BASEDNU ' yu ayarladığınızda, LDAP sıradüzeninde kimliği ararken yalnızca bir sonuç döndürüldüğünden emin olmanız gerekir.



Şekil 8. Örnek bir LDAP sıradüzeni

Örneğin, Şekil 8 sayfa 71 BASEDNU içinde "ou=users, o=ibm, c = UK" ya da ", o=ibm, c = UK" olarak ayarlanabilir. Ancak, hem "o = ibm" dalında hem de "o=Company" dalında "cn = useradm" içeren bir ayırt edici ad bulunduğundan, BASEDNU "c = UK" olarak ayarlanamaz. Performans ve güvenlik nedenleriyle, LDAP sıradüzeninizdeki, gereksinim duyduğunuz tüm kullanıcı kimliklerine başvurabileceğiniz en yüksek noktayı kullanın. Bu örnekte "ou=users, o=ibm, c = UK".

Uygulamanız, LDAP öznitelik adını (örneğin, CN=) sağlamadan kuyruk yöneticisine kullanıcı kimliğini sunabilir. USRFIELD değerini LDAP öznitelik adına ayarlarsanız, bu değer uygulamadan gelen kullanıcı kimliğine önek olarak eklenir. Bu, işletim sistemi kullanıcı kimliklerinden LDAP kullanıcı kimliklerine geçtiğinizde yararlı bir geçiş yardımı olabilir; böylece uygulama her iki durumda da aynı dizgiyi sunabilir ve uygulamayı değiştirmekten kaçınabilirsiniz.

Bu nedenle, LDAP sunucusuna sunulan tam kullanıcı kimliği şöyle görünür:

```
USRFIELD = ID_from_application BASEDNU
```

İlgili kavramlar

“Bağlantı kimlik doğrulaması” sayfa 64

“Bağlantı kimlik doğrulaması: Yapılandırma” sayfa 65
Bir kuyruk yöneticisi, kullanıcının kaynaklara erişim yetkisinin olup olmadığını denetlemek için, sağlanan bir kullanıcı kimliğini ve parolasını kullanacak şekilde yapılandırılabilir.

“Bağlantı kimlik doğrulaması: Uygulama değişiklikleri” sayfa 69

Kullanıcı kimliği ve parola eklemek için istemci tarafı güvenlik çıkışı (`mqccred`)

If you have any client applications that are required to send a user ID or password but you are unable to change the source yet, there is a security exit shipped with IBM MQ 8.0 called **`mqccred`** that you can use. **`mqccred`** , bir `.ini` dosyasından istemci uygulaması adına bir kullanıcı kimliği ve parola sağlar. Bu kullanıcı kimliği ve parolası kuyruk yöneticisine gönderilir; bunu yapmak üzere yapılandırıldıysa, bunları doğrulayacaktır.

Genel Bakış

`mqccred` , istemci uygulamanızın aynı makinesinde çalışan bir güvenlik çıkışıdır. Bu bilgi, kullanıcı kimliği ve parola bilgilerinin, uygulamanın kendisi tarafından sağlanmadığı istemci uygulaması adına sağlanmasına olanak sağlar. Kullanıcı kimliği ve parola bilgileri, Bağlantı Güvenliği Parametreleri (MQCSP) olarak bilinen bir yapı içinde sağlanır ve bağlantı kimlik doğrulaması yapılandırıldıysa, kuyruk yöneticisi tarafından doğrulanır.

Kullanıcı kimliği ve parola bilgileri, istemci makinesinde bulunan bir `.ini` dosyasından alınır. Dosyadaki parolalar, **`runmqccred`** komutu kullanılarak karartılarak korunur ve `.ini` dosyasındaki dosya izinlerinin, yalnızca istemci uygulamasını çalıştıran kullanıcı kimliğinin (ve dolayısıyla çıkış) bunu okuyabilecek şekilde ayarlanmasını sağlayarak, bu parolaların korunmasını sağlar.

Konum

`mqccred` kurulu:

Windows Platformlar
`installation_directory``\Tools\c\Samples\mqccred\` dizininde

UNIX Platformlar
`installation_directory``/samp/mqccred` dizininde

Notlar: Çıkış:

1. Tamamen bir güvenlik kanalı çıkışı gibi davranır ve bir kanalda tanımlanan tek çıkış olması gerekir.
2. Genellikle, Client Channel Definition Table (CCDT) aracılığıyla adlandırılır; ancak, Java istemcisi, JNDI nesnelerinde doğrudan doğruya çıkılabilir ya da çıkış, MQCD yapısını el ile yapılandıran uygulamalar için yapılandırılmış olabilir.
3. **`mqccred`** ve **`mqccred_r`** programlarını `var/mqm/exits` dizinine kopyalamanız gerekir.

   Örneğin, 64 bit UNIX altyapı makinesinde şu komutu verin:

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

   Ek bilgi için mqccred test etme örneğinin adım adım başlıklı konuya bakın.
4. Is capable of running on previous versions of IBM MQ, as far back as IBM WebSphere MQ 7.0.1.

Kullanıcı Kimlikleri ve Parolaların Ayarlanmasını

`.ini` dosyası, belirtilmeyen kuyruk yöneticileri için genel bir ayara sahip her kuyruk yöneticisi için stanzalar içerir. Her bir stanza, kuyruk yöneticisinin adını, bir kullanıcı kimliğini ve düz metin ya da karartılmış bir parola içerir.

İstediğiniz düzenleyiciyi kullanarak `.ini` dosyasını el ile düzenlemeniz ve stanzalara düz metin parolası özniteliğini eklemeniz gerekir. Run the provided, **runmqccred** program, which takes the `.ini` file and replaces the **Password** attribute with the **OPW** attribute, an obfuscated form of the password.

Komutun ve parametrelerinin açıklaması için runmqccred konusuna bakın.

`mqccred.ini` dosyası, kullanıcı kimliğinizi ve parola bilgilerinizi içerir.

Bir şablon `.ini` dosyası, işletmeniz için bir başlangıç noktası sağlamak üzere çıkışta belirtilen dizinde bulunur.

Varsayılan olarak, bu dosya $HOME/`.mqs/mqccred.ini`içinde ararlanacaktır. Başka bir yerde bulmak için, *MQCCRED* ortam değişkenini kullanarak aşağıdakileri gösterebilirsiniz:

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

*MQCCRED*kullanıyorsanız, değişken herhangi bir `.ini` kütük tipi de içinde olmak üzere, yapılanış kütüğünün tam adını içermelidir. Bu dosya parola içerdiği için (karartılmış olsa da), yetkisiz kişilerin okuyamadığından emin olmak için dosyayı işletim sistemi ayrıcalıklarını kullanarak korumanız beklenir. Doğru dosya iznine sahip değilseniz, çıkış başarılı bir şekilde çalışmaz.

Uygulama önceden bir MQCSP yapısı sağladıysa, çıkış olağan olarak buna dikkat eder ve `.ini` dosyasından hiçbir bilgi eklemez. Ancak, bu özelliği, stanza içindeki **Force** özniteliğini kullanarak geçersiz kılabilirsiniz.

Force değerini *TRUE* değerine ayarlamak, uygulama tarafından sağlanan kullanıcı kimliğini ve parolayı kaldırır ve bunları ini dosya sürümüyle değiştirir.

Dosyanın varsayılan değerini ayarlamak için, dosyanın genel bölümünde **Force** özniteliğini de ayarlayabilirsiniz.

Force için varsayılan değer *FALSE*değeridir.

Tüm kuyruk yöneticileri için ya da her bir kuyruk yöneticisi için bir kullanıcı kimliği ve parola sağlayabilirsiniz. Bu, `mqccred.ini` dosyasına bir örnektir:

```
# 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
```

Notlar:

1. Tek tek kuyruk yöneticisi tanımlamaları, genel ayara göre önceliklidir.
2. Öznitelikler büyük ve küçük harfe duyarlı değildir.

Kısıtlamalar

Bu çıkış kullanımda olduğunda, uygulamayı çalıştıran kişinin yerel kullanıcı kimliği istemciden sunucuya doğru akıp atmaz. Kullanılabilir tek kimlik bilgileri, ini dosyası içeriğinden kullanılabilir.

Bu nedenle, kuyruk yöneticisini **ADOPTCTX(YES)** kullanacak şekilde yapılandırmanız ya da gelen bağlantı isteğini kullanılabilir mekanizmalardan biri aracılığıyla uygun bir kullanıcı kimliği ile eşlemelisiniz; örneğin, "Kanal doğrulama kayıtları" sayfa 47.

Önemli: Yeni parolalar eklerseniz ya da eski olanları güncelseniz, **runmqccred** komutu yalnızca düz metin parolalarını işlerse, karartılmış olanlarınızı dokunulmaz olarak kaldırır.

Hata Ayıklama

Çıkış geçerli kılındığında standart IBM MQ izleme yazısına yazar.

Yapılandırma sorunlarında hata ayıklamaya yardımcı olmak için, çıkış doğrudan stdout ' a da yazabilir.

Kanal güvenliği çıkış verisi yok (**SCYDATA**) kanal için yapılandırma olağan bir şekilde gereklidir. Ancak, şunları belirtebilirsiniz:

HATA
Yapılanış kütüğünü bulamamak gibi, yalnızca bilgi yazdırma hata koşullarını yazdırır.

DEBUG
Bu hata koşullarını ve bazı ek izleme deyimlerini görüntüler.

NOCHKS
Dosya izinlerindeki kısıtlamaların atlanması ve `.ini` dosyasının korumasız parola içermemesi gereken ek kısıtlama.

Bu öğelerden birini ya da birkaçını, herhangi bir sırada virgülle ayrılmış olarak **SCYDATA** alanına yerleştirebilirsiniz. Örneğin, `SCYDATA=(NOCHECKS,DEBUG)`.

Öğelerin büyük ve küçük harfe duyarlı olduğunu ve büyük harfle girileceğini unutmayın.

Kullanılan `mqccred`

Dosyanızı ayarladıktan sonra, istemcin-bağlantı kanalı tanımınızı `SCYEXIT('mqccred(ChlExit)')` özniteliğini içerecek şekilde güncelleyerek kanal çıkışını başlatabilirsiniz:

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

İlgili başvurular
SCYDATA
SCYEXIT
runmqccred

Java istemcisi ile bağlantı kimlik doğrulaması

Bağlantı kimlik doğrulaması, IBM MQ ' da kuyruk yöneticisinin, sağlanan bir kullanıcı kimliği ve parola kullanarak uygulamaların kimliğini doğrulamak üzere yapılandırılmasını sağlayan bir özeldir. Uygulama istemci bağ tanımlarını kullanan bir Java uygulaması olduğunda, bağlantı kimlik doğrulaması uyumluluk kipinde ya da MQCSP kimlik doğrulama kipinde çalıştırılabilir.

Uyumluluk kipi

IBM MQ 8.0öncesinde, Java istemcisi istemci-bağlantı kanalından sunucu bağlantısı kanalına bir kullanıcı kimliği ve parola gönderebilir ve bunları, MQCD yapısının **RemoteUserIdentifier** ve **RemotePassword** alanlarında bir güvenlik çıkışa gönderebilmesini sağlar. Uyumluluk kipinde bu davranış korunur.

Bu kipi, bağlantı kimlik doğrulamasıyla birlikte kullanabilir ve önceden aynı işi yapmak için kullanılan tüm güvenlik çıkışlarından uzaklaşmanız gerekebilir.

Uyumluluk kipini kullanırken MCAUSER çalıştırmak için, bu kipte olduğu gibi, istemci tarafı kullanıcı kimliği kuyruk yöneticisine gönderilmediği için, ADOPTTCTX (YES) ya da TLS sertifikasına dayalı bir CHLAUTH kuralı gibi başka bir yönteme sahip olmanız gerekir.

Uyumluluk kipi, bağlantı temelinde ya da genel olarak bir bağlantıyla etkinleştirilebilir:

- In IBM MQ classes for Java, set the property *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* to `yanlış` in the properties hashtable that is passed to the **`com.ibm.mq.MQQueueManager`** constructor.
- IBM MQ classes for JMS' ta, bağlantıyı oluşturmadan önce uygun bağlantı üreticisinde *JmsConstants.USER_AUTHENTICATION_MQCSP* özelliğini `yanlış`olarak ayarlayın.
- Aşağıdaki örnekte gösterildiği gibi, uygulamanızı başlatırken komut satırında Java sistem özelliğini *-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication= N* belirtin:

```
java -Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N application_name
```

Uyumluluk kipi varsayılan ayardır.

MQCSP kimlik doğrulama kipi

Bu kipte, kimlik doğrulanacak kullanıcı kimliği ve parolanın yanı sıra, istemci tarafı kullanıcı kimliği de gönderilir. Bu nedenle, ADOPTCTX (NO) seçeneğini kullanabilirsiniz. Kullanıcı kimliği ve parolası, MQCXP yapısında sağlanan MQCSP yapısındaki bir sunucu bağlantısı güvenlik çıkışı için kullanılabilir.

Bu işlem kipi, bağlantı temelinde ya da genel olarak bir bağlantıyla etkinleştirilebilir:

- IBM MQ classes for Javaiçinde, **`com.ibm.mq.MQQueueManager`** oluşturucusuna aktarılan özellikler HASH çizelgesinde *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* özelliğini `true` değerine ayarlayın.
- IBM MQ classes for JMS' ta, bağlantıyı oluşturmadan önce uygun bağlantı üreticisinde *JmsConstants.USER_AUTHENTICATION_MQCSP* özelliğini `doğru`olarak ayarlayın.
- Genel olarak, *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* sistem özelliğini, komut satırına `-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=Y` ekleyerek doğru (true) değerini gösteren bir değere ayarlayın.

IBM MQ Explorer' ta kimlik doğrulama kipini seçme

IBM MQ Explorer bir Java uygulamasıdır, bu nedenle bu iki kip, uyumluluk kipi ve MQCSP kimlik doğrulama kipi, bu kip için de geçerlidir.

V 9.1.0 IBM MQ 9.1.0' tan, MQCSP kimlik doğrulama kipi varsayılan değerdir. IBM MQ 9.1öncesinde, uyumluluk kipi varsayılan değerdir.

Kullanıcı kimliğinin belirlendiği panolarda uyumluluk modunu etkinleştirmek ya da devre dışı bırakmak için bir onay kutusu vardır:

- V 9.1.0 IBM MQ 9.1.0' dan varsayılan olarak, bu onay kutusu seçili değildir. Uyumluluk modunu kullanmak için bu onay kutusunu işaretleyin.
- IBM MQ 9.1.0öncesinde, varsayılan olarak bu onay kutusu etkindir. MQCSP kimlik doğrulamasını kullanmak için onay kutusunun işaretini kaldırın.

İlgili kavramlar

“Bağlantı kimlik doğrulaması” sayfa 64

“Bağlantı kimlik doğrulaması: Uygulama değişiklikleri” sayfa 69

“Bağlantı kimlik doğrulaması: Kullanıcı havuzları” sayfa 70

Kuyruk yöneticilerinizin her biri için, kullanıcı kimliklerini ve parolaları doğrulamak üzere farklı tiplerde kimlik doğrulama bilgileri nesnesi seçebilirsiniz.

IBM MQiçinde ileti güvenliği

IBM MQ altyapısında ileti güvenliği Advanced Message Securitytarafından sağlanır.

Advanced Message Security (AMS) İleti düzeyinde veri imzalama ve şifreleme sağlamak için IBM MQ güvenlik hizmetlerini genişletir. Genişletilmiş hizmetler, ilk olarak bir kuyruğa yerleştirildiğinde ve alındığında ileti verilerinin değiştirilmediğini garanti eder. Buna ek olarak, AMS , ileti verilerinin göndericisinin, imzalı iletileri bir hedef kuyruğa yerleştirmeye yetkili olduğunu doğrular.

İlgili kavramlar

"Advanced Message Security" sayfa 541
Advanced Message Security (AMS) is a component of IBM MQ that provides a high level of protection for sensitive data flowing through the IBM MQ network, while not impacting the end applications.

Güvenlik gereksinimlerinizin planlanması

Bu konu derlemi, IBM MQ ortamında güvenliği planlarken göz önünde bulundurmanız gereken bilgileri açıklar.

You can use IBM MQ for a wide variety of applications on a range of platforms. Güvenlik gereksinimlerinin her uygulama için farklı olması beklenir. Bazıları için, güvenlik açısından kritik önem verilecektir.

IBM MQ , Transport Layer Security (TLS) desteği de içinde olmak üzere, bağlantı düzeyinde bir güvenlik hizmetleri aralığı sağlar.

IBM MQürününü kurmayı planlarken, güvenliğin belirli yönlerini göz önünde bulundurmanız gerekir:

- Multi Multiplatforms'ta, bu yönlerini yoksayabilir ve hiçbir şey yapmazsanız, IBM MQ' u kullanamazsınız.
- z/OS z/OS' ta, bu yönlerini yoksaymanın etkisi IBM MQ kaynaklarınızın korumasız olması olabilir. That is, all users can access and change all IBM MQ resources.

IBM MQyönetimi yetkisi

IBM MQ yöneticilerinin aşağıdakileri yapmak için yetkisi gerekir:

- IBM MQ' ı yönetmek için komut verme komutları
- Şunu kullanın:IBM MQ Explorer
- IBM i IBM i denetim panolarını ve komutlarını kullanın.
- z/OS z/OSüzerindeki işlemleri ve denetim panolarını kullanma
- z/OS z/OSüzerinde CSQUTIL, IBM MQ yardımcı programı programını kullanın.
- z/OS z/OSüzerindeki kuyruk yöneticisi veri kümelerine erişin

Daha fazla bilgi için bkz.

- ULW "UNIX, Linux, and Windowsüzerinde IBM MQ yönetimi yetkisi" sayfa 386
- IBM i "IBM iüzerinde IBM MQ yönetimi yetkisi" sayfa 81
- z/OS "z/OSüzerinde IBM MQ yönetimi yetkisi" sayfa 81

IBM MQ nesneleriyle çalışma yetkisi

Uygulamalar, MQI çağrıları yayınlayarak aşağıdaki IBM MQ nesnelerine erişebilir:

- Kuyruk yöneticileri
- Kuyruklar
- Süreçler
- Ad listeleri
- Konular

Uygulamalar, bu IBM MQ nesnelerine erişmek ve kanallara ve kimlik doğrulama bilgi nesnelerine erişmek için Programlanır Komut Biçimi (PCF) komutlarını da kullanabilir. Bu nesneler IBM MQ ile korunabilir; böylece, uygulamalarla ilişkili kullanıcı kimlikleri bunlara erişmek için yetkiye gereksinim duyarlar.

Daha fazla bilgi için "Authorization for applications to use IBM MQ" sayfa 83 başlıklı konuya bakın.

Kanal güvenliği

İleti kanalı aracıları (MCA ' lar) ile ilişkili kullanıcı kimlikleri, çeşitli IBM MQ kaynaklarına erişmek için yetkiye gereksinim duyarlar. Örneğin, bir MCA ' nın kuyruk yöneticisine bağlanabilmesi gerekir. MCA gönderiyorsa, kanala ilişkin iletim kuyruğunu açabilmelidir. Alıcı bir MCA ise, hedef kuyrukları açabilmelidir. Kanalları, kanal başlatıcılarını ve dinleyicileri denetlemek için gereken uygulamalarla ilişkili kullanıcı kimlikleri ilgili PCF komutlarını kullanma yetkisine sahip olmalıdır. Ancak, uygulamaların çoğu bu tür erişime sahip değildir.

Daha fazla bilgi için "Kanal yetkisi" sayfa 103 başlıklı konuya bakın.

Ek konular

Yalnızca belirli IBM MQ işlevini ya da temel ürün uzantılarını kullanıyorsanız, aşağıdaki güvenlik yönlerini göz önünde bulundurmanız gerekir:

- "Kuyruk yöneticisi kümeleri için güvenlik" sayfa 116
- "IBM MQ Yayınlama/Abone Olma Güvenliği" sayfa 116
- "IBM MQ Internet Pass-Thrugüvenliği" sayfa 118

Planlama tanıtıcısı ve kimlik doğrulaması

Kullanılacak kullanıcı kimliklerinin ve kimlik doğrulama denetimlerini uygulamak istediğiniz düzeylere nasıl ve ne kadar düzeyde istediğinizi belirleyin.

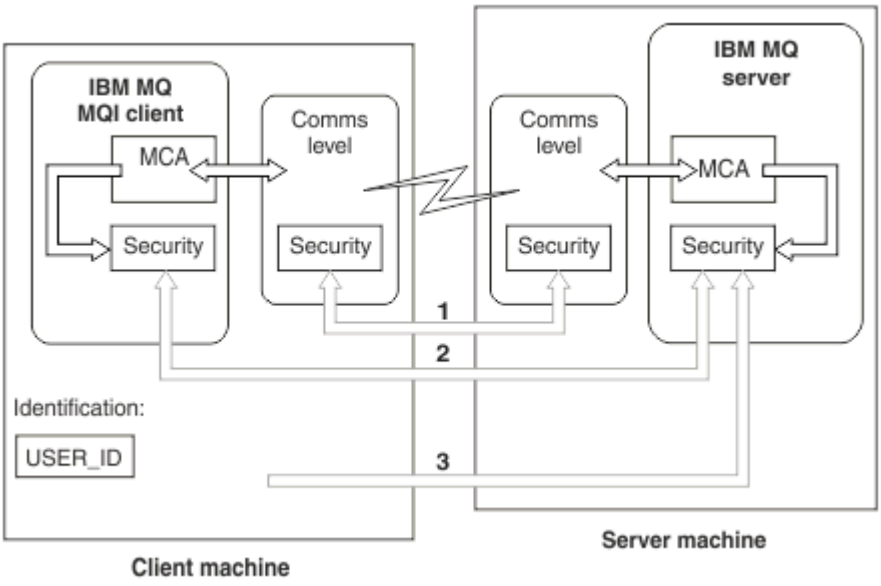
Farklı işletim sistemlerinin kullanıcı kimliklerini farklı uzunluklarda desteklediğine göz önünde olmak üzere, IBM MQ uygulamalarınızın kullanıcılarını nasıl tanımlayacağınıza karar vermelisiniz. Kanal doğrulama kayıtlarını, bir kullanıcı kimliğiyle başka bir kullanıcı kimliğiyle eşlemek ya da bağlantının bazı özniteliklerine dayalı olarak bir kullanıcı kimliği belirtmek için kullanabilirsiniz. TLS ' yi kullananIBM MQ kanalları, tanımlama ve kimlik doğrulaması için bir mekanizma olarak dijital sertifikalar kullanır. Her dijital sertifikada, kanal kimlik doğrulama kayıtları kullanılarak belirli kimliklerle eşleştirilebilen bir konu ayırt edici adı vardır. Buna ek olarak, anahtar havuzundaki CA sertifikaları, IBM MQ' ta kimlik doğrulamak için hangi sayısal sertifikaların kullanılabileceğini belirler. Daha fazla bilgi için bakınız:

- "Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi" sayfa 371
- "İstemci kullanıcı kimliğinin MCAUSER kullanıcı kimliğiyle eşlenmesi" sayfa 372
- "SSL ya da TLS Ayırt Edici Adının MCAUSER kullanıcı kimliğine eşlenmesi" sayfa 372
- "Bir IP adresinin MCAUSER kullanıcı kimliği ile eşlenmesi" sayfa 374

İstemci uygulaması için kimlik doğrulaması planlama

Kimlik doğrulama denetimlerini dört düzeyden uygulayabilirsiniz: iletişim düzeyinde, güvenlik çıkışlarında, kanal kimlik doğrulama kayıtlarıyla ve güvenlik çıkışa geçirilen tanıtıcı açısından.

Göz önünde bulundurulması gereken dört bir güvenlik düzeyi vardır. Çizge, bir sunucuya bağlı bir IBM MQ MQI client ' i gösterir. Güvenlik, aşağıdaki metinde açıklandığı gibi dört düzeyde uygulanır. MCA, Message Channel Agent 'dir.



Şekil 9. İstemci/sunucu bağlantısında güvenlik

1. İletişim düzeyi

   Bkz. ok 1. İletişim düzeyinde güvenliği uygulamak için TLS ' yi kullanın. Daha fazla bilgi için bkz. “Şifreleme güvenlik iletişim kuralları: TLS” sayfa 14

2. Kanal doğrulama kayıtları

   Bkz. ok 2 ve 3. Kimlik doğrulama, IP adresi ya da güvenlik düzeyinde TLS ayırt edici adları kullanılarak denetlenebilir. Bir kullanıcı kimliği de engellenebilir ya da değerlendirilen bir kullanıcı kimliği geçerli bir kullanıcı kimliğiyle eşlenebilir. “Kanal doğrulama kayıtları” sayfa 47' ta tam açıklama verilir.

3. Bağlantı kimlik doğrulaması

   Bkz. ok 3. İstemci bir kimlik ve parola gönderir. Daha fazla bilgi için “Bağlantı kimlik doğrulaması: Yapılandırma” sayfa 65 başlıklı konuya bakın.

4. Kanal güvenlik çıkışları

   Bkz. ok 2. İstemcinin sunucu iletişimine ilişkin kanal güvenliği çıkışları, sunucu iletişiminin sunucu ile aynı şekilde çalışabileceği şekilde çalışır. İstemci ile sunucu arasında karşılıklı kimlik doğrulaması sağlamak için, iletişim kuralı bağımsız bir çift çıkışa yazılabilir. Kanal güvenlik çıkış programlarıiçinde tam bir açıklama verilir.

5. Kanal güvenlik çıkışa geçilen tanıtıcı

   Bkz. ok 3. İstemcide, iletişim sunucusu iletişimi için kanal güvenliği çıkışlarının bir çift olarak çalışması gerekmez. IBM MQ istemci tarafındaki çıkış atlanabilir. Bu durumda, kullanıcı kimliği kanal tanımlayıcısına (MQCD) yerleştirilir ve gerekiyorsa, sunucu tarafındaki güvenlik çıkışı bunu değiştirebilir.

   Windows istemcileri, tanımlamaya yardımcı olmak için ek bilgiler de gönderir.

   - Sunucuya geçirilen kullanıcı kimliği, istemcideki şu anda oturum açmış olan kullanıcı kimliğidir.
   - Şu anda oturum açmış olan kullanıcının güvenlik tanıtıcısı.

   Kullanıcı kimliğinin ve varsa, güvenlik kimliğinin değerleri, sunucu güvenliği çıkışı tarafından IBM MQ MQI client' ın kimliğini oluşturmak için kullanılabilir.

IBM MQ 8.0' tan, MQCSP yapısına dahil edilen parolaları gönderebilirsiniz.

Uyarı: Bazı durumlarda, istemci uygulaması için bir MQCSP yapısındaki parola, düz metindeki bir ağ üzerinden gönderilir. İstemci uygulaması parolalarının uygun şekilde korunmasını sağlamak için bkz. “MQCSP parola koruması” sayfa 28.

Kullanıcı Kimlikleri

İstemci uygulamaları için kullanıcı kimlikleri yarattığınızda, kullanıcı kimliklerinin izin verilen uzunluk üst sınırından uzun olması gerekir. UNKNOWN ve NOBODY olarak ayrılmış kullanıcı kimliklerini kullanmamalısınız. İstemcinin bağlanacağı sunucu bir IBM MQ for Windows sunucuysa, @ işaretinin kullanılmasından kaçmanız gerekir. Kullanıcı kimliklerinin izin verilen uzunluğu, sunucu için kullanılan platforma bağımlıdır:

- z/OS Linux UNIX z/OS ve UNIX and Linuxüzerinde, bir kullanıcı kimliği uzunluğu üst sınırı 12 karakterdir.
- IBM i IBM iüzerinde, bir kullanıcı kimliğinin uzunluk üst sınırı 10 karakterdir.
- Windows Windowsüzerinde, hem IBM MQ MQI client, hem de IBM MQ sunucusu Windowsüzerinse ve sunucu, istemci kullanıcı kimliğinin tanımlı olduğu etki alanına erişiyorsa, bir kullanıcı kimliğinin uzunluk üst sınırı 20 karakterdir. Ancak, IBM MQ sunucusu bir Windows sunucusu değilse, kullanıcı kimliği 12 karaktere kısaltılır.
- Kimlik bilgilerini geçirmek için MQCSP yapısını kullanırsanız, kullanıcı kimliğinin uzunluk üst sınırı 1024 karakterdir. MQCSP yapısı kullanıcı kimliği, yetki için IBM MQ tarafından kullanılan kullanıcı kimliği uzunluğu üst sınırını geçersiz kılacak şekilde kullanılamaz. MQCSP yapısı hakkında daha fazla bilgi için bkz. “MQCSP yapısını kullanarak kullanıcıların belirlenmesi ve doğrulanmaları” sayfa 320.

UNIX and Linux sistemlerinde varsayılan değer, kimlik doğrulaması için kullanılan kullanıcı kimliklerinin ve grupların yetkilendirme için kullanılmasıdır. Ancak, bu sistemleri kullanıcı Ids 'e karşı yetkilendirmek için yapılandırabilirsiniz. Daha fazla bilgi için bkz “OAM user-based permissions on UNIX and Linux” sayfa 337. Windows sistemleri, yetkilendirme için hem kimlik doğrulama, hem de yetkilendirme için hem kullanıcı kimliklerini hem de kullanıcı kimliklerini kullanabilir.

Hizmet hesapları oluşturursanız, gruplara dikkat etmeden ve tüm kullanıcı kimlikleri için farklı bir şekilde yetki verdiyseniz, her kullanıcı diğer her kullanıcının bilgilerine erişebilir.

Kısıtlı kullanıcı kimlikleri

The user IDs `UNKNOWN` and group `NOBODY` have special meanings to IBM MQ. Creating a user ID in the operating system called `UNKNOWN` or a group called `NOBODY` could have unintended results.

IBM MQ for Windows Server sunucusuna bağlanırken kullanıcı kimlikleri

Windows

An IBM MQ for Windows server does not support the connection of a Windows client if the client is running under a user ID that contains the @ character, for example, `abc@d`. İstemcideki `MQCONN` çağrısına dönüş kodu MQRC_NOT_AUTONIZED (MQRC_NOT_AUTY) değerine sahip.

Ancak, iki @ karakterini kullanarak kullanıcı kimliğini belirtebilirsiniz; örneğin, `abc@@d`. Using the `id@domain` format is the preferred practice, to ensure that the user ID is resolved in the correct domain consistently; thus `abc@@d@domain`.

Planlama yetkilendirmesi

Plan the users who will have administrative authority and plan how to authorize users of applications to appropriately use IBM MQ objects, including those connecting from an IBM MQ MQI client.

IBM MQ' u kullanabilmek için kişilere ya da uygulamalara erişim izni verilmelidir. Gerekli olan erişim, üstlendikleri rollere ve gerçekleştirmeye gereksinim duydukları görevlere bağlıdır. IBM MQ içindeki yetki, iki ana kategoriye ayrılabilir:

- Yönetim işlemlerini gerçekleştirme yetkisi
- Authorization for applications to use IBM MQ

Her iki işlem sınıfı da aynı bileşen tarafından denetlenir ve her iki işlemi de gerçekleştirmek için her iki sınıf da yetki verilebilir.

Aşağıdaki konularda, göz önünde bulundurmanız gereken belirli yetki alanları hakkında daha fazla bilgi edinmeniz gerekir:

IBM MQyönetimi yetkisi

IBM MQ denetimcileri, çeşitli işlevleri gerçekleştirmeye ilişkin yetkiye gereksinim duyarlar. Bu yetki farklı platformlarda farklı şekillerde elde edilir.

IBM MQ yöneticilerinin aşağıdakileri yapmak için yetkisi gerekir:

- IBM MQ' ı denetlemek için komut verin.
- Linux Windows IBM MQ Explorer' yi kullanın.
- z/OS z/OSüzerindeki işlemleri ve denetim panolarını kullanın.
- z/OS z/OSüzerinde CSQUTIL IBM MQ yardımcı programı (CQUItil) programını kullanın.
- z/OS Access the queue manager data sets on z/OS.

Daha fazla bilgi için işletim sisteminize uygun olan konuya bakın.

Windows UNIX *UNIX ve Windows sistemlerinde IBM MQ yönetimi yetkisi*

IBM MQ yöneticisi, mqm grubunun bir üyesidir. Bu grubun tüm IBM MQ kaynaklarına erişimi vardır ve IBM MQ denetim komutlarını yayınlayabilirler. Bir yönetici, belirli yetkiler için diğer kullanıcılara yetki verebilir.

UNIX ve Windows sistemlerinde bir IBM MQ yöneticisi olmak için, kullanıcının *mqm group*üyesi olması gerekir. Bu grup, IBM MQ' u kurduğunuzda otomatik olarak oluşturulur. Kullanıcıların denetim komutlarını yayınlamasına izin vermek için bunları mqm grubuna eklemelisiniz. Bu, UNIXüzerindeki kök kullanıcıyı içerir.

Mqm grubuna üye olmayan kullanıcılar için yönetici ayrıcalıkları verilebilir, ancak IBM MQ denetim komutları yayınlayamaz ve yalnızca erişim verilen komutları yürütme yetkisine sahip olur.

Additionally, on Windows systems, the SYSTEM and Administrator accounts have full access to IBM MQ resources.

Mqm grubunun tüm üyeleri, sistemde çalışan kuyruk yöneticisini yönetebilmek de içinde olmak üzere, sistemdeki tüm IBM MQ kaynaklarına erişime sahiptir. Bu erişim, yalnızca mqm grubundan bir kullanıcı kaldırılarak iptal edilebilir. Windows sistemlerinde, Administrators (Yöneticiler) grubunun üyelerinin de tüm IBM MQ kaynaklarına erişimleri vardır.

Denetimciler, IBM MQ Script (MQSC) komutlarını vermek için **runmqsc** denetim komutunu kullanabilir. **runmqsc** uzak kuyruk yöneticisine MQSC komutları göndermek için dolaylı kipte kullanıldığında, her MQSC komutu bir Escape PCF komutu içinde kapsüllenmiş olur. Denetimcilerin, uzak kuyruk yöneticisi tarafından işlenecek MQSC komutlarına ilişkin gerekli yetkileri olmalıdır.

IBM MQ Explorer , denetim görevlerini gerçekleştirmek için PCF komutları verir. Denetimciler, yerel sistemde kuyruk yöneticisini denetlemek için IBM MQ Explorer ' i kullanmak üzere ek yetkilere gerek duymaz. IBM MQ Explorer , bir kuyruk yöneticisini başka bir sistemde denetlemek için kullanıldığında, denetimcilerin, PCF komutlarının uzak kuyruk yöneticisi tarafından işlenmesine ilişkin gerekli yetkilere sahip olması gerekir.

PCF ve MQSC komutları işlendiğinde gerçekleştirilen yetki denetimlerine ilişkin ek bilgi için aşağıdaki konulara bakın:

- Kuyruk yöneticileri, kuyruklar, kanallar, işlemler, ad listeleri ve kimlik doğrulama bilgileri nesneleri üzerinde işlem yapan komutlar için bkz. “Authorization for applications to use IBM MQ” sayfa 83.
- Kanallar, kanal başlatıcıları, dinleyiciler ve kümelerde çalışan komutlar için bkz. Kanal güvenliği.
- z/OS IBM MQ for z/OSüzerinde komut sunucusu tarafından işlenen MQSC komutları için bkz. “z/OSüzerinde komut güvenliği ve komut kaynağı güvenliği” sayfa 82.

UNIX ve Windows sistemlerinde IBM MQ ' i yönetmek için gereken yetkiyle ilgili daha fazla bilgi için ilgili bilgilere bakın.

IBM i *IBM iüzerinde IBM MQ yönetimi yetkisi*

IBM iüzerinde IBM MQ yöneticisi olmak için, *QMQMADM grubu*üyesi olmanız gerekir. Bu grubun özellikleri, UNIX ve Windows sistemlerinde mqm grubunun benzerlerine benzer. Özellikle, QMQMADM grubu, IBM MQ for IBM i' u kurduğunuzda yaratılır ve QMQMADM grubunun üyeleri sistemdeki tüm IBM MQ kaynaklarına erişir. Ayrıca, *ALLOBJ yetkiniz varsa tüm IBM MQ kaynaklarına da erişiminiz vardır.

Yöneticiler, IBM MQ' u yönetmek için CL komutlarını kullanabilirler.Bu komutlardan biri, diğer kullanıcılara yetki vermek için kullanılan GRTMQMAUT komutlarından biridir. STRMQMQSC başka bir komut, bir denetimcinin yerel bir kuyruk yöneticisine MQSC komutları yayınlamasını sağlar.

IBM MQ for IBM itarafından sağlanan iki grup CL komutu grubu vardır:

Grup 1
Bu kategoride bir komut vermek için, kullanıcının QMQMADM grubunun üyesi olması ya da *ALLOBJ yetkisinin olması gerekir. Örneğin, GRTMQMAUT ve STRMQMMQSC bu kategoriye ait.

Grup 2
Bu kategoride bir komut yayınlamak için, kullanıcının QMQMADM grubunun üyesi olması ya da *ALLOBJ yetkisinin olması gerekmez. Bunun yerine, iki yetki düzeyi gereklidir:

- Kullanıcı, komutu kullanmak için IBM i yetkisini gerektirir. Bu yetki, GRTOBJAUT komutu kullanılarak verilir.
- Kullanıcı, komutla ilişkilendirilmiş herhangi bir IBM MQ nesnesine erişmek için IBM MQ yetkisini gerektirir. Bu yetki, GRTMQMAUT komutu kullanılarak verilir.

Aşağıdaki örnekler, bu grupta yer alan komutları gösterir:

- CRTMQMQ, MQM Kuyruğu Yarat
- CHGMQMPRC, MQM sürecini değiştir
- DDLTMQMNL, MQM Namelist 'i Sil
- DSPMQMAUTI, MQM Kimlik Doğrulama Bilgilerini Görüntüle
- CRTMQMCHL, MQM kanalı yarat

Bu komut grubuyla ilgili daha fazla bilgi için bkz. “Authorization for applications to use IBM MQ” sayfa 83.

Grup 1 ve grup 2 komutlarının tam listesi için bkz. “IBM iüzerindeki IBM MQ nesnelerine erişim yetkileri” sayfa 149

IBM i'ta IBM MQ ' i yönetmeniz için gereken yetkiyle ilgili daha fazla bilgi için bkz. IBM i Yönetimi.

z/OS *z/OSüzerinde IBM MQ yönetimi yetkisi*

Bu konular grubunda, IBM MQ for z/OS' i yönetmeniz gereken çeşitli yetkilerin çeşitli yönlerini ele alınmıştır.

z/OS *z/OSüzerinde yetki denetimleri*

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

It is assumed that you are using RACF as your ESM. Farklı bir ESM kullanıyorsanız, RACF için sağlanan bilgileri, ESM ' niz ile ilgili bir şekilde yorumlamak isteyebilirsiniz.

Her kuyruk yöneticisi için ya da her kuyruk yöneticisi için bir kuyruk paylaşım grubundaki her kuyruk yöneticisi için yetki denetimlerinin açık ya da kapalı olup olmadığını belirleyebilirsiniz.Bu denetim düzeyine *altsistem güvenliği*adı verilir. Altsistem güvenliğini belirli bir kuyruk yöneticisi için kapatıyorsanız, o kuyruk yöneticisi için herhangi bir yetki denetimi gerçekleştirilmez.

Belirli bir kuyruk yöneticisi için altsistem güvenliğini döndürdüyseniz, yetki denetimleri iki düzeyde gerçekleştirilebilir:

Kuyruk paylaşım grubu düzeyinde güvenlik
Yetki denetimleri, kuyruk paylaşım grubundaki tüm kuyruk yöneticileri tarafından paylaşılan RACF profillerini kullanır. Bu, güvenlik yönetimini daha kolay tanımlamak ve sürdürmek için daha az profil olduğu anlamına gelir.

Kuyruk yöneticisi düzeyinde güvenlik
Yetki denetimleri, kuyruk yöneticisine özgü RACF profillerini kullanır.

Kuyruk paylaşım grubu ve kuyruk yöneticisi düzeyinde güvenlik birleşimi kullanabilirsiniz. Örneğin, bir kuyruk yöneticisine özgü tanıtımlar için, ait olduğu kuyruk paylaşım grubunun adını geçersiz kılacak bir düzenleme yapabilirsiniz.

Subsystem security, queue sharing group level security, and queue manager level security are turned on or off by defining *anahtar profilleri*. Anahtar tanıtımı, IBM MQiçin özel bir anlamı olan olağan bir RACF tanıtımdır.

z/OS *z/OSüzerinde komut güvenliği ve komut kaynağı güvenliği*

Komut güvenliği, bir komut verme yetkisi ile ilgilidir; komut kaynağı yetkisi, bir kaynak üzerinde işlem gerçekleştirmek için gereken yetkiyle ilgilidir. Her ikisi de RACF sınıflarını kullanarak uygulanır.

Bir IBM MQ yöneticisi bir MQSC komutu verdiğinde, yetki denetimleri gerçekleştirilir. Buna *komut güvenliği*adı verilir.

Komut güvenliğini uygulamak için, belirli RACF profillerini tanımlamanız ve gerekli gruplar ve kullanıcı kimlikleri için gerekli düzeylerde bu tanıtımlara erişebilmesini gerçekleştirmeniz gerekir. Komut güvenliği için bir tanıtımın adı, bir MQSC komutunun adını içerir.

Bazı MQSC komutları, yerel kuyruk yaratmak için DEFINE QLOCAL komutu gibi bir IBM MQ kaynağı üzerinde bir işlem gerçekleştirir. Bir denetimci bir MQSC komutu verdiğinde, istenen işlemin komutta belirtilen kaynak üzerinde gerçekleştirilip gerçekleştirilmeyeceğini belirlemek için yetki denetimleri gerçekleştirilir. Buna *komut kaynağı güvenliği*adı verilir.

Komut kaynağı güvenliğini uygulamak için, belirli RACF profillerini tanımlamanız ve gerekli gruplar ve kullanıcı kimlikleri için gerekli düzeylerde bu tanıtımlara erişebilmesini gerçekleştirmeniz gerekir. Bir IBM MQ kaynağının adını ve tipini (QUEUE, PROCESS, NAMELIST, TOPIC, AUTHINFO ya da CHANNEL) içeren komut kaynağı güvenliği için bir profil adı.

Komut güvenliği ve komut kaynağı güvenliği bağımsızdır. Örneğin, bir denetimci komutu verince aşağıdaki komutu verir:

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

aşağıdaki yetki denetimleri gerçekleştirilir:

- Komut güvenliği, denetimcinin DEFINE QLOCAL komutunu verme yetkisine sahip olduğunu denetler.
- Komut kaynağı güvenliği, denetimcinin MOON.EUROPA.

Anahtar tanıtımları tanımlanarak, komut güvenliği ve komut kaynağı güvenliği açılabilir ya da kapatılabilir.

z/OS *MQSC commands and the system command input queue on z/OS*

Komut sunucusunun, z/OSişletim sisteminde sistem komut giriş kuyruğuna yönlendirilen MQSC komutlarını nasıl işlediğini anlamak için bu konuyu kullanın.

Komut sunucusu, sistem komut giriş kuyruğundan bir MQSC komutu içeren bir iletiyi alırken, komut güvenliği ve komut kaynağı güvenliği de kullanılır.Yetki denetimleri için kullanılan kullanıcı kimliği, MQSC komutunu içeren iletinin ileti tanımlayıcısında bulunan *UserIdentifier* alanında bulunan tanıtıcıdır. Bu kullanıcı kimliğinin, komutun işlendiği kuyruk yöneticinde gerekli yetkilerin olması gerekir. *UserIdentifier* alanıyla ve nasıl ayarlansa ilişkin ek bilgi için Message contextbaşlıklı konuya bakın.

MQSC komutlarını içeren iletiler sistem komut girişi kuyruğuna aşağıdaki durumlarda gönderilir:

- İşlemler ve denetim panoları, MQSC komutlarını hedef kuyruk yöneticisinin sistem komut girişi kuyruğuna gönderir. MQSC komutları, panolarda seçtiğiniz eylemlere karşılık gelir. Her iletindeki *UserIdentifier* alanı, denetimcinin TSO kullanıcı kimliğine ayarlanır.
- IBM MQ yardımcı programı CSQUTIL programının KOMUTU işlevi, giriş verilerinde bulunan MQSC komutlarını hedef kuyruk yöneticisinin sistem komut girişi kuyruğuna gönderir. COPY ve EMPTY işlevleri, DISPLAY QUEUE ve DISPLAY STGCLASS komutlarının gönderilmesini sağlar. Her iletindeki *UserIdentifier* (Kullanıcı Kimliği) alanı, iş kullanıcısı kimliğine ayarlanır.
- CSQINPX veri kümelerindeki MQSC komutları, kanal başlatıcısının bağlı olduğu kuyruk yöneticisinin sistem komut giriş kuyruğuna gönderilir. Her iletindeki *UserIdentifier* alanı, kanal başlatıcı adres alanı kullanıcı kimliğine ayarlanır.

  No authority checks are performed when MQSC commands are issued from the CSQINP1 and CSQINP2 data sets. RACF veri kümesi korumasını kullanarak bu veri kümelerini güncelleştirmesine izin verilen kişileri denetleyebilirsiniz.
- Bir kuyruk paylaşım grubu içinde, kanal başlatıcısı, bağlantı kurulan kuyruk yöneticisinin sistem komut girişi kuyruğuna START KANAL komutları gönderebilir. Bir komut, paylaşılan bir iletim kuyruğunu kullanan bir giden kanal tetikleyerek başlatıldığında gönderilir. Her iletindeki *UserIdentifier* alanı, kanal başlatıcı adres alanı kullanıcı kimliğine ayarlanır.
- Bir uygulama, MQSC komutlarını bir sistem komut girişi kuyruğuna gönderebilir. Varsayılan değer olarak, her iletindeki *UserIdentifier* alanı, uygulamayla ilişkili kullanıcı kimliğine ayarlanır.
- On UNIX, Linux, and Windows systems, the **runmqsc** control command can be used in indirect mode to send MQSC commands to the system command input queue of a queue manager on z/OS. Her iletindeki *UserIdentifier* alanı, **runmqsc** komutunu veren denetimcinin kullanıcı kimliğine ayarlanır.

z/OS *z/OSüzerindeki kuyruk yöneticisi veri kümelerine erişim*

IBM MQ for z/OS denetimcileri kuyruk yöneticisi veri kümelerine erişmek için yetkiye gereksinim duyarlar. Hangi veri kümelerinin RACF korumasını gerektiğini anlamak için bu konuyu kullanın.

Bu veri kümeleri şunları içerir:

- V 9.1.0 Kuyruk yöneticisinin başlatılan görev yordamında CSQINP1, CSQINP2ve CSQINPT tarafından gönderme yapılan veri kümeleri.
- Kuyruk yöneticisinin sayfa kümeleri, etkin günlük veri kümeleri, arşiv günlüğü veri kümeleri ve önyükleme veri kümeleri (BSDSs)
- Kanal başlatıcısının başlattığı görev yordamında, CSQXLIB ve CSQINPX tarafından gönderme yapılan veri kümeleri

Yetkisiz kullanıcıların bir kuyruk yöneticisini başlatabilmesi ya da kuyruk yöneticisi verilerine erişim elde edebilmesi için veri kümelerini korumalısınız. Bunu yapmak için RACF veri kümesi korumasını kullanın.

Authorization for applications to use IBM MQ

Uygulamalar nesnelere eriştiğinde, uygulamalara ilişkin kullanıcı kimliklerinin uygun yetkiye gereksinimi vardır.

Uygulamalar, MQI çağrıları yayınlayarak aşağıdaki IBM MQ nesnelerine erişebilir:

- Kuyruk yöneticileri
- Kuyruklar
- Süreçler
- Ad listeleri
- Konular

Uygulamalar, IBM MQ nesnelerini yönetmek için PCF komutlarını da kullanabilir. PCF komutu işlendiğinde, PCF iletisini alan kullanıcı kimliğinin yetki bağlamını kullanır.

Uygulamalar, bu bağlamda kullanıcılar ve satıcılar tarafından yazılanlar ve IBM MQ for z/OSile birlikte verilen uygulamaları içerir. IBM MQ for z/OS ile verilen uygulamalar arasında şunlar yer alır:

- İşlemler ve denetim panoları
- IBM MQ yardımcı programı (CQUOtil)
- Ölü mektup kuyruğu işleyici yardımcı programı, CSQUDLQH

C/C++ ve .NET için IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NETya da Message Service Clients kullanan uygulamalar, dolaylı olarak MQI ' yi kullanır.

MCA 'lar ayrıca, bu IBM MQ nesnelerine erişmek için MCA' lar ile ilişkili kullanıcı kimlikleri ve MQI çağrıları da yayınlamakla ilgili bilgi verir. Bu kullanıcı kimlikleri ve gerekli yetkiler hakkında daha fazla bilgi için bkz. “Kanal yetkisi” sayfa 103.

z/OSüzerinde uygulamalar, bu IBM MQ nesnelerine erişmek için MQSC komutlarını da kullanabilir, ancak komut güvenliği ve komut kaynağı güvenliği bu durumlarda yetki denetimlerini sağlar. z/OS Daha fazla bilgi için bkz. “z/OSüzerinde komut güvenliği ve komut kaynağı güvenliği” sayfa 82 ve “MQSC commands and the system command input queue on z/OS” sayfa 82.

IBM iüzerinde, Grup 2 'de bir CL komutu veren bir kullanıcı, komutla ilişkilendirilmiş bir IBM MQ nesnesine erişmek için yetki gerektirebilir. Daha fazla bilgi için “Yetki denetimi gerçekleştirildiğinde” sayfa 84 başlıklı konuya bakın.

Yetki denetimi gerçekleştirildiğinde

Bir uygulama kuyruk yöneticisine, kuyruğa, sürece ya da ad listesine erişmeyi denediğinde, yetki denetimleri gerçekleştirilir.

IBM iüzerinde, kullanıcı bu IBM MQ nesnelerinden herhangi birine erişen Grup 2 'de bir CL komutu yayınlarken de yetki denetimleri gerçekleştirilebilir. Çekler aşağıdaki durumlarda gerçekleştirilir:

Bir uygulama `MQCONN` ya da `MQCONNX` çağrısını kullanarak bir kuyruk yöneticisine bağlandığında
Kuyruk yöneticisi, uygulamayla ilişkili kullanıcı kimliği için işletim sistemini ister. Daha sonra kuyruk yöneticisi, kullanıcı kimliğinin ona bağlanma yetkisine sahip olup olmadığını denetler ve ileride yapılacak denetlere ilişkin kullanıcı kimliğini korur.

Kullanıcıların IBM MQ' ta oturum açmak zorunda kalmaması gerekir. IBM MQ , kullanıcıların temeldeki işletim sisteminde oturum açmakta olduğunu ve bunun için kimlik doğrulaması gerçekleştirdiğini varsayar.

Bir uygulama `MQOPEN` ya da `MQPUT1` çağrısını kullanarak IBM MQ nesnesini açtığında
Bir nesne açıldığında, daha sonra erişildiğinde değil, tüm yetki denetimleri gerçekleştirilir. Örneğin, yetki denetimleri, uygulama bir kuyruk açtığında gerçekleştirilir. Bunlar, uygulama kuyruğa ileti yerleştirdiğinde ya da kuyruktan ileti aldıklarında gerçekleştirilmez.

Bir uygulama bir nesneyi açtığında, nesne üzerinde gerçekleştirmesi gereken işlem tiplerini belirtir. Örneğin, bir uygulama üzerindeki iletilere göz atmak, ileti almak, ancak ileti koymak için bir kuyruk açabilir, ancak bu iletiyi bir ileti yazmayabilir. Her işlem tipi için, kuyruk yöneticisi, uygulamayla ilişkili kullanıcı kimliğinin bu işlemi gerçekleştirme yetkisine sahip olduğunu denetler.

Bir uygulama bir kuyruk açtığında, nesne tanımlayıcısının `ObjectName` alanında belirtilen nesneye göre yetki denetimi gerçekleştirilir. `ObjectName` alanı, `MQOPEN` ya da `MQPUT1` çağrılarında kullanılır. Nesne bir diğer ad kuyruğunysa ya da uzak bir kuyruk tanımlıysa, yetki denetimleri nesnenin kendisine karşı gerçekleştirilir. Bunlar, diğer ad kuyruğunun ya da uzak kuyruk tanımlamasının çözümlediği kuyruklarda gerçekleştirilmez. Bu, kullanıcının ona erişmek için izin gerekmediği anlamına gelir. Ayrıcalıklı kullanıcılara kuyruk yaratma yetkisi sınırlayın. Bunu yapmazsanız, kullanıcılar bir diğer ad oluşturarak normal erişim denetimini atlayabilirler.

Bir uygulama uzak bir kuyruğa belirtik olarak başvuruda bulunabilir. Nesne tanımlayıcısındaki `ObjectName` ve `ObjectQMgrName` alanlarını uzak kuyruk ve uzak kuyruk yöneticisi adlarına ayarlar. Yetki denetimleri, uzak kuyruk yöneticisiyle aynı adı taşıyan iletim kuyruğuna ilişkin olarak gerçekleştirilir. z/OS' ta, RACF kuyruk tanıtımsında uzak kuyruk yöneticisi adıyla eşleşen bir denetim yapılır. Multiplatforms' ta, kümeleme kullanılıyorsa, uzak kuyruk yöneticisi adıyla eşleşen RQMNAME

tanıtıma yönelik bir denetim yapılır. Bir uygulama, nesne tanımlayıcısındaki `ObjectName` alanını küme kuyruğunun adına ayarlayarak belirtik olarak bir küme kuyruğuna başvurabilir. Yetki denetimleri, küme iletim kuyruğuna (`SYSTEM.CLUSTER.TRANSMIT.QUEUE`) ilişkin olarak gerçekleştirilir.

Dinamik bir kuyruğa ilişkin yetki, türetildiği model kuyruğuna dayalıdır, ancak aynı zamanda aynı olmayabilir; bkz. not 1.

Kuyruk yöneticisinin yetki denetimleri için kullandığı kullanıcı kimliği işletim sisteminden elde edilir. Kullanıcı kimliği, uygulama kuyruk yöneticisine bağlandığında elde edilir. Uygun bir şekilde yetkili bir uygulama, alternatif bir kullanıcı kimliği belirterek bir `MQOPEN` çağrısı yayınlayabilir; daha sonra alternatif kullanıcı kimliği üzerinde erişim denetimi denetimleri yapılır. Diğer bir kullanıcı kimliği kullanılması, uygulama ile ilişkili kullanıcı kimliğini değiştirmez, yalnızca erişim denetimi denetimleri için kullanılan kullanıcı kimliğini değiştirmez.

Bir uygulama, `MQSUB` çağrısını kullanarak bir konuya abone olduğunda

Bir uygulama bir konuya abone olduğunda, gerçekleştirmesi gereken işlem tipini belirtir. Bir abonelik yaratır, var olan bir aboneliği değiştirir ya da değiştirmeden var olan bir aboneliğin sürdürülmesini sağlar. Her işlem tipi için, kuyruk yöneticisi, uygulamayla ilişkili kullanıcı kimliğinin, işlemi gerçekleştirme yetkisine sahip olduğunu denetler.

Bir uygulama bir konuya abone olduğunda, konu ağacında bulunan konu nesnelerine karşı yetki denetimi gerçekleştirilir. Konu nesneleri, uygulamanın abone olduğu konu ağacındaki nokta ya da bu noktadaki noktadır. Yetki denetimleri birden fazla konu nesnesi üzerinde denetim içerebilir. Kuyruk yöneticisinin yetki denetimleri için kullandığı kullanıcı kimliği işletim sisteminden elde edilir. Kullanıcı kimliği, uygulama kuyruk yöneticisine bağlandığında elde edilir.

Kuyruk yöneticisi, yetki denetimlerini abone kuyruklarında gerçekleştirir, ancak yönetilen kuyruklarda işlem yapar.

When an application deletes a permanent dynamic queue using an `MQCLOSE` call

`MQCLOSE` çağrısında belirtilen nesne tanıtıcı değeri, kalıcı dinamik kuyruğu yaratan `MQOPEN` çağrısı tarafından döndürülen aynı anda olmayabilir. Farklı bir değer varsa, kuyruk yöneticisi, `MQCLOSE` çağrısını yayınlayan uygulamayla ilişkili kullanıcı kimliğini denetler. Kullanıcı kimliğinin kuyruğu silme yetkisi olup olmadığını denetler.

Aboneliği kaldırmak için aboneliği kapatan bir uygulama bunu oluşturmadığında, bu uygulamayı kaldırmak için uygun yetkiye sahip olur.

Bir IBM MQ nesnesi üzerinde çalışan bir PCF komutu komut sunucusu tarafından işlendiğinde

Bu kural, bir PCF komutunun bir kimlik doğrulama bilgi nesnesi üzerinde çalıştığı vakayı içerir.

Yetki denetimleri için kullanılan kullanıcı kimliği, PCF komutunun ileti tanımlayıcısındaki `UserIdentifier` alanında bulunan tanıtıcıdır. Bu kullanıcı kimliğinin, komutun işlendiği kuyruk yöneticinde gerekli yetkilerin olması gerekir. Bir Escape PCF komutu içinde kapsüllenmiş eşdeğer MQSC komutu da aynı şekilde işlem görür. `UserIdentifier` (Kullanıcı Kimliği) alanı ve nasıl ayarlansa hakkında daha fazla bilgi için bkz. “İleti bağlamı” sayfa 86.

IBM i **On IBM i, when a user issues a CL command in Group 2 that operates on an IBM MQ object**

Bu kural, Grup 2 'deki bir CL komutunun bir kimlik doğrulama bilgi nesnesi üzerinde çalıştığı vakayı içerir.

Kullanıcının, komutla ilişkili bir IBM MQ nesnesi üzerinde işlem yapmak için yetkiye sahip olup olmadığını belirlemek için denetimler gerçekleştirilir. Bu denetimler, kullanıcı `QMQMADM` grubunun bir üyesi değilse ya da `*ALLOBJ` yetkisine sahip değilse gerçekleştirilir. Gereken yetki, komutun nesne üzerinde gerçekleştireceği işlemin tipine bağlıdır. Örneğin, **CHGMQMQ**komutu, MQM kuyruğunu değiştir komutu, komutun belirlediği kuyruğun özniteliklerini değiştirmesini gerektirir. Bunun tersine, **DSPMQMQ**komutu, MQM kuyruğunu görüntüle komutu, komutun belirttiği kuyruğun özniteliklerini görüntülüme yetkisini gerektirir.

Birçok komut birden çok nesne üzerinde çalışır. Örneğin, **DLTMQMQ**komutunu vermek için, MQM kuyruğunu silin, aşağıdaki yetkiler gereklidir:

- Komutla belirlenen kuyruk yöneticisine bağlanma yetkisi

- Komut tarafından belirlenen kuyruğu silme yetkisi

Bazı komutlar hiçbir nesne üzerinde işlem görmez. Bu durumda, kullanıcı yalnızca IBM i yetkisini gerektirir ve bu komutlardan birini yayınlamayı gerektirir. **STRMQMLSR**, MQM Listener 'ı başlatın, bu tür bir komutla ilgili bir örnektir.

Diğer kullanıcı yetkisi

Bir uygulama bir nesneyi açtığında ya da bir konuya abone olduğunda, uygulama MQOPER, MQPUT1ya da MQSUB çağrısında bir kullanıcı kimliği sağlayabilir. Kuyruk yöneticisiyle, uygulama ile ilişkili olan yerine yetki denetimleri için bu kullanıcı kimliğini kullanmasını isteyebilir.

Uygulama, yalnızca aşağıdaki koşulların her ikisi de karşılanırsa, nesneyi açmada başarılı olur:

- Uygulamayla ilişkili kullanıcı kimliği, yetki denetimleri için farklı bir kullanıcı kimliği sağlama yetkisine sahiptir. Uygulamanın *diğer kullanıcı yetkisine*sahip olduğu söyleniyor.
- Uygulama tarafından sağlanan kullanıcı kimliği, istenen işlem tipleri için nesneyi açma ya da konuya abone olma yetkisine sahiptir.

İleti bağlamı

İleti bağlamı bilgileri, iletiyi alan uygulamanın, iletiyi oluşturan iletiyi bulmasını sağlayan bir iletiyi sağlar. Bilgiler ileti tanımlayıcısında yer alan alanlarda tutulur ve alanlar üç mantıksal bölüme ayrılır

Bu parçalar aşağıdaki gibidir:

kimlik bağlamı
Bu alanlar, iletiyi kuyruğa yerleştiren uygulamanın kullanıcısına ilişkin bilgiler içerir.

kaynak bağlamı
Bu alanlar, uygulamanın kendisi ve ileti kuyruğuna konduğunda, uygulamanın kendisiyle ilgili bilgileri içerir.

kullanıcı bağlamı
Bu alanlar, uygulamaların kuyruk yöneticisinin teslim etmesi gereken iletileri seçmek için kullanabilecekleri ileti özelliklerini içerir.

Bir uygulama bir iletiyi kuyruğa yerleştirdiğinde, uygulama kuyruk yöneticisinde bu iletteki bağlam bilgilerini oluşturmasını isteyebilir. Varsayılan işlem budur. Diğer bir seçenek olarak, bağlam alanlarının hiçbir bilgi içermemesini de belirtebilir. Bir uygulamayla ilişkili kullanıcı kimliği, bunların hiçbirini yapmak için özel bir yetkiye sahip olmamasını gerektirir.

Bir uygulama, bir iletide kimlik bağlamı alanlarını ayarlayabilir ve kuyruk yöneticisinin kaynak bağlamı oluşturmasını ya da tüm bağlam alanlarını ayarlayabilmesini sağlar. Bir uygulama, kimlik bağlamı alanlarını, bir kuyruğa yerleştirdiği bir iletiye aldığı bir iletiden de geçirebilir ya da tüm bağlam alanlarını geçirebilir. Ancak, bir uygulamayla ilişkili kullanıcı kimliği, bağlam bilgilerinin ayarlanması ya da geçişi için yetki gerektirir. Bir uygulama, iletileri koymak üzere olduğu kuyruğu açtığında bağlam bilgilerini ayarlamayı ya da geçirmeyi amaçladığını ve yetkisinin bu sırada denetlendiğini belirtir.

Aşağıda, bağlam alanlarının her birine ilişkin kısa bir açıklama yer alıyor:

Kimlik bağlamı

UserIdentifier
İletiyi koyan uygulamayla ilişkili kullanıcı kimliği. Kuyruk yöneticisi bu alanı ayarlarsa, uygulama kuyruk yöneticisine bağlandığında, işletim sisteminden elde edilen kullanıcı kimliği olarak ayarlanır.

AccountingToken
İletinin bir sonucu olarak yapılan çalışmalardan sorumlu olarak kullanılabilecek bilgiler.

ApplIdentityVerileri
Bir uygulamayla ilişkilendirilen kullanıcı kimliğinin, kimlik bağlamı alanlarını belirleme yetkisi varsa ya da tüm bağlam alanlarını ayarlamaya ilişkin yetkisi varsa, uygulama bu alanı tanıtıcı ile ilgili herhangi bir değere ayarlayabilir. Kuyruk yöneticisi bu alanı ayarlarsa, boş olarak ayarlanır.

Kaynak bağlamı

PutApplTipi
Örneğin, iletiyi koyan uygulamanın tipi; örneğin, CICS işlemi.

PutApplAdı
İletiyi koyan uygulamanın adı.

PutDate
İletinin konulduğu tarih.

PutTime
İletinin konulduğu saat.

ApplOriginVerileri
Bir uygulamayla ilişkili kullanıcı kimliği tüm bağlam alanlarını belirleme yetkisine sahipse, uygulama bu alanı kaynak olarak herhangi bir değere ayarlayabilir. Kuyruk yöneticisi bu alanı ayarlarsa, boş olarak ayarlanır.

Kullanıcı bağlamı

Aşağıdaki değerler **MQINQMP** ya da **MQSETMP**için desteklenir:

MQPD_USER _BAğLAMı

Özellik, kullanıcı bağlamıyla ilişkilendirilir.

MQSETMP çağrısını kullanarak, kullanıcı bağlamıyla ilişkili bir özelliği ayarlayabilmek için özel bir yetki gerekmez.

Bir V7.0 ya da sonraki kuyruk yöneticisi üzerinde, kullanıcı bağlamıyla ilişkili bir özellik, MQOO_SAVE_ALL_CONTEXT için açıklandığı şekilde saklanır. MQOO_PASS_ALL_CONTEXT ile belirtilen bir MQPUT, özelliğin saklanan bağlamdan yeni iletiye kopyalanmasına neden oluyor.

MQPD_NO_CONTEXT

Özellik bir ileti bağlamıyla ilişkilendirilmemiş.

Tanınmayan bir değer MQRC_PD_ERROR ile reddedilir. Bu alanın başlangıç değeri **MQPD_NO_CONTEXT**' dir.

Bağlam alanlarının her birine ilişkin ayrıntılı açıklamalar için MQMD-Message Descriptorbaşlıklı konuya bakın. İleti bağlamının nasıl kullanılacağı hakkında daha fazla bilgi için bkz. İleti bağlamı.

ULW IBM i IBM i *IBM i , UNIX, Linux, and Windows sistemlerinde IBM MQ nesneleriyle çalışma yetkisi*

IBM MQ ile sağlanan yetki hizmeti bileşenine, *object authority manager* (OAM) adı verilir. Kimlik doğrulama ve yetkilendirme denetimleri aracılığıyla erişim denetimi sağlar.

Kimlik doğrulaması.
The authentication check performed by the OAM provided with IBM MQ is basic, and is only performed in specific circumstances. Yüksek düzeyde güvenli bir ortamda beklenen katı gereksinimleri karşılamaya yönelik değildir.

OAM, bir uygulama kuyruk yöneticisine bağlandığında kimlik doğrulama denetimini gerçekleştirir ve aşağıdaki koşullar doğru olur:

- Bağlantı uygulama tarafından bir MQCSP yapısı sağlandıysa ve
- MQCSP yapısındaki *AuthenticationType* özniteliğine MQCSP_AUTH_USER_ID_AND_PWD değeri verilir ve
- Yapılandırılan AUTHINFO nesnesindeki CHCKLOCL ya da CHKCCLNT değeri 'NONE' değil

OAM ' daki kimlik doğrulama adımları, kullanıcı adının çok fazla yanlış parola sınaması denemelerine sahip olmadığından emin olmak gibi ek denetimleri gerçekleştirmek üzere yapılandırılmış olan işletim sistemi hizmetlerini kullanarak parolayı doğrular.

Yeni bir yetki hizmeti bileşeni yazarsanız ya da bir satıcıdan aldığınız diğer kimlik doğrulama mekanizmaları için bu olanak kullanılabilir.

Yetki.
Yetki denetimleri kapsamlı ve çoğu normal gereksinimleri karşılamaya yönelikir.

Bir uygulama, kuyruk yöneticisine, kuyruğa, sürece, konuya ya da ad listesine erişmek için bir MQI çağrısı yayınlarken, yetkilendirme denetimleri gerçekleştirilir. Örneğin, komut sunucusu tarafından bir komut gerçekleştirilmekte olan bir komut, diğer zamanlarda da gerçekleştirilir.

On IBM i IBM i , UNIX, Linux, and Windows systems, the *yetkilendirme hizmeti* provides the access control when an application issues an MQI call to access an IBM MQ object that is a queue manager, queue, process, topic, or namelist. Bu, alternatif kullanıcı yetkisi ve bağlam bilgilerini belirleme ya da geçirme yetkisi için denetimleri içerir.

Windows Windows üzerinde, OAM, UAC etkin olduğunda bile, Yöneticilerin üyelerine tüm IBM MQ nesnelerine erişim yetkisi verir. Ayrıca, Windows sistemlerinde, SYSTEM hesabında IBM MQ kaynaklarına tam erişim olanağı bulunur.

Ayrıca, yetki hizmeti, bir PCF komutu bu IBM MQ nesnelerinden birinde ya da bir kimlik doğrulama bilgisi nesnesinden birinde çalıştığında yetki denetimi de sağlar. Bir Escape PCF komutu içinde kapsüllenmiş eşdeğer MQSC komutu da aynı şekilde işlem görür.

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

Yetkilendirme hizmeti, bir ya da daha fazla *kurulabilir hizmet bileşeni*tarafından gerçekleştirildiği anlamına gelen bir *kurulabilir hizmettir*. Her bileşen, belgelenmiş bir arabirim kullanılarak çağrılır. Bu, kullanıcıların ve satıcıların, IBM MQ ürünleri tarafından sağlanan bileşenleri genişletmeleri ya da değiştirmeleri için bileşenler sunmalarına olanak sağlar.

IBM MQ ile sağlanan yetki hizmeti bileşeni, nesne yetkili yöneticisi (OAM) olarak adlandırılır. OAM, yarattığınız her kuyruk yöneticisi için otomatik olarak etkinleştirilir.

OAM, erişimi denetleyen her bir IBM MQ nesnesi için bir erişim denetleme listesi (EDL) sağlar. UNIX and Linux sistemlerinde, bir EDL ' de yalnızca grup tanıtıcıları görüntülenebilir. Bu, bir grubun tüm üyelerinin aynı yetkiyi sahip olduğu anlamına gelir. IBM i IBM i ve üzerinde Windows sistemlerinde, her iki kullanıcı kimliği ve grup tanıtıcısı bir EDL ' de görüntülenebilir. Bu, yetkililerin bireysel kullanıcılara ve gruplara tanınabileceği anlamına gelir.

12 karakter sınırlaması hem grup, hem de kullanıcı kimliği için geçerlidir. UNIX platformları genel olarak bir kullanıcı kimliğinin uzunluğunu 12 karakterle sınırlar. AIX ve Linux bu sınırı yükseltti; ancak IBM MQ , tüm UNIX platformlarında 12 karakterlik bir kısıtlamayı gözlemlemeye devam eder. 12 karakterden uzun bir kullanıcı kimliği kullanırsanız, IBM MQ bu tanıtıcıyı "UNKNOWN"değeriyle değiştirir. Do not define a user ID with a value of "BILINMIYOR".

OAM, bir kullanıcının kimliğini doğrulayabilir ve uygun kimlik bağlamı alanlarını değiştirebilir.
Bu seçeneği, MQCONNX çağrısında bir bağlantı güvenliği değiştirgeleri yapısı (MQCSP) belirterek etkinleştirmenizi sağlar. Yapı, uygun kimlik bağlamı alanlarını belirleyen OAM Authenticate User (MQZ_AUTHENTICATE_USER) işlevine geçirilir. Bir IBM MQ istemcisinden bir MQCONNX bağlantısı varsa, MQCSP içindeki bilgiler istemcinin istemci bağlantısı ve sunucu bağlantısı kanalı üzerinden bağlanacağı kuyruk yöneticisine akıtılır. Bu kanalda güvenlik çıkışları tanımlanırsa, MQCSP her güvenlik çıkışa geçirilir ve çıkışa göre değiştirilebilir. Güvenlik çıkışları MQCSP ' yi de yaratabilir. Bu bağlamdaki güvenlik çıkışlarının kullanılmasına ilişkin ayrıntılar için Kanal güvenlik çıkış programlarıbaşlıklı konuya bakın.

Uyarı: Bazı durumlarda, istemci uygulaması için bir MQCSP yapısındaki parola, düz metindeki bir ağ üzerinden gönderilir. İstemci uygulaması parolalarının uygun şekilde korunmasını sağlamak için bkz. IBM MQCSP parola koruması.

On UNIX, Linux and Windows systems, the control command **setmqaut** grants and revokes authorities and is used to maintain the ACLs. Örneğin, komut:

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

Voyager grubunun üyelerinin MOON.EUROPA , kuyruk yöneticisi Jüpiter 'e aittir. Bu, üyelerin kuyruktan ileti almalarını sağlar. Daha sonra bu yetkileri iptal etmek için aşağıdaki komutu girin:

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

Komut:

```
setmqaut -m JUPITER -t queue -n MOON.* -g VOYAGER +put
```

Voyager grubunun üyelerinin, `MOON.` karakterleriyle başlayan bir adla herhangi bir kuyruğa ileti koymasına olanak sağlar. MOON.* soysal bir tanıtımın adıdır.*Soysal tanıtım* , tek bir **setmqaut** komutunu kullanarak bir nesne kümesi için yetki vermenize olanak sağlar.

Bir kullanıcının ya da grubun belirli bir nesne için sahip olduğu yürürlükteki yetkileri görüntülemek için **dspmqaut** denetim komutu kullanılabilir.The control command **dmpmqaut** is also available to display the current authorities associated with generic profiles.

IBM i Bir denetimci, IBM i' ta yetki vermek için GRTMQMAUT CL komutunu ve RVKMQMAUT Denetim dili (CL) komutunu yetkililerden geri almak için kullanır. Genel tanıtımlar da kullanılabilir.Örneğin, CL komutu:

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

Bir **setmqaut** komutunun önceki örneğiyle aynı işlevi sağlar; grup VOYAGER üyelerinin, `MOON.` karakterleriyle başlayan bir adla herhangi bir kuyruğa ileti koymasını sağlar.

IBM i DPMQMAUT CL komutu, kullanıcının ya da grubun belirli bir nesne için sahip olduğu yürürlükteki yetkileri görüntüler. WRKMQMAUT ve WRKMQMAUTD CL komutlarının, nesnelerle ve soysal tanıtımla ilişkili yürürlükteki yetkilerle birlikte çalışabilmesini sağlar.

Herhangi bir yetki denetimi istemiyorsanız, örneğin, bir test ortamında, OAM ' yi devre dışı bırakabilirsiniz.

Multi *OAM komutlarına erişmek için PCF ' nin kullanılması*

IBM i, UNIX, Linux, and Windows sistemlerinde, OAM yönetim komutlarına erişmek için PCF komutlarını kullanabilirsiniz.

PCF komutları ve eşdeğer OAM komutları aşağıdaki gibidir:

Çizelge 8. PCF komutları ve eşdeğer OAM komutları

PCF komutu	**OAM komutu**
Yetki Kayıtlarını Sorgula	dmpmqaut
Bilgi Varlığı Yetkilisi	dspmqaut
Yetki Kaydını Ayarla	setmqaut
Yetki Kaydını Sil	setmqaut ile -remove seçeneği

setmqaut ve **dmpmqaut** komutları, mqm grubunun üyeleri ile sınırlandırılmıştır. Eşdeğer PCF komutları, kuyruk yöneticisinde dsp ve chg yetkilerine sahip tüm gruplardaki kullanıcılar tarafından yürütülebilir.

Bu komutların kullanılmasıyla ilgili ek bilgi için Programlanır Komut Biçimlerine Girişbaşlıklı konuya bakın.

z/OS z/OSüzerinde IBM MQ nesneleriyle çalışma yetkisi

z/OS' ta, MQI çağrılarıyla ilişkili yedi yetki denetimi kategorisi vardır. Belirli RACF profillerini tanımlamanız ve bu profillere uygun erişim vermelisiniz. Kaç kullanıcı kimliği denetlendiğini denetlemek için *RESLEVEL* tanıtımını kullanın.

MQI ' ya çağrılarla ilişkili yedi yetki denetimi kategorisi:

Bağlantı güvenliği
Bir uygulama bir kuyruk yöneticisine bağlandığında gerçekleştirilen yetki denetimleri

Kuyruk güvenliği
Uygulama bir kuyruğu açtığında ya da kalıcı bir dinamik kuyruğu sildiğinde gerçekleştirilen yetki denetimleri

Süreç güvenliği
Bir uygulama bir süreç nesnesini açtığında gerçekleştirilen yetki denetimleridir

Ad listesi güvenliği
Bir uygulama bir ad listesi nesnesini açtığında gerçekleştirilen yetki denetimlerinin

Diğer kullanıcı güvenliği
Bir uygulama, bir nesneyi açarken başka bir kullanıcı yetkisi istediğinde gerçekleştirilen yetki denetimleridir.

Bağlam güvenliği
Bir uygulama bir kuyruğu açtığında ve bağlam bilgilerini kuyruğa yerleştirdiği iletilerde ayarlamayı ya da geçirmeyi amaçladığını belirten yetki denetimleri gerçekleştirilir.

Konu güvenliği
Bir uygulama bir konuyu açtığında gerçekleştirilen yetki denetimlerinin

Her yetki denetimi kategorisi, komut güvenliği ve komut kaynağı güvenliği uygulananlarla aynı şekilde uygulanır. Belirli RACF tanıtımlarını tanımlamanız ve gerekli gruplar ve kullanıcı kimlikleri için gerekli düzeylerde bu tanıtımlara erişebilmeleri gerekir. Kuyruk güvenliği için erişim düzeyi, uygulamanın bir kuyruğun üzerinde gerçekleştirebileceği işlem tiplerini belirler. Bağlam güvenliği için, erişimin düzeyi, uygulamanın aşağıdakileri yapabildiğini belirler:

- Tüm bağlam alanlarını geçir
- Tüm bağlam alanlarını geçirin ve kimlik bağlamı alanlarını ayarlayın
- Tüm bağlam alanlarını geçir ve ayarla

Her yetki denetimi kategorisi, anahtar tanıtımları tanımlanarak açılabilir ya da kapatılabilir.

Bağlantı güvenliği dışında tüm kategoriler toplu olarak *API-kaynak güvenliği*olarak bilinir.

Varsayılan olarak, toplu iş bağlantısı kullanan bir uygulamadan bir MQI çağrısının sonucu olarak bir API-kaynak güvenlik denetimi gerçekleştirildiğinde, yalnızca bir kullanıcı kimliği işaretlendi. When a check is performed as a result of an MQI call from a CICS or IMS application, or from the channel initiator, two user IDs are checked.

Ancak, bir *RESVELL tanıtımı*tanımlayarak, sıfır, bir ya da iki kullanıcı kimliği olup olmadığını denetleyebilirsiniz. Denetlenen kullanıcı kimliklerinin sayısı, bir uygulama kuyruk yöneticisine bağlandığında ve kullanıcı kimliğinin RESLEVELL tanıtımı için sahip olduğu erişim düzeyine bağlandığında, bağlantı tipiyle ilişkilendirilen kullanıcı kimliği tarafından belirlenir. Her bağlantı tipiyle ilişkilendirilen kullanıcı kimliği:

- Toplu iş bağlantılarına ilişkin bağlama görevinin kullanıcı kimliği
- CICS bağlantıları için CICS adres alanı kullanıcı kimliği
- IMS bağlantıları için IMS bölgesi adres alanı kullanıcı kimliği
- Kanal başlatıcı bağlantıları için kanal başlatıcı adres alanı kullanıcı kimliği

z/OSüzerindeki IBM MQ nesneleriyle çalışma yetkisiyle ilgili daha fazla bilgi için bkz. “z/OSüzerinde IBM MQ yönetimi yetkisi” sayfa 81.

Uzaktan ileti sistemine ilişkin güvenlik

Bu bölümde, güvenlik ile uzaktan ileti sistemi konuları ele verilmektedir.

Kullanıcılara, IBM MQ olanaklarını kullanma yetkisi sağlamanız gerekir. Bu, nesnelerle ve tanımlarla ilgili olarak yapılacak işlemlere göre düzenlenmiştir. Örneğin:

- Kuyruk yöneticileri yetkili kullanıcılar tarafından başlatılabilir ve durdurulabilir
- Uygulamaların kuyruk yöneticisine bağlanması ve kuyruklar kullanma yetkisi olması gerekir
- İleti kanalları yetkili kullanıcılar tarafından yaratılmalı ve denetlenmiş olmalıdır
- Nesneler kitaplıklarda tutulur ve bu kitaplıklara erişimler kısıtlanabilir

Uzak bir yerdeki ileti kanalı aracısının, teslim edilmekte olan iletinin, bu uzak yerde bu işlemi yapma yetkisi olan bir kullanıcıdan kaynaklandığı denetlememesi gerekir. Ayrıca, MCA 'ların uzaktan başlatılabildiği gibi, MCA' larınızı başlatmaya çalışan uzak işlemlerin bunu yapmaya yetkili olduğunu doğrulamanız gerekebilir. Bununla başa çıkabilmek için dört olası yol var:

1. Gelen iletiler kuyruklarınıza yerleştirilecek zaman için hangi kullanıcının yetki denetimi için kullanıldığını denetlemek üzere, RCVR, RQSTR ya da CLUSTRVR kanal tanımlamasındaki PutAuthority özniteliğinin uygun şekilde kullanılmasını sağlar. MQSC Command Reference 'da DESCRIPTION CHANNEL komut tanımına bakın.
2. İstenmeyen bağlantı girişimlerini reddetmek ya da aşağıdakine dayalı bir MCAUSER değeri ayarlamak için kanal kimlik doğrulama kayıtlarını uygulayın: uzak IP adresi, uzak kullanıcı kimliği, sağlanan TLS Konusu Ayırt Edici Adı (DN) ya da uzak kuyruk yöneticisi adı.
3. Karşılık gelen ileti kanalının yetkilendirildiğinden emin olmak için *kullanıcı çıkışı* güvenlik denetimini gerçekleştirin. İlgili kanalı bulunduran kuruluşun güvenliği, tek tek iletileri denetlemenize gerek kalmaması için tüm kullanıcıların düzgün şekilde yetkilendirilmelerini sağlar.
4. Yetkilendirme için tek tek iletilerin incelendiğinden emin olmak için *kullanıcı çıkışı* ileti işleme işlemini gerçekleştirin.

IBM i *IBM MQ for IBM i nesnelerinin güvenliği*

Bu bölümde, güvenlik ile uzaktan ileti sistemi konuları ele verilmektedir.

Kullanıcılara, IBM MQ for IBM i olanaklarından kullanım için yetki sağlamanız gerekir. Bu yetki, nesnelerle ve tanımlarla ilgili olarak yapılacak işlemlere göre düzenlenir. Örneğin:

- Kuyruk yöneticileri yetkili kullanıcılar tarafından başlatılabilir ve durdurulabilir
- Uygulamaların kuyruk yöneticisine bağlanması ve kuyrukların kullanılması için yetki sahibi olması gerekir
- Yetkili kullanıcılar tarafından ileti kanallarının oluşturulması ve denetlenmeleri gerekir

Uzak bir yerdeki ileti kanalı aracısının, teslim edilmekte olan iletinin, bu uzak yerde iletiyi idava yetkisi olan bir kullanıcıdan türetilmiş olduğunu denetlememesi gerekir. Ayrıca, MCA 'ların uzaktan başlatılabildiği gibi, MCA' larınızı başlatmaya çalışan uzak işlemlerin bunu yapmaya yetkili olduğunu doğrulamanız gerekebilir. Bununla başa çıkabilmek için dört olası yol var:

- Kanal tanımlamasındaki kararname, iletilerin kabul edilebilir *bağlam* yetkisi içermesi gerektiğini, aksi takdirde atılırlar.
- İstenmeyen bağlantı girişimlerini reddetmek ya da aşağıdakilerden birine dayalı bir MCAUSER değeri ayarlamak için kanal kimlik doğrulama kayıtlarını uygulayın: uzak IP adresi, uzak kullanıcı kimliği, sağlanan TLS Ayırt Edici Adı (DN) ya da uzak kuyruk yöneticisi adı.
- İlgili ileti kanalının yetkilendirildiğinden emin olmak için kullanıcı çıkışı güvenlik denetimini uygulayın. İlgili kanalı bulunduran kuruluşun güvenliği, tek tek iletileri denetlemenize gerek kalmaması için tüm kullanıcıların düzgün şekilde yetkilendirilmelerini sağlar.
- Yetki için tek tek iletilerin incelendiğinden emin olmak için kullanıcı çıkışı ileti işleme işlemini uygulayın.

Aşağıda, IBM MQ for IBM i ' in güvenliği işlemesiyle ilgili bazı bilgiler bulunmaktadır:

- Kullanıcılar IBM itarafından tanımlanır ve doğrulanır.

- Uygulamalar tarafından çağrılan kuyruk yöneticisi hizmetleri, kuyruk yöneticisi kullanıcı tanıtımının yetkisiyle çalıştırılır, ancak kullanıcının sürecindeki yetkiyle çalıştırılır.
- Kullanıcı komutları tarafından çağrılan kuyruk yöneticisi hizmetleri, kuyruk yöneticisi kullanıcı tanıtımının yetkisiyle çalıştırılır.

Linux UNIX *UNIX and Linuxüzerindeki nesnelerin güvenliği*

Bu kimlik IBM MQ denetim komutlarını kullanacaksa, yönetim kullanıcılarının sisteminizdeki mqm grubunun bir parçası (kök dahil) olmalıdır.

Amqcrsta 'yı her zaman "mqm" kullanıcı kimliği olarak çalıştırmalısınız.

UNIX and Linuxüzerindeki kullanıcı kimlikleri

Kuyruk yöneticisi tüm büyük ya da karışık büyük/küçük harf kullanıcı tanıtıcılarını küçük harfe dönüştürür. Daha sonra kuyruk yöneticisi, kullanıcı tanıtıcılarını bir iletinin bağlam kısmına ekler ya da yetkilendirmelerini denetler. Bu nedenle, yetkiler yalnızca küçük harfli tanıtıcılara dayalıdır.

Windows *Windows sistemlerindeki nesnelerin güvenliği*

Administration users must be part of both the mqm group and the administrators group on Windows systems if this ID is going to use IBM MQ administration commands.

Windows sistemlerindeki kullanıcı kimlikleri

Windows sistemlerinde, *herhangi bir ileti çıkışı kurulu değilse*, kuyruk yöneticisi büyük ya da karışık büyük harfli kullanıcı tanıtıcılarını küçük harfe dönüştürür. Daha sonra kuyruk yöneticisi, kullanıcı tanıtıcılarını bir iletinin bağlam kısmına ekler ya da yetkilendirmelerini denetler. Bu nedenle, yetkiler yalnızca küçük harfli tanıtıcılara dayalıdır.

Sistemler arasında kullanıcı kimlikleri

Windowsdışındaki platformlar, UNIX and Linux sistemleri, iletilerde kullanıcı kimlikleri için büyük harfli karakterler kullanır. To allow Windows, UNIX and Linux systems to use lowercase user IDs in messages, the message channel agent (MCA) must carry out the appropriate conversions of alphabetic characters.

Windowssistemlerinde, UNIX and Linux sistemlerinde, iletilerde küçük harfli kullanıcı kimlikleri kullanılmasına izin vermek için, aşağıdaki dönüştürmeler bu altyapılarda Message Channel Agent (MCA) tarafından gerçekleştirilir:

Gönderme bitişindeki
Herhangi bir ileti çıkışı kurulu değilse, tüm kullanıcı kimliklerindeki alfabetik karakterler büyük harfli karakterlere dönüştürülür.

Alıcı uçta
Herhangi bir ileti çıkışı kurulu değilse, tüm kullanıcı kimliklerindeki alfabetik karakterler küçük harfe dönüştürülür.

Diğer herhangi bir nedenle UNIX, Linux, and Windows üzerinde bir ileti çıkışı sağlıyorsanız, otomatik dönüştürmeler gerçekleştirilmez.

Özel bir yetki hizmetinin kullanılması

IBM MQ , kurulabilir bir yetkilendirme hizmeti sağlar. Alternatif bir hizmet kurmayı seçebilirsiniz.

IBM MQ ile sağlanan yetki hizmeti bileşeni, Object Authority Manager (OAM) olarak adlandırılır. OAM, gereksinim duyardığınız yetkilendirme olanaklarını sağlamazsa, kendi yetkilendirme hizmeti bileşeninizi yazabilirsiniz. Bir yetki hizmeti bileşeni tarafından uygulanması gereken kurulabilir hizmet işlevleri, Kurulabilir hizmetler arabirimi başvuru bilgilerialtında açıklanmıştır.

İstemciler için erişim denetimi

Erişim denetimi kullanıcı kimliklerine dayalıdır. Denetlenecek birçok kullanıcı kimliği olabilir ve kullanıcı kimlikleri farklı biçimlerde olabilir. İstemciler tarafından kullanılmak üzere, MCAUSER sunucu bağlantısı kanal özelliğini özel bir kullanıcı kimliği değerine ayarlayabilirsiniz.

IBM MQ içindeki erişim denetimi kullanıcı kimliklerine dayalıdır. MQI çağrılarını yapan işlemin kullanıcı kimliği olağan bir şekilde kullanılır. For MQ MQI clients, the server-connection MCA makes MQI calls on behalf of MQ MQI clients. MQI çağrıları yapmak için kullanılacak sunucu bağlantısı MCA için diğer bir kullanıcı kimliği seçebilirsiniz. Diğer kullanıcı kimliği, istemci iş istasyonuyla ya da istemcilerin erişimini düzenlemek ve denetlemek için seçtiğiniz herhangi bir şeyle ilişkilendirilebilir. Kullanıcı kimliğinin, sunucuda MQI çağrılarını yayınlamak için gerekli yetkilerin sunucuya tahsis edilmesi gerekir. Diğer bir kullanıcı kimliğinin seçilmesi, istemcilerin, sunucu bağlantısı MCA ' nın yetkisiyle MQI çağrıları yapmasına izin verebilmek için tercih edilir.

Çizelge 9. Sunucu bağlantısı kanalı tarafından kullanılan kullanıcı kimliği

Kullanıcı kimliği	Kullanıldığı Zaman
Güvenlik çıkışı tarafından ayarlanan kullanıcı kimliği	Bir **CHLAUTH TYPE(BLOCKUSER)** kuralı tarafından engellenmedikçe kullanılır. Daha fazla bilgi için aşağıdaki bölüme (“Güvenlik çıkışındaki kullanıcı kimliğinin ayarlanması” sayfa 94) bakın.
CHLAUTH kuralı tarafından ayarlanan kullanıcı kimliği	Bir güvenlik çıkışı tarafından sona ermiş olmadıkça kullanılır. Ek bilgi için Kanal Kimlik Doğrulama Kayıtları başlıklı konuya bakın.
SVRCONN kanal tanımlamasındaki **MCAUSER** özniteisinde tanımlı olan kullanıcı kimliği	Bir güvenlik çıkışı ya da CHLAUTH kuralı tarafından geçersiz kılınmadıysa kullanılır.
İstemci makinesinden akıtılan kullanıcı kimliği	Hiçbir kullanıcı kimliği başka bir araç tarafından belirlenmezse kullanılır.
Sunucu bağlantısı kanalını başlatan kullanıcı kimliği	Hiçbir kullanıcı kimliği başka bir araç tarafından belirlenmezse ve hiçbir istemci kullanıcı kimliği aktarılmadığında kullanılır. Daha fazla bilgi için aşağıdaki bölüme (“Kanal programını çalıştıran kullanıcı kimliği” sayfa 94) bakın.

Sunucu bağlantısı MCA, MQI 'yi uzak kullanıcılar adına çağırdığı için, uzak istemciler adına ve potansiyel olarak çok sayıda kullanıcının erişimini nasıl yönetebileceğiniz, sunucu bağlantısı MCA' nın MQI çağrılarını yayınlayan sunucu bağlantısının güvenlik etkilerinin göz önünde bulundurulması önemlidir.

- Tek bir yaklaşım, sunucu bağlantısı MCA ' nın kendi yetkisi ile ilgili MQI çağrılarını yayınlamaya yönelik bir yaklaşıma sahip olması. Ancak, sunucu bağlantısı MCA ' nın güçlü erişim yetenekleriyle, istemci kullanıcıları adına MQI çağrıları yayınlamaması genellikle istenmeyen bir durum olduğundan emin olun.
- Başka bir yaklaşım, istemciden akan kullanıcı kimliğini kullanmandır. Sunucu bağlantısı MCA, istemci kullanıcı kimliğinin erişim yeteneklerini kullanarak MQI çağrılarını yayınlayabilir. Bu yaklaşım, dikkate alınması gereken bir dizi soru sunar:
  1. Farklı platformlarda kullanıcı kimliği için farklı biçimler vardır. Bu bazen, istemcideki kullanıcı kimliğinin biçimi, sunucudaki kabul edilebilir biçimlerden farklıysa sorunlara neden olur.
  2. Farklı ve değişen kullanıcı kimliklerine sahip birçok istemci vardır. Tanıtıcılar sunucuda tanımlanmalıdır ve yönetilmelidir.
  3. Kullanıcı kimliği güvenilir mi? Herhangi bir kullanıcı kimliği bir istemciden akıtılabilir, oturum açmış kullanıcının kimliği gerekmez. Örneğin, istemci, güvenlik nedenleriyle yalnızca sunucuda tanımlı olan tam `mqm` yetkisine sahip bir tanıtıcı akıp akabilir.
- Tercih edilen yaklaşım, sunucuda istemci tanımlama simgelerinin tanımlanmasıdır ve bu nedenle, istemci bağlantılı uygulamaların yeteneklerini sınırlayabilirsiniz. Bu genellikle, sunucu bağlantısı kanalı özelliği MCAUSER, istemciler tarafından kullanılacak özel bir kullanıcı kimliği değerine ayarlanarak

ve sunucu üzerinde farklı yetki düzeyine sahip istemciler tarafından kullanılmak üzere birkaç tanıtıcı tanımlanarak yapılır.

Güvenlik çıkışındaki kullanıcı kimliğinin ayarlanması

IBM MQ MQI clientsiçin, MQI çağrılarını içeren işlem sunucu bağlantısı MCA 'sıdır. Sunucu bağlantısı MCA tarafından kullanılan kullanıcı kimliği, MQCD ' nin `MCAUserIdentifier` ya da `LongMCAUserIdentifier` alanlarında yer alır. Bu alanların içeriği aşağıdaki gibi ayarlanır:

- Güvenlik çıkışlarına göre ayarlanan değerler
- İstemciden kullanıcı kimliği
- MCAUSER (sunucu-bağlantı kanalı tanımlamasında)

Güvenlik çıkışı, çağrıldığında, görünür olan değerleri geçersiz kılabilir.

- Sunucu bağlantısı kanalı MCAUSER özniteliği boş değer olarak ayarlanmışsa, MCAUSER değeri kullanılır.
- Sunucu bağlantısı kanalı MCAUSER özniteliği boş bırakılırsa, istemciden alınan kullanıcı kimliği kullanılır.
- Sunucu bağlantısı kanalı MCAUSER özniteliği boşsa ve istemciden herhangi bir kullanıcı kimliği alınmazsa, sunucu bağlantısı kanalını başlatan kullanıcı kimliği kullanılır.

Bir istemci tarafı güvenlik çıkışı kullanımda olduğunda, IBM MQ istemcisi, belirtilen kullanıcı kimliğini sunucuya akıtmaz.

Kanal programını çalıştıran kullanıcı kimliği

Kullanıcı kimliği alanları, sunucu bağlantısı kanalını başlatan kullanıcı kimliğinden türetildiğinde, aşağıdaki değer kullanılır:

- z/OS z/OSiçin, kanal başlatıcı için atanan kullanıcı kimliği, z/OS başlatma yordamları tablosuna göre görevi başlattı.
- TCP/IP (z/OS dışı) için, `inetd.conf` girişinden kullanıcı kimliği ya da dinleyiciye başlatan kullanıcı kimliği.
- SNA (non- z/OS) için, SNA Server girişinden kullanıcı kimliği ya da (Yok ise) gelen bağlantı isteği ya da dinleyiciye başlatan kullanıcı kimliği.
- NetBIOS ya da SPX için, dinleyiciye başlatan kullanıcı kimliği.

MCAUSER özniteliği boş olarak ayarlanmış bir sunucu-bağlantı kanalı tanımlıysa, istemciler bu kanal tanımlamasını, istemci tarafından sağlanan kullanıcı kimliği tarafından belirlenen erişim yetkisi bulunan kuyruk yöneticisine bağlanmak için kullanabilirler. Kuyruk yöneticisinin üzerinde çalıştığı sistem yetkisiz ağ bağlantılarına izin veriyorsa, bu bir güvenlik açığı olabilir. IBM MQ varsayılan sunucu bağlantısı kanalı (SYSTEM.DEF.SVRCONN), MCAUSER özniteliği boş olarak ayarlanmış olmalıdır. Yetkisiz erişimi önlemek için, varsayılan tanımın MCAUSER özniteliğini, IBM MQ MQ nesnelerine erişimi olmayan bir kullanıcı kimliğiyle güncelleyin.

Kullanıcı Kimlikleri

`runmqscile` bir kanal tanımladığınızda, kullanıcı kimliği tek tırnak içine alınmadıkça, MCAUSER özniteliği büyük harfe çevrilir.

ULW UNIX, Linux, and Windowsüzerindeki sunucular için, istemciden alınan `MCAUserIdentifier` alanının içeriği küçük harfe çevrilir.

IBM i IBM iüzerindeki sunucular için, istemciden alınan `LongMCAUserIdentifier` alanının içeriği büyük harfe çevrilir.

Linux UNIX UNIX and Linux sistemlerindeki sunucular için, istemciden alınan `LongMCAUserIdentifier` alanının içeriği küçük harfe çevrilir.

Varsayılan olarak, bir IBM MQ JMS bağ tanımı uygulaması kullanıldığında geçirilen kullanıcı kimliği, uygulamanın çalışmakta olduğu JVM ' nin kullanıcı kimliğidir.

Ayrıca, `createQueueConnection` yöntemi aracılığıyla bir kullanıcı kimliği de geçirmeniz mümkündür.

Planlama gizliliği

Verilerinizin gizli tutulmasını planlayın.

Gizlilik, uygulama düzeyinde ya da bağlantı düzeyinde uygulayabilirsiniz. TLS kullanmayı tercih edebilirsiniz, bu durumda dijital sertifikalar kullanımınızı planlamalısınız. Standart tesisler gereksinimlerinizi karşılamazsa, kanal çıkış programlarını da kullanabilirsiniz.

İlgili kavramlar

“Bağlantı düzeyi güvenlik ve uygulama düzeyi güvenliği karşılaştırılıyor” sayfa 95
Bu konu, bağlantı düzeyi güvenlik ve uygulama düzeyi güvenliğinin çeşitli yönleriyle ilgili bilgileri içerir ve iki güvenlik düzeyini karşılaştırır.

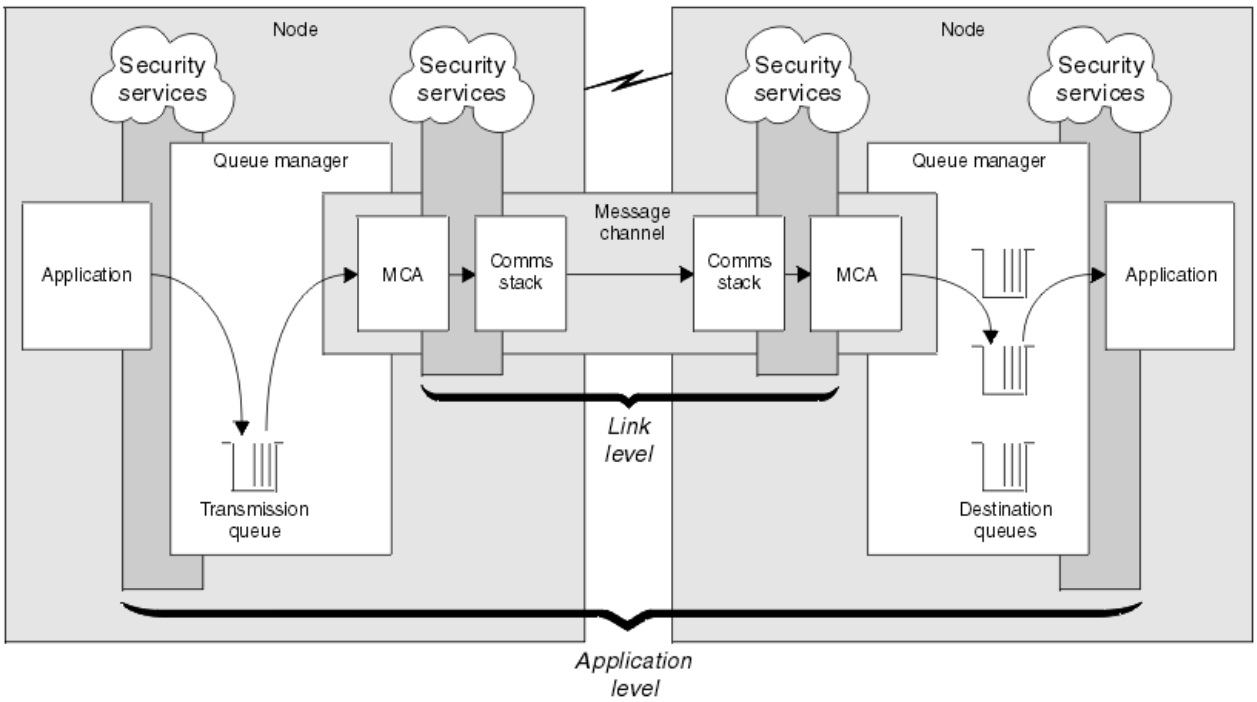
“Kanal çıkış programları” sayfa 99
Kanal çıkış programları , MCA ' nın işlem sırasında tanımlı yerlerde çağrılan programlardır. Kullanıcılar ve satıcılar kendi kanal çıkış programlarını yazabilirler. Bazıları IBMtarafından sağlanır.

“SSL/TLS ile kanalları koruma” sayfa 106
IBM MQ ' ta TLS desteği, kuyruk yöneticisi kimlik doğrulama bilgileri nesnesini ve çeşitli MQSC komutlarını kullanır. Ayrıca, dijital sertifikalar kullanımınızı da göz önünde bulundurmanız gerekir.

Bağlantı düzeyi güvenlik ve uygulama düzeyi güvenliği karşılaştırılıyor

Bu konu, bağlantı düzeyi güvenlik ve uygulama düzeyi güvenliğinin çeşitli yönleriyle ilgili bilgileri içerir ve iki güvenlik düzeyini karşılaştırır.

Bağlantı düzeyi ve uygulama düzeyi güvenliği Şekil 10 sayfa 95içinde gösterilmektedir.



Şekil 10. Bağlantı düzeyinde güvenlik ve uygulama düzeyi güvenliği

Kuyruklardaki iletilerin korunması

Bağlantı düzeyi güvenliği, bir kuyruk yöneticisinden başka bir kuyruk yöneticisinden aktarılırken iletileri koruyabilir. Özellikle, iletilerin güvenli olmayan bir ağ üzerinden iletilince önem önemlidir. Ancak, iletiler

kaynak kuyruk yöneticisinde, hedef kuyruk yöneticisinde ya da ara kuyruk yöneticisinde kuyruklarda saklarken, iletileri korumaz.

z/OS V 9.1.4 z/OS veri kümesi şifrelemesi, kuyruklarda saklanan iletilerin bazı korunmasını sağlayabilir, ancak yalnızca yerel bir kuyruk yöneticisinde kalan verilerdir. confidentiality for data at rest on IBM MQ for z/OS with data set encryption.bölümüne bakın. daha fazla bilgi için.

Uygulama düzeyinde güvenlik, iletiler kuyruklarda saklanırken iletileri koruyabilir ve dağıtımlı kuyruğa alma kullanılmadığında bile iletiler uygulanabilir. Bu, bağlantı düzeyi güvenlik ile uygulama düzeyi güvenliği arasındaki büyük farktır ve Şekil 10 sayfa 95' ta gösterilmektedir.

Denetlenen ve güvenilir ortamlarda çalışmayan kuyruk yöneticileri

Bir kuyruk yöneticisi denetimli ve güvenilir bir ortamda çalıştırılıyorsa, IBM MQ tarafından sağlanan erişim denetimi mekanizmaları, kuyruklarında saklanan iletileri korumak için yeterli olarak düşünülebilirdi. Bu özellikle, yalnızca yerel kuyruğa alma işlemi varsa ve iletiler kuyruk yöneticisini hiçbir zaman bırakmazsa, bu özellikle doğrudur. Bu durumda uygulama düzeyinde güvenlik gereksiz olarak düşünülebilebilir.

İletiler denetimli ve güvenilir bir ortamda da çalıştırılan başka bir kuyruk yöneticisine aktarılırsa ya da bu tür bir kuyruk yöneticisinden alınırsa, uygulama düzeyi güvenlik de gereksiz olarak düşünülebilir. İletiler denetimli ve güvenilir bir ortamda çalışmayan bir kuyruk yöneticisinden aktarıldığında ya da alınan iletiler aktarıldığında, uygulama düzeyi güvenliği gereksinmesi daha yüksek olur.

Maliyetteki farklılıklar

Uygulama düzeyi güvenlik, yönetim ve performans açısından bağlantı düzeyi güvenlik düzeylerinden fazlasına mal olabilir.

Yapılandırılması ve bakımı için daha fazla koşul olması nedeniyle, yönetim maliyetinin büyük olasılıkla daha büyük olması gerekir. Örneğin, belirli bir kullanıcının yalnızca belirli sayıda ileti göndermesini ve yalnızca belirli hedeflere ileti göndermesini sağlamanız gerekebilir. Tersi durumda, belirli bir kullanıcının yalnızca belirli tipteki iletileri almasını ve iletileri yalnızca belirli kaynaklardan almasını sağlamanız gerekebilir. Bağlantı düzeyi güvenlik hizmetlerini tek bir ileti kanalında yönetmek yerine, bu kanalda ileti alışverişi yapan her kullanıcı çifti için kurallar yapılandırmanız ve bakımının yapılması gerekir.

Bir uygulama her başlatıldığında ya da bir ileti aldığında, güvenlik hizmetleri çağrılırsa, başarım üzerinde bir etkisi olabilir.

Kuruluşlar, ilk önce bağlantı düzeyinde güvenliği göz önünde bulunmaya eğilimlidir, çünkü daha kolay bir şekilde uygulamak daha kolay olabilir. Bağlantı düzeyi güvenliğinin tüm gereksinimlerini yerine getirmediğini öğrenirlerse, uygulama düzeyindeki güvenliği göz önünde bulundururlar.

Bileşenlerin kullanılabilirliği

Genellikle, dağıtılmış bir ortamda, bir güvenlik hizmeti için en az iki sistem üzerinde bir bileşen gerekir. Örneğin, bir ileti bir sistemde şifrelenmiş ve başka bir ileti üzerinde şifresi çözülen bir ileti olabilir. Bu, hem bağlantı düzeyinde güvenlik, hem de uygulama düzeyinde güvenlik için geçerlidir.

Farklı platformlardaki farklı platformlarda, her biri farklı güvenlik işlevleriyle farklı türdeş olmayan bir ortamda, bir güvenlik hizmetinin gerekli bileşenleri, gerekli oldukları her platform için ve kullanımı kolay olan bir formda kullanılamayabilir. Bu sorun, özellikle çeşitli kaynaklardan bileşenlerde satın alarak kendi uygulama düzeyi güvenliğinize sağlamayı amaçlıyorsanız, bağlantı düzeyi güvenliği için daha çok uygulama düzeyi güvenlik sorunu olabilir.

Ölü bir mektup kuyruğundaki iletiler

Bir ileti uygulama düzeyinde güvenlik tarafından korunuyorsa, herhangi bir nedenle iletinin hedefine ulaşılamaması ve bir ileti kuyruğunda olması durumunda bir sorun ortaya çıkabilirsiniz. İleti açıklayıcısı ve ölü harf üstbilgisindeki bilgilerden iletinin nasıl işleneceğini çözemezseniz, uygulama verilerinin içeriğini incelemeniz gerekebilir. Uygulama verileri şifrelenmişse ve yalnızca amaçlanan alıcı şifresini çözebilirse bunu yapamazsınız.

Hangi uygulama düzeyinde güvenlik işlemi yapamıyor

Uygulama düzeyi güvenlik tam bir çözüm değil. Uygulama düzeyi güvenliği uygulansanız bile, bazı bağlantı düzeyi güvenlik hizmetleri de gerekebilir. Örneğin:

- Bir kanal başlatıldığında, iki MCA ' nın karşılıklı kimlik doğrulaması yine de bir gereksinim olabilir. Bu işlem yalnızca bir bağlantı düzeyi güvenlik hizmeti tarafından yapılabilir.
- Uygulama düzeyi güvenlik, yerleşik ileti tanımlayıcısını içeren iletim kuyruğu üstbilgisini, MQXQH ' yi koruyamaz. Ayrıca, IBM MQ kanal iletişim kuralı akışındaki verileri ileti verileri dışında da koruyabilir. Bu korumayı yalnızca bağlantı düzeyinde güvenlik sağlayabilir.
- Uygulama düzeyinde güvenlik hizmetleri bir MQI kanalının sunucu ucunda çağrılırsa, hizmetler, kanal üzerinden gönderilen MQI çağrılarının parametrelerini koruyamaz. Özellikle, bir MQPUT, MQPUT1ya da MQGET çağrısındaki uygulama verileri korunmayan bir veri. Bu durumda yalnızca bağlantı düzeyi güvenliği korumanın sağlayabileceği bir koruma sağlayabilir.

Bağlantı düzeyi güvenliği

Bağlantı düzeyi güvenliği , doğrudan ya da dolaylı olarak bir MCA, iletişim altsistemi ya da birlikte çalışan ikisinin bir birleşimiyle çağrılan güvenlik hizmetlerine gönderme yapar.

Bağlantı düzeyi güvenliği Şekil 10 sayfa 95içinde gösterilmektedir.

Aşağıda, bağlantı düzeyi güvenlik hizmetlerine ilişkin bazı örnekler bulunmaktadır:

- Bir ileti kanalının her ucundaki MCA, iş ortağının kimliğini doğrulayabilir. Bu işlem, kanal başlatıldığında ve iletişim bağlantısı kurulduğunda yapılır, ancak herhangi bir ileti akışa başlamadan önce gerçekleştirilir. Herhangi bir uçta kimlik doğrulama işlemi başarısız olursa, kanal kapatılır ve hiçbir ileti aktarılamaz. Bu bir tanımlama ve kimlik doğrulama hizmetidir.
- Bir ileti, bir kanalın gönderme sonunda şifrelenebilir ve alıcı uçta şifreleri çözülabilir. Bu, bir gizlilik hizmetine bir örnektir.
- Bir ileti, ağın ağ üzerinden iletilirken, içeriğinin kasıtlı olarak değiştirilip değiştirilmediğini belirlemek için bir kanalın alıcı ucunda denetlenmiş olabilir. Bu, bir veri bütünlüğü hizmetine bir örnektir.

IBM MQtarafından sağlanan bağlantı düzeyi güvenliği

The primary means of provision of confidentiality and data integrity in IBM MQ is by the use of TLS. IBM MQ' ta TLS kullanımı hakkında daha fazla bilgi için bkz. “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22. For authentication, IBM MQ provides the facility to use channel authentication records. Kanal doğrulama kayıtları, tek tek kanal ya da kanal grupları düzeyinde, birbirine bağlanma erişim yetkisi üzerinden kesin bir denetim sunar. Daha fazla bilgi için “Kanal doğrulama kayıtları” sayfa 47 başlıklı konuya bakın.

Kendi bağlantı düzeyi güvenliğinizin sağlanması

Kendi bağlantı düzeyi güvenlik hizmetlerinizi sağlayabilirsiniz. kendi kanal çıkış programlarınızı yazmak, kendi link seviyesi güvenlik hizmetlerinizi sağlamanın temel yoludur.

Kanal çıkış programları “Kanal çıkış programları” sayfa 99içinde tanıtılır. Aynı konu, IBM MQ for Windows (SSPI kanal çıkış programı) ile birlikte verilen kanal çıkış programını da açıklar. Bu kanal çıkış programı kaynak biçimde sağlanır; böylece kaynak kodu gereksinimlerinize uyacak şekilde değiştirebilirsiniz.
Bu kanal çıkış programı ya da diğer satıcılardan sağlanan kanal çıkış programları, gereksinimlerinizi karşılamıyorsa, kendi tasarımlarınızı tasarlayabilir ve yazabilirsiniz. Bu konuda, kanal çıkış programlarının güvenlik hizmetleri sağlayabileceği yöntemler gösterilmektedir. Kanal çıkış programının nasıl yazılacağı hakkında bilgi için Kanal çıkış programları yazmabaşlıklı konuya bakın.

Güvenlik çıkışı kullanarak bağlantı düzeyinde güvenlik

Güvenlik olağan koşullarda çiftlerde çalışır; bir kanalda her bir uçta bir tane vardır. Bunlar, kanal başlatma sırasında ilk veri görüşmesi tamamlandıktan hemen sonra çağrılır.

Güvenlik çıkışları, kimlik doğrulama, kimlik doğrulama, erişim denetimi ve gizlilik sağlamak için kullanılabilir.

İleti çıkışı kullanarak bağlantı düzeyinde güvenlik
İleti çıkışı yalnızca bir MQI kanalında değil, ileti kanallarında kullanılabilir. Bu, hem iletim kuyruğu üstbilgisine, hem de yerleşik ileti tanımlayıcısını içeren MQXQH ' ye ve bir iletiyle uygulama verilerine erişir. İletinin içeriğini değiştirebilir ve uzunluğunu değiştirebilir.

İleti çıkışı, iletinin bir kısmı yerine tüm iletiye erişim gerektiren herhangi bir amaç için kullanılabilir.

Kimlik doğrulama, erişim denetimi, erişim denetimi, gizlilik, veri bütünlüğü ve itibar dışındaki nedenler ve güvenlik dışındaki nedenler için de kullanılabilir.

Gönderme ve alma çıkışlarını kullanarak bağlantı düzeyi güvenliği
Gönderme ve alma çıkışları hem ileti, hem de MQI kanallarında kullanılabilir. Bir kanalda akan her tür veri için ve her iki yönde de akışlar için çağrılır.

Gönderme ve alma çıkışlarının her iletim kesimine erişimi vardır. İçeriğini değiştirebilirler ve uzunluğunu değiştirebilirler.

İleti kanalında, MCA ' nın bir iletiyi ayıp birden çok iletim kesimine göndermesi gerekiyorsa, iletinin bir bölümünü içeren her iletim kesimi için bir gönderme çıkışı çağrılır ve alıcı uçta her iletim kesimi için bir alma çıkışı çağrılır. Bir MQI çağrısının giriş ya da çıkış değiştirgeleri tek bir iletim kesimine gönderilmek için çok büyükse, bir MQI kanalında da aynı durum ortaya çıkar.

Bir MQI kanalında, iletim kesiminin 10 baytı, MQI çağrısını tanıtır ve iletim kesiminin çağrıya ilişkin giriş ya da çıkış parametrelerini içerip içermediğini belirtir. Gönderme ve alma çıkışları, MQI çağrısının korunması gerekebilecek uygulama verileri içerip içermediğini saptamak için bu baytı inceleyebilir.

Bir gönderme çıkışı ilk kez çağrıldığında, gereksinim duyduğu kaynakları edinip ilk kullanıma hazırlarken, MCA ' nın bir iletim kesimini bulunduran arabelleğde belirli bir alanı ayırmasını isteyebilir. Bir iletim kesimini işlemek için daha sonra çağrıldığında, örneğin, şifrelenmiş bir anahtar ya da sayısal bir imza eklemek için bu alanı kullanabilir. Kanalın diğer ucundaki karşılık gelen alma çıkışı, gönderme çıkışı tarafından eklenen verileri kaldırabilir ve iletim kesimini işlemek için bu verileri kullanabilir.

Gönderme ve alma çıkışları, işledikleri verilerin yapısını anlamalarına ve bu nedenle her iletim kesimini ikili bir nesne olarak ele almalarına gerek olmadığı amaçlar için en uygun çözümlerdir.

Gönderme ve alma çıkışları, gizlilik ve veri bütünlüğü sağlamak ve güvenlik dışındaki kullanım dışındaki kullanımlar için kullanılabilir.

İlgili görevler
Gönderme ya da alma çıkış programındaki API çağrısının tanımlanması

Uygulama düzeyinde güvenlik
Uygulama düzeyi güvenliği , bir uygulama ile bağlı olduğu bir kuyruk yöneticisi arasındaki arabirimde çağrılan güvenlik hizmetlerini belirtir.

Bu hizmetler, uygulama MQI çağrıları kuyruk yöneticisine çağrıldığında çağrılır. Hizmetler doğrudan ya da dolaylı olarak, uygulama, kuyruk yöneticisi, IBM MQ' u destekleyen başka bir ürün ya da bu çalışmalardan herhangi birinin birleşiminden çağrılabilir. Uygulama düzeyi güvenlik Şekil 10 sayfa 95' ta gösterilmektedir.

Uygulama düzeyi güvenliği, *uçtan uca güvenlik* ya da *ileti düzeyi güvenlik*olarak da bilinir.

Aşağıda, uygulama düzeyinde güvenlik hizmetlerine ilişkin bazı örnekler bulunmaktadır:

- Bir uygulama bir kuyruğa ileti yerleştirdiğinde, ileti tanımlayıcısı uygulamayla ilişkili bir kullanıcı kimliği içerir. Ancak, kullanıcı kimliğinin kimliğini doğrulamak için kullanılabilecek şifrelenmiş bir parola gibi bir veri yok. Bir güvenlik hizmeti bu verileri ekleyebilir. İleti alan uygulama tarafından alındığında, hizmetin başka bir bileşeni, iletiyle birlikte seyahat eden verileri kullanarak kullanıcı kimliğinin kimliğini doğrulayabilir. Bu bir tanımlama ve kimlik doğrulama hizmetidir.
- Bir ileti, bir uygulama tarafından bir kuyruğa konduğunda ve teslim alma uygulaması tarafından alındığında şifresi çözüldüğünde şifrelenebilir.Bu, bir gizlilik hizmetine bir örnektir.
- İleti, alma uygulaması tarafından alındığında imlenmiş bir ileti olabilir. Bu denetim, gönderme uygulaması tarafından kuyruğa ilk kez konulduğundan bu yana, içeriğinin kasıtlı olarak değiştirilip değiştirilmediğini belirler.Bu, bir veri bütünlüğü hizmetine bir örnektir.

Advanced Message Securityplanlaması
Advanced Message Security (AMS) is a component of IBM MQ that provides a high level of protection for sensitive data flowing through the IBM MQ network, while not impacting the end applications.

eğer son derece hassas veya değerli bilgiler taşıyorsanız, özellikle hasta kayıtları veya kredi kartı detayları gibi gizli ya da ödeme ile ilgili bilgiler, bilgi güvenliğine özel önem vermelisiniz. Kuruluşun çevresinde hareket eden bilgilerin bütünlüğünü korumasını ve yetkisiz erişimden korunmasını sağlamak, devam eden bir meydan okuma ve sorumluluğa sahiptir. Ayrıca, güvenlik düzenlemelerine uymanız, kurallara uymayanlara verilen cezalar riskiyle uyumlu olmanız da gerekebilir.

You can develop your own security extensions to IBM MQ. Ancak bu tür çözümler uzman becerilere gereksinim duyar ve bakımı için karmaşık ve pahalı olabilir. Advanced Message Security , sanal olarak her tür ticari BT sistemi arasında bilgi taşınırken bu zorlukların ele lanmasına yardımcı olur.

Advanced Message Security , IBM MQ güvenlik özelliklerini aşağıdaki şekillerde genişletir:

- İletilerin şifreleme ya da dijital imzalama özelliğini kullanarak ileti sistemi altyapısını noktalamak için uygulama düzeyinde, uçtan uca veri koruması sağlar.
- Karmaşık güvenlik kodu yazmadan ya da var olan uygulamaları değiştirmeksizin ya da yeniden derlemeden kapsamlı güvenlik sağlar.
- İletiler için kimlik doğrulama, yetkilendirme, gizlilik ve veri bütünlüğü hizmetleri sağlamak için Public Key Infrastructure (PKI) teknolojisini kullanır.
- Ana bilgisayar ve dağıtılmış sunucular için güvenlik ilkelerinin yönetimini sağlar.
- Hem IBM MQ sunucularını, hem de istemcilerini destekler.
- Uçtan uca güvenli bir ileti sistemi çözümü sağlamak için Managed File Transfer ile bütünleşir.

Daha fazla bilgi için “Advanced Message Security” sayfa 541 başlıklı konuya bakın.

Kendi uygulama düzeyinde güvenliğinizin sağlanması
Kendi uygulama düzeyinde güvenlik hizmetlerinizi sağlayabilirsiniz. Uygulama düzeyinde güvenliği uygulamanıza yardımcı olmak için IBM MQ , iki çıkış, API çıkışı ve API geçiş çıkışı sağlar.

API çıkışı ve API geçiş çıkışı, kimlik doğrulama, kimlik doğrulama, erişim denetimi, gizlilik, veri bütünlüğü ve itibar olmayan hizmetler ve güvenlik ile ilgili olmayan diğer işlevler sağlayabilir.

API çıkışı ya da API geçiş çıkışı, sistem ortamınızda desteklenmiyorsa, kendi uygulama düzeyi güvenliğinize ilişkin diğer yöntemleri de göz önünde bulundurmanız gerekebilir. Bunun bir yolu da, MQI ' yi sarmalayan daha yüksek düzeyli bir API geliştirmesi. Programmers then use this API, instead of the MQI, to write IBM MQ applications.

Daha yüksek düzeyli bir API ' nin kullanılmasının en yaygın nedenleri şunlardır:

- MQI ' nin programcılardan daha gelişmiş özelliklerini gizlemek için.
- MQI ' nin kullanımında standartları uygulamak için.
- MQI ' ye işlev eklemek için. Bu ek işlev, güvenlik hizmetleri olabilir.

Bazı satıcı ürünleri, IBM MQiçin uygulama düzeyinde güvenlik sağlamak üzere bu tekniği kullanır.

Güvenlik hizmetlerini bu şekilde sağlamayı planlıyorsanız, veri dönüştürmeyle ilgili olarak aşağıdakine dikkat edin:

- Sayısal imza gibi bir güvenlik simgesi, bir iletide uygulama verilerine eklendiyse, veri dönüştürmesi gerçekleştiren kodun bu simgenin varlığından haberdar olması gerekir.
- Bir güvenlik simgesi, uygulama verilerinin ikili görüntülerinden türetilmiş olabilir. Bu nedenle, verileri dönüştürmeden önce simgenin herhangi bir denetimi yapılması gerekir.
- Bir iletteki uygulama verileri şifrelenmişse, veri dönüştürmeden önce bu dosyanın şifresi çözülmelidir.

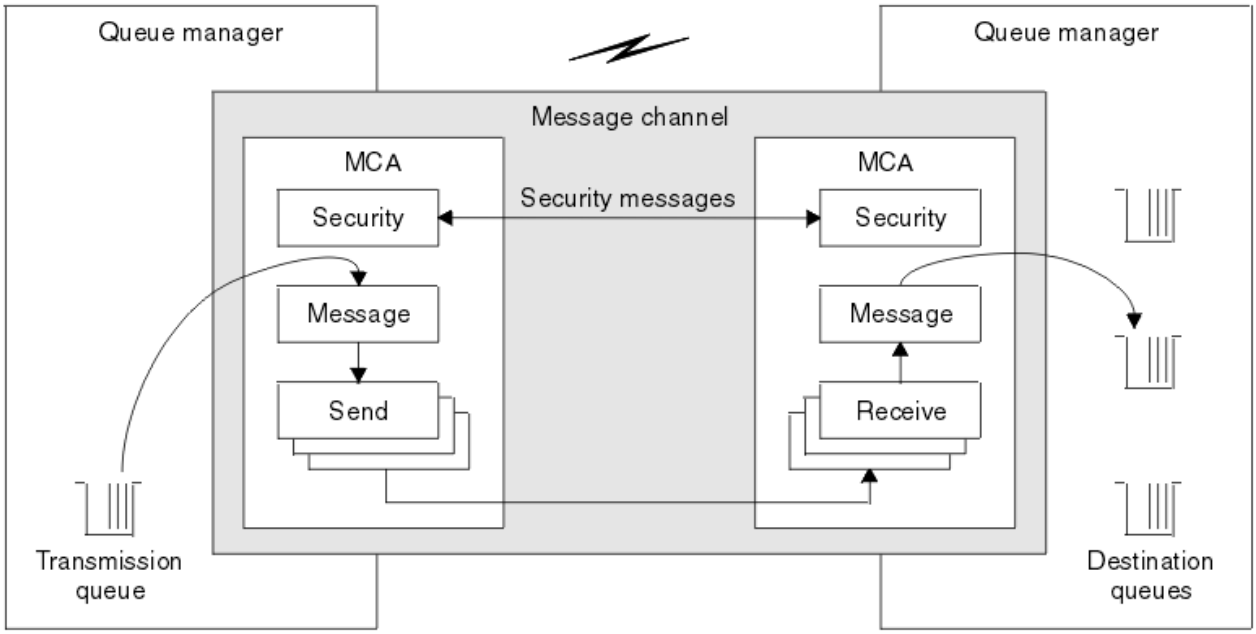
Kanal çıkış programları

Kanal çıkış programları , MCA ' nın işlem sırasında tanımlı yerlerde çağrılan programlardır. Kullanıcılar ve satıcılar kendi kanal çıkış programlarını yazabilirler. Bazıları IBMtarafından sağlanır.

Birkaç tip kanal çıkış programı vardır; ancak, bağlantı düzeyi güvenliği sağlamada yalnızca dört tür rol vardır:

- Güvenlik Çıkışı
- İleti çıkışı
- Çıkış gönder
- Çıkış al

Bu dört kanal çıkış programı tipi Şekil 11 sayfa 100 ' de gösterilmektedir ve aşağıdaki konularda açıklanmaktadır.



Şekil 11. İleti kanalından güvenlik, ileti, gönderme ve alma çıkışları

İlgili kavramlar
İleti alışverişi kanallarına ilişkin kanal çıkışı programları

Güvenlik çıkışa genel bakış

Güvenlik, normal olarak çiftler halinde çalışır. Bunlar, ileti akışından önce çağrılır ve amaçları, bir MCA ' nın iş ortağının kimliğini doğrulamasına izin vermeleridir.

Güvenlik çıkışları , normalde bir kanalın her ucunda bir çift olarak çalışır. Bunlar, kanal başlatma sırasında ilk veri görüşmesi tamamlandıktan hemen sonra çağrılır, ancak herhangi bir ileti akışa başlamadan önce çağrılır. Güvenlik çıkışlarının birincil amacı, bir kanalın her bir ucundaki MCA ' yı iş ortağının kimliğini doğrulamaya olanak sağlamaktır. Ancak, bir güvenlik çıkışısının diğer işlevi gerçekleştirmesini önleyecek hiçbir şey yoktur, bunun güvenlik ile hiçbir ilgisi olmayan işlev bile yoktur.

Güvenlik çıkışları, *güvenlik iletileri*gönderilerek birbirleriyle iletişim kurabilir. Bir güvenlik iletisinin biçimi tanımlanmaz ve kullanıcı tarafından belirlenir. Güvenlik mesajlarının değişmesinin olası bir sonucu, güvenlik çıkışlarından birinin daha fazla devam etmemesine karar verebileceği. Bu durumda, kanal kapatılır ve iletiler akışmaz. Bir kanalın yalnızca bir ucunda bir güvenlik çıkışı varsa, çıkış hala çağrılır ve devam edip etmeyeceğini ya da kanalın kapatılıp kapatılmayacağını seçebilir.

Güvenlik çıkışları hem ileti, hem de MQI kanallarında çağrılabilir. Güvenlik çıkışısının adı, kanal tanımında bir kanalın her ucundaki bir parametre olarak belirtilir.

Güvenlik çıkışlarıyla ilgili daha fazla bilgi için bkz. “Güvenlik çıkışı kullanarak bağlantı düzeyinde güvenlik” sayfa 97.

İleti çıkışı

İleti çıkışları yalnızca ileti kanallarında çalışır ve genellikle çiftler halinde çalışılır. İleti çıkışı, tüm iletide işlem yapabilir ve üzerinde çeşitli değişiklikler yapabilir.

Bir kanalın gönderme ve alma uçlarındaki*İleti çıkışları* , normal olarak çiftler halinde çalışır. MCA ' nın iletim kuyruğundan bir ileti aldıktan sonra, bir kanalın gönderme bitiminde ileti çıkışı çağrılır. Bir kanalın alıcı ucunda, MCA ' nın hedef kuyruğuna bir ileti yerleştirmeden önce bir ileti çıkışı çağrılır.

İleti çıkışı, hem iletim kuyruğu üstbilgisine, hem de yerleşik ileti tanımlayıcısını içeren MQXQH ' ye ve bir iletiyle uygulama verilerine erişir. İleti çıkışı, iletinin içeriğini değiştirebilir ve uzunluğunu değiştirebilir. Uzunluk değişikliği, iletinin sıkıştırılması, açılması, şifrelenmesi ya da şifrelerinin çözülmesi sonucunda ortaya çıkan bir sonuç olabilir. Ayrıca, iletiye veri ekleme ya da ondan veri kaldırma işleminin sonucu da olabilir.

İleti çıkışları, bir kısmı yerine, tüm iletiye erişim gerektiren herhangi bir amaç için kullanılabilir ve güvenlik için gerekli değildir.

İleti çıkışı, işlemekte olduğu iletinin, hedefine doğru ilerlemek zorunda kalmadığını saptayabilir. Daha sonra MCA ileti kuyruğunda ileti yerleştirir. Bir ileti çıkışı kanalı da kapatabilir.

İleti çıkışları yalnızca ileti kanallarında çağrılabilir, MQI kanallarında çağrılamaz. This is because the purpose of an MQI channel is to enable the input and output parameters of MQI calls to flow between the IBM MQ MQI client application and the queue manager.

Kanal tanımında, kanal tanımında bir değiştirge olarak belirtilen ileti çıkışı adı belirtilir. Ayrıca, art arda çalıştırılacak ileti çıkışlarının bir listesini de belirleyebilirsiniz.

İleti çıkışlarına ilişkin daha fazla bilgi için bkz. “İleti çıkışı kullanarak bağlantı düzeyinde güvenlik” sayfa 98.

Gönderme ve alma çıkışları

Gönderme ve alma çıkışları genellikle çiftler halinde çalışılır. İletim segmentlerinde faaliyet gösterirler ve en iyi şekilde, işledikleri verilerin yapısının ilgili olmadığı durumlarda kullanılır.

Bir kanalın bir ucundaki *çıkış gönder* ve diğer uçtaki *alma çıkışı* genellikle çiftler halinde çalışır. MCA, iletişim bağlantısı üzerinden veri göndermek için bir iletişim göndermesi işleminden hemen önce bir gönderme çıkışı çağrılır. Alma çıkışı, bir MCA ' nın iletişim alma işleminden sonra denetimi yeniden kazanmasından ve bir iletişim bağlantısından veri aldıktan hemen sonra çağrılır. Paylaşımı paylaşımda kullanılırsa, bir MQI kanalı üzerinden, her etkileşim için farklı bir gönderme ve alma çıkıştan farklı bir yönetim ortamı çağrılır.

İleti kanalındaki iki MCA arasındaki IBM MQ kanalı iletişim kuralı akışları, ileti verilerinin yanı sıra denetim bilgilerini de içerir. Benzer şekilde, bir MQI kanalında, akışlar denetim bilgilerinin yanı sıra, MQI çağrılarının parametrelerini de içerir. Tüm veri tipleri için gönderme ve alma çıkışları çağrılır.

İleti verileri bir ileti kanalında tek bir yönde akar, ancak bir MQI kanalında, bir MQI çağrı akışının giriş değiştirgeleri tek bir yönde ve çıkış değiştirgeleri diğerinde akış olur. Hem ileti, hem de MQI kanallarında, denetim bilgileri her iki yönde de akar. Sonuç olarak, bir kanalın her iki ucunda da gönderme ve alma çıkışları çağrılabilir.

İki MCA arasında tek bir akışta iletilen veri birimi, *iletim bölümü*adı verilir. Gönderme ve alma çıkışlarının her iletim kesimine erişimi vardır. İçeriğini değiştirebilirler ve uzunluğunu değiştirebilirler. Ancak bir gönderme çıkışı, iletim kesiminin ilk 8 baytı değiştirmemelidir. Bu 8 bayt, IBM MQ kanal iletişim kuralı üstbilgisinin bir parçasıdır. Bir gönderme çıkışısının iletim kesiminin uzunluğunu ne kadar artırabileceğiyle ilgili kısıtlamalar da vardır. Özellikle, bir gönderme çıkışı, kanal başlatma sırasında iki MCA arasında kararlaştırılan maksimum uzunluğun uzunluğunu artıramaz.

Bir ileti kanalında, ileti tek bir iletim kesiminde gönderilmek üzere çok büyükse, gönderme MCA iletiyi böler ve birden çok iletim kesimine gönderir. Sonuç olarak, iletinin bir bölümünü içeren her iletim kesimi için bir gönderme çıkışı çağrılır ve alıcı uçta her iletim kesimi için bir alma çıkışı çağrılır. Alma MCA, alma çıkışı tarafından işlendikten sonra iletim kesimlerinden iletiyi yeniden oluşturur.

Benzer şekilde, bir MQI kanalında, bir MQI çağrısının giriş ya da çıkış değiştirgeleri çok büyükse, birden çok iletim kesiminde gönderilir. Bu durum, örneğin, uygulama verileri yeterince büyükse, bir MQPUT, MQPUT1ya da MQGET çağrısına neden olabilir.

Bu konuları dikkate alarak, gönderdikleri verilerin yapısını anlamalarına ve bu nedenle her bir iletim kesimini ikili bir nesne olarak ele almalarına gerek olmadığı için, gönderme ve alma işlemlerinin kullanılması daha uygun olur.

Gönderme ya da alma çıkışı bir kanalı kapatabilir.

Bir kanalın her ucundaki kanal tanımında parametre olarak, bir gönderme çıkığı ve alma çıkışı adları belirlenir. Ayrıca, art arda çalıştırılacak gönderme çıkışlarının bir listesini de belirleyebilirsiniz. Benzer şekilde, alma çıkışlarının bir listesini de belirleyebilirsiniz.

Gönderme ve alma çıkışlarıyla ilgili daha fazla bilgi için bkz. “Gönderme ve alma çıkışlarını kullanarak bağlantı düzeyi güvenliği” sayfa 98.

Planlama verileri bütünlüğü

Verilerinizin bütünlüğünün nasıl korunacağını planlayın.

Veri bütünlüğünü uygulama düzeyinde ya da bağlantı düzeyinde uygulayabilirsiniz.

Uygulama düzeyinde, standart tesisler gereksinimlerinizi karşılamazsa, API çıkış programlarını kullanabilirsiniz. Onaylanmayan değişikliklere karşı korumak için iletileri dijital olarak imzalamak için Advanced Message Security (AMS) olanağını kullanmayı seçebilirsiniz.

Bağlantı düzeyinde TLS kullanmayı seçebilirsiniz, bu durumda dijital sertifikalar kullanımınızı planlamanız gerekir. Standart tesisler gereksinimlerinizi karşılamazsa, kanal çıkış programlarını da kullanabilirsiniz.

İlgili kavramlar

“SSL/TLS ile kanalları koruma” sayfa 106
IBM MQ ' ta TLS desteği, kuyruk yöneticisi kimlik doğrulama bilgileri nesnesini ve çeşitli MQSC komutlarını kullanır. Ayrıca, dijital sertifikalar kullanımınızı da göz önünde bulundurmanız gerekir.

“IBM MQiçindeki veri bütünlüğü” sayfa 22
Bir iletinin değiştirilip değiştirilmediğini saptamak için veri bütünlüğü hizmetini kullanabilirsiniz.

“Advanced Message Securityplanlaması” sayfa 99
Advanced Message Security (AMS) is a component of IBM MQ that provides a high level of protection for sensitive data flowing through the IBM MQ network, while not impacting the end applications.

Kanal-çıkış çağrıları ve veri yapıları

İlgili başvurular

API çıkış başvurusu

Planlama denetimi

Denetim için gereken verileri ve denetleme bilgilerini nasıl yakalayacağınıza ve nasıl işleyeceğine karar verin. Sisteminizin doğru yapılandırıldığını nasıl denetlemeyi düşünün.

Etkinlik izlemenin birkaç yönü vardır. Göz önünde bulundurmanız gereken noktalar genellikle denetçi gereksinimleri tarafından tanımlanır ve bu gereksinimler genellikle HIPAA (Health Insurance Portability and Accountability Act) ya da SOX (Sarbanes-Oxley) gibi düzenleyici standartlara göre belirlenir. IBM MQ , bu tür standartlara uyulmasına yardımcı olmak üzere özellikler sağlar.

Yalnızca özel durumlarla mı ilgilendiğinizi, yoksa tüm sistem davranışlarıyla mı ilgilendiğinizi düşünün.

Denetlemenin bazı yönleri de operasyonel izleme olarak kabul edilebilir; denetlemeye yönelik bir ayrım, sadece gerçek zamanlı uyarılara bakmak için değil, genellikle tarihi verilere bakmakta olduğunuz. İzleme, bölüm İzleme ve performansbölümünde yer alıyor.

Denetlenecek veriler

Aşağıdaki bölümlerde açıklandığı gibi, denetlemek için gereksinim duyardığınız veri tiplerini ya da etkinliği göz önünde bulundurun:

IBM MQ arabirimlerini kullanarak IBM MQ üzerinde yapılan değişiklikler
Özel olarak komut olayları ve yapılandırma olayları olmak üzere, özel işlemden geçirme olaylarını yayınlamak için IBM MQ ' i yapılandırın.

IBM MQ ' ta denetimin dışında yapılan değişiklikler
Bazı değişiklikler IBM MQ ' in davranışını etkileyebilir, ancak IBM MQtarafından doğrudan izlenemez. Bu tür değişikliklere örnek olarak, `mqs.ini`, `qm.inive` `mqclient.ini`yapılandırma dosyalarında yapılan değişiklikler, kuyruk yöneticilerinin yaratılması ve silinmesi, kullanıcı çıkış programları gibi ikili dosyaların kurulması ve dosya izinlerinde yapılan değişiklikler gibi değişiklikler yer alır. Bu etkinlikleri izlemek için işletim sisteminin düzeyinde çalışan araçları kullanmanız gerekir. Farklı araçlar kullanılabilir ve farklı işletim sistemleri için uygundur. You might also have logs created by associated tools such as *sudo*.

Operational control of IBM MQ
Kuyruk yöneticilerinin başlatılması ve durdurulması gibi etkinlikleri denetlemek için işletim sistemi araçlarını kullanmak zorunda kalabilirsiniz. Bazı durumlarda, IBM MQ , özel işlemden geçirme olaylarını yayınlayabilecek şekilde yapılandırılabilir.

IBM MQiçindeki uygulama etkinliği
Uygulamaların eylemlerini denetlemek, örneğin kuyrukların açılması ve iletilerin yerleştirilip alınması, uygun olayları yayınlamak için IBM MQ ' i yapılandırın.

İzinsiz giriş uyarıları
Güvenlik ihlallerini denetlemek için, sisteminizi yetkilendirme olaylarını yayınlamak üzere yapılandırın. Kanal olayları, özellikle bir kanal beklenmedik şekilde sona ererse, etkinliği göstermek için yararlı olabilir.

Denetim verilerinin yakalanmasını, görüntülenmesini ve arşivlenmesini planlama

Gereksinim duyardığınız öğelerin çoğu IBM MQ olay iletisi olarak raporlanır. Bu iletileri okuyabilecek ve biçimlendirebilecek araçları seçmelisiniz. Uzun süreli depolama ve çözümlemelerle ilgileniyorsanız, bunları veritabanı gibi bir yardımcı depolama mekanizmasını taşımalısınız. Bu iletileri işlemezseniz, bunlar olay kuyruğunda kalır ve kuyruğun doldurulması olabilir. Bazı olaylara dayalı olarak otomatik olarak harekete geçen bir araç (örneğin, bir güvenlik hatası olduğunda uyarı yayınlamaya) karar verebilirsiniz.

Sisteminizin doğru yapılandırıldığı doğrulanıyor

A set of tests are supplied with the IBM MQ Explorer. Sorun olup olmadığını görmek için nesne tanımlarınızı denetlemek için bunları kullanın.

Ayrıca, sistem yapılandırmasının beklediğiniz gibi olduğundan düzenli olarak emin olun. Komut ve yapılandırma olayları bir şey değiştiğinde rapor verse de, aynı zamanda yapılandırmanın dökümünü almak ve bilinen bir iyi kopyayla karşılaştırmak da yararlı olur.

Topolojinin güvenliğini planlama

Bu bölüm, kanallar, kuyruk yöneticisi kümeleri, yayınlama/abone olma ve çok noktaya gönderim uygulamaları ve bir güvenlik duvarı kullanılırken güvenliği belirli durumlarda kapsar.

Daha fazla bilgi için aşağıdaki alt başlıklara bakın:

Kanal yetkisi

Bir kanal aracılığıyla bir ileti gönderdiğinizde ya da aldığınızda, çeşitli IBM MQ kaynaklarına erişim sağlamanız gerekir. Message Channel Agents (MCAs) are essentially IBM MQ applications that move messages between queue managers, and as such require access to various IBM MQ resources to operate correctly.

MCA ' lar için PUT işlemi sırasında ileti almak için, MCA ile ilişkili kullanıcı kimliğini ya da iletiyle ilişkili kullanıcı kimliğini kullanabilirsiniz.

At CONNECT time you can map the asserted user ID to an alternative user, by using **CHLAUTH** channel authentication records.

IBM MQ' ta kanallar TLS desteği ile korunabilir.

MCAUSER özniteliğinin kullanılmadığı gönderici kanalı dışında, gönderme ve alma kanallarıyla ilişkili kullanıcı kimlikleri, aşağıdaki kaynaklara erişim gerektirir:

- Bir gönderme kanalıyla ilişkilendirilen kullanıcı kimliği kuyruk yöneticisine, iletim kuyruğuna, ölü harf kuyruğuna ve kanal çıkışlarının gerektirdiği diğer kaynaklara erişmenizi gerektirir.
- Bir alıcı kanalının MCAUSER kullanıcı kimliği *+ setall* yetkisine sahip olmalıdır. Bunun nedeni, alıcı kanalının, uzak gönderen kanalından aldığı verileri kullanarak tüm bağlam alanları da içinde olmak üzere tüm MQMD ' yi yaratması gerekir. Bu nedenle, kuyruk yöneticisi, bu etkinliği gerçekleştiren kullanıcının *+ setall* yetkisine sahip olmasını gerektirir. Bu kullanıcı için bu *+ setall* yetkisi verilmelidir:
  - Alıcı kanalının geçerli bir şekilde iletileri yerleştirdiği tüm kuyruklar.
  - Kuyruk yöneticisi nesnesi. Daha fazla bilgi için bakınız: Authorizasyons for context.
- Kaynak COA ' nın rapor iletisi istediği bir alıcı kanalının MCAUSER kullanıcı kimliği, rapor iletisini döndüren iletim kuyruğunda *+ passid* yetkisine ihtiyaç duyar. Bu yetki olmadan, AMQ8077 hata iletileri günlüğe kaydedilir.
- Alma kanalıyla ilişkili kullanıcı kimliğiyle, iletileri kuyruklara yerleştirmek için hedef kuyrukları açabilirsiniz. Bu, Message queuing Interface (MQI) olanağını içerir; bu nedenle IBM MQ Object Authority Manager (OAM) olanağını kullanmıyorsa, ek erişim denetimi denetimlerinin yapılması gerekebilir. Yetki denetimlerinin MCA ile ilişkili kullanıcı kimliğine (bu konuda anlatıldığı gibi) ya da iletiyle ilişkili kullanıcı kimliğine (MQMD UserIdentifier alanından) ilişkin olarak mı yapıldığını belirleyebilirsiniz.

  Geçerli olduğu kanal tipleri için, kanal tanımının **PUTAUT** parametresi, bu denetimler için hangi kullanıcı kimliğinin kullanılacağını belirtir.
  - Kanal, varsayılan olarak kuyruk yöneticisinin hizmet hesabının kullanılmasını sağlar; bu hesap, tam yönetim haklarına sahiptir ve özel yetkiler gerektirmez.
  - Sunucu-bağlantı kanallarında, yönetim bağlantıları CHLAUTH kuralları tarafından varsayılan olarak engellenir ve belirtik yetkilendirmeyi gerektirir.
  - Denetimci, bu erişimi kısıtlamak için adım atmadığı sürece, alıcı, istek ve küme alıcısının kanalları, herhangi bir bitişik kuyruk yöneticisi tarafından yerel denetimde yer alır.
  - Bir alıcı kanalının MCAUSER kullanıcı kimliği için *dsp* ve *ctrlx* yetkisi verilmesine gerek yoktur.
  - IBM MQ 8.0.0 Fix Pack 4öncesinde, IBM MQ yönetim ayrıcalıklarından yoksun bir kullanıcı kimliği kullanırsanız, kanal için kanal için bu kullanıcı kimliğinin çalışabilmesi için **dsp** ve **ctrlx** yetkisine sahip olmanız gerekir.

    IBM MQ 8.0.0 Fix Pack 4' tan, bir kanal kendisini yeniden eşitlediğinde ve sıra numaralarını düzeldiğinde herhangi bir yetki denetimi yoktur.

    Ancak, RESET CHANNEL komutunu el ile yayınlamak, tüm yayınlarda **+dsp** ve **+ctrlx** ' yi gerektirir.

    Uyarı: İleti toplu onayı için bir kanal ilk durumuna getirildiğinde, IBM MQ kanalı sorgulamaya çalışır; bu durumda **+dsp** yetkisi gerekir.
  - MCAUSER özniteliği SDR kanal tipi için kullanılmıyor.
  - İletiyle ilişkilendirilen kullanıcı kimliğini kullanırsanız, kullanıcı kimliğinin uzak bir sistemden olması olası olabilir. Bu uzak sistem kullanıcı kimliği, hedef sistem tarafından tanınmalıdır. Aşağıdaki komutlar, uzak sistemden bir kullanıcı kimliğine yetki vermek için yapabildiğiniz komut tipine örneklerdir:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect +inq +setall
```

```
setmqaut -m QMgrName -t chl -n Profile -g GroupName +dsp +ctrlx
```

Burada *Profil* bir kanaldır.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

Burada *Profil* , ayarlandıysa, bir ölü-mektup kuyruğidir.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

Burada *Profil* , yetkili kuyrukların bir listesidir.

Uyarı: Bir kullanıcı kimliğinin, iletileri Komut Kuyruğu 'na ya da diğer hassas sistem kuyruklarına yerleştirmesi için yetki verilirken dikkatli olun.

MCA ile ilişkili kullanıcı kimliği MCA tipine bağlıdır. MCA ' nın iki tipi vardır:

Arayan MCA
Kanal başlatan MCA ' lar. Çağıran MCA ' lar tek tek işlemler olarak, kanal başlatıcısında iş parçacıkları olarak ya da bir süreç havuzunun iş parçacıkları olarak başlatılabilir. Kullanılan kullanıcı kimliği, üst süreçle (kanal başlatıcı) ilişkili kullanıcı kimliğidir ya da MCA ' yı başlatan işlemle ilişkilendirilmiş kullanıcı kimliğidir.

Yanıt Veren MCA
Yanıtlayıcı MCA 'lar, arayan MCA tarafından yapılan bir isteğin sonucu olarak başlatılan MCA' lardır. Yanıt veren MCA ' lar tek tek işlemler olarak, dinleyicilerin iş parçacıkları olarak ya da bir süreç havuzunun iş parçacıkları olarak başlatılabilir. Kullanıcı kimliği aşağıdaki tiplerden herhangi biri olabilir (bu tercihin sırasıyla):

1. APPC 'de, çağıran MCA, yanıtlayıcı MCA için kullanılacak kullanıcı kimliğini gösterebilir. Bu, ağ kullanıcı kimliği olarak adlandırılır ve yalnızca tek tek işlemler olarak başlatılan kanallar için geçerlidir. Kanal tanımının USERID parametresini kullanarak ağ kullanıcı kimliğini ayarlayın.
2. **USERID** parametresi kullanılmıyorsa, yanıt veren MCA 'nın kanal tanımlaması, MCA' nın kullanması gereken kullanıcı kimliğini belirtebilir. Kanal tanımının **MCAUSER** parametresini kullanarak kullanıcı kimliğini ayarlayın.
3. Kullanıcı kimliği önceki (iki) yöntemden biri tarafından ayarlanmadıysa, MCA ' yı başlatan işlemin kullanıcı kimliği ya da üst sürecin kullanıcı kimliği (dinleyici) kullanılır.

İlgili kavramlar
“Kanal doğrulama kayıtları” sayfa 47
Kanal düzeyinde bağlanan sistemlere verilen erişim üzerinde daha kesin denetim sağlamak için kanal kimlik doğrulama kayıtlarını kullanabilirsiniz.

Kanal kimlik doğrulama kaydı özellikleri

Kanal başlatıcı tanımlarının korunması
Kanal başlatıcılarını yalnızca mqm grubunun üyeleri yönlendirebilir.

IBM MQ kanal başlatıcıları IBM MQ nesneleri değildir; bunlara erişim OAM tarafından denetlenmez. IBM MQ does not allow users or applications to manipulate these objects, unless their user ID is a member of the mqm group. If you have an application that issues the PCF command **StartChannelInitiator**, the user ID specified in the message descriptor of the PCF message must be a member of the mqm group on the target queue manager.

Bir kullanıcı kimliği, Escape PCF komutuyla eşdeğer MQSC komutlarını vermek için ya da dolaylı kipte `runmqsc` komutunu kullanarak, hedef makineden bir mqm grubunun üyesi olmalıdır.

İletim kuyrukları
Kuyruk yöneticileri uzak iletileri otomatik olarak bir iletim kuyruğuna yerleştirdi; bunun için özel bir yetki gerekli değildir.

Ancak, bir iletiyi doğrudan iletim kuyruğuna koymanız gerekiyorsa, bu özel yetki gerektirir; bkz. Çizelge 12 sayfa 123.

Kanal çıkışları

Kanal kimlik doğrulama kayıtları uygun değilse, ek güvenlik için kanal çıkışlarını kullanabilirsiniz. Bir güvenlik çıkışı, iki güvenlik çıkış programı arasında güvenli bir bağlantı oluşturur. Bir program, ileti kanalı aracısının (MCA) gönderilmesi, diğeri ise MCA ' nın alınması içindir.

Kanal çıkışlarıyla ilgili daha fazla bilgi için bkz. “Kanal çıkış programları” sayfa 99 .

SSL/TLS ile kanalları koruma

IBM MQ ' ta TLS desteği, kuyruk yöneticisi kimlik doğrulama bilgileri nesnesini ve çeşitli MQSC komutlarını kullanır. Ayrıca, dijital sertifikalar kullanımınızı da göz önünde bulundurmanız gerekir.

Sayısal sertifikalar ve anahtar havuzları

Kuyruk yöneticisi sertifika etiketi özniteliğini ayarlamak iyi bir uygulamadır (**CERTLABL**) Farklı sertifikalar gerektiren kanallardaki sertifika etiketini ayarlayarak, kanalların büyük bölümü için kullanılacak kişisel sertifikana ilişkin adı ve kural dışı durumlar için geçersiz kılabilirsiniz.

Kuyruk yöneticisinde varsayılan sertifika kümesinden farklı sertifikalar içeren birçok kanala gereksinim duyarsanız, farklı bir sertifika sunmak için, kanalları birkaç kuyruk yöneticisi arasında bölmeyi ya da kuyruk yöneticisinin önünde bir MQIPT yetkili sunucusu kullanmayı düşünmelisiniz.

Her kanal için farklı bir sertifika kullanabilirsiniz; ancak, anahtar havuzunda çok fazla sertifika saklıyorsa, TLS kanallarını başlatırken başarım etkilenmesini bekleyebilirsiniz. Anahtar havuzundaki sertifikaların sayısını 50 'den az bir yere saklamaya çalışın ve GSKit performansı daha büyük anahtar havuzlarıyla sert bir şekilde azaldıkça 100 ile 100 arasında bir değer elde edin.

Aynı kuyruk yöneticisine birden çok sertifika verilmesi, birden çok CA sertifikasının aynı kuyruk yöneticisi üzerinde kullanılmasına olanak sağlar. Bu durum, ayrı sertifika yetkilileri tarafından verilen sertifikalar için Sertifika Konusu Ayırt Edici Ad ad alanı çakışmalarını artırır.

Profesyonel sertifika yetkilileri daha dikkatli olmaya devam ederken, şirket içi sertifika yetkilileri genellikle net adlandırma kurallarından yoksun ve bir CA ile başka bir kuruluş arasında istenmeyen eşleşmeler ortaya çıkacaktır.

Özel Ayırt Edici Adı 'na ek olarak Sertifika Veren Ayırt Edici Adını (DN) denetlemeniz gerekir. Bunu yapmak için, bir kanal kimlik doğrulaması SSLPEERMAP kaydı kullanın ve hem **SSLPEER** hem de **SSLCERTI** alanlarını, sırasıyla Konu DN ve Sertifika Veren DN ile eşleşecek şekilde ayarlayın.

Kendinden onaylı ve CA imzalı sertifikalar

Uygulamanızı geliştirirken ve test ederken ve üretimde kullanımı için, dijital sertifikalar kullanımınızı planlamak önemlidir. Kuyruk yöneticilerinizin ve istemci uygulamalarınızın kullanımına bağlı olarak, CA imzalı sertifikalar ya da kendinden imzalı sertifikalar kullanabilirsiniz.

CA imzalı sertifikalar
Üretim sistemleri için, sertifikalarınızı güvenilir bir sertifika yetkilisinden (CA) edinin. Dış bir CA ' dan bir sertifika aldığınızda, hizmet için ödeme ödemenizi sağlar.

kendinden imzalı sertifikalar
Uygulamanızı geliştirirken, platforma bağlı olarak, yerel bir CA tarafından verilen kendinden onaylı sertifikaları ya da sertifikaları kullanabilirsiniz:

ULW Windows, UNIXve Linux sistemlerinde kendinden onaylı sertifikalar kullanabilirsiniz. Yönergeler için bkz. “UNIX, Linux, and Windows üzerinde kendinden onaylı kişisel sertifika oluşturma” sayfa 281.

IBM i IBM i sistemlerinde, yerel CA ' nın imzaladığı sertifikaları kullanabilirsiniz. Yönergeler için bkz. “IBM iüzerinde bir sunucu sertifikası istenmesi” sayfa 266 .

z/OS z/OS' ta kendinden imzalı ya da yerel CA imzalı sertifikalar kullanabilirsiniz. Yönergeler için “z/OSüzerinde kendinden onaylı bir kişisel sertifika oluşturma” sayfa 308 ya da “z/OSüzerinde kişisel sertifika isteme” sayfa 308 başlıklı konuya bakın.

Kendinden onaylı sertifikalar üretim kullanımı için uygun değildir; bu nedenle, aşağıda belirtilen nedenler şunlardır:

- Kendinden onaylı sertifikalar iptal edilemez; bu, bir saldırganın özel bir anahtarın gizliliğinin ihlal edilmesinden sonra bir kimliği bozmasına olanak verebilir. CU ' lar ihlal edilen bir sertifikayı iptal edebilir, bu da daha fazla kullanım yapılmasını önleyebilir. Bu nedenle, kendi kendine imzalanmış sertifikalar bir test sistemi için daha uygun olsa da, CA imzalı sertifikalar üretim ortamında kullanılmak üzere daha güvenli olur.
- Kendinden imzalı sertifikaların süresi hiçbir zaman sona ermez. Bu, test ortamında hem uygun hem de güvenli bir ortamda, ancak üretim ortamında, onları nihai güvenlik ihlalleri için açık bırakıyor. Bu risk, kendinden imzalı sertifikaların iptal edilemeyeceği gerçeğidir.
- Kendinden onaylı bir sertifika hem kişisel sertifika olarak, hem de kök (ya da güven çıpası) CA sertifikası olarak kullanılır. Kendinden onaylı kişisel sertifikasına sahip bir kullanıcı, diğer kişisel sertifikaları imzalamak için bunu kullanabilir. Genel olarak, bu, bir CA tarafından verilen kişisel sertifikalar için geçerli değildir ve önemli bir maruziyeti temsil eder.

CipherSpecs ve dijital sertifikalar

Desteklenen tüm sayısal sertifikalar için yalnızca desteklenen CipherSpecs ' in bir alt kümesi kullanılabilir. Bu nedenle, dijital sertifikalarınız için uygun bir CipherSpec seçmeniz gerekir. Benzer bir şekilde, kuruluşunuzun güvenlik ilkesi belirli bir CipherSpec ' in kullanılmasını gerektiriyorsa, uygun dijital sertifikalar edinmeniz gerekir.

CipherSpecs ve dijital sertifikalar arasındaki ilişkiyle ilgili daha fazla bilgi için bkz. “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42

Sertifika geçerlilik denetimi ilkeleri

IETF RFC 5280 standardı, taklitleme saldırılarını önlemek için uyumlu uygulama yazılımların gerçekleştirmesi gereken bir dizi sertifika geçerlilik denetimi kuralı dizisini belirtir. Sertifika geçerlilik denetimi kuralları kümesi, sertifika geçerlilik denetimi ilkesi olarak bilinir. IBM MQ' ta sertifika doğrulama ilkelerine ilişkin daha fazla bilgi için bkz. “IBM MQiçindeki sertifika geçerlilik denetimi ilkeleri” sayfa 41.

Sertifika iptal denetiminin planlanması

Farklı sertifika yetkililerinden birden çok sertifikana izin verilmesi, gereksiz ek sertifika iptal denetmesine neden olabilir.

Belirli bir CA 'dan bir geri alma sunucusu kullanımını belirtik olarak yapılandırdıysanız, örneğin, bir AUTHINFO nesnesi ya da Kimlik Doğrulama bilgileri kaydı (MQAIR) yapısı kullanılarak, farklı bir CA' dan gelen bir sertifikayla sunulduğunda iptal denetimi başarısız olur.

Belirtik sertifika iptal sunucusu yapılandırmalarını önlemeniz gerekir. Bunun yerine, her sertifikanda bir sertifika uzantısında kendi geri alma sunucusu konumunu (CRL Distribution Point ya da OCSP AuthorityInfoerişimi) içerdiğini örtük olarak denetlemeniz gerekir.

Daha fazla bilgi için bkz. OCSPCheckExtensions ve CDPCheckExtensions.

TLS desteği için komutlar ve öznitelikler

TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolü, dinleme, kurcalama ve kimliğine bürünme karşı koruma ile kanal güvenliği sağlar. TLS içinIBM MQ desteği, kanal tanımlamasında, belirli bir kanalda TLS güvenliğini kullanacağını belirtmenizi sağlar. Ayrıca, kullanmak istediğiniz şifreleme algoritması gibi, istediğiniz güvenlik tipine ilişkin ayrıntıları da belirtebilirsiniz.

- Aşağıdaki MQSC komutları TLS ' yi destekler:

ALTER AUTHINFO
Bir kimlik doğrulama bilgileri nesnesinin özniteliklerini değiştirir.

DEFINE YAZAR
Bir kimlik doğrulama bilgisi nesnesi oluşturur.

YAZAR BILGILERINI SIL
Bir kimlik doğrulama bilgisi nesnesini siler.

AUTHENTICAFO GÖRÜNTÜLE
Belirli bir kimlik doğrulama bilgileri nesnesine ilişkin öznitelikleri görüntüler.

- Aşağıdaki kuyruk yöneticisi parametreleri TLS ' yi destekler:

  CERTLABEL
  Kullanılacak kişisel sertifika etiketini tanımlar.

  SSLCRLNL
  SSLCRLNL özniteliği, geliştirilmiş TLS sertifikası denetmesine izin vermek üzere sertifika iptal konumlarını sağlamak için kullanılan kimlik doğrulama bilgileri nesnelerinin bir ad listesini belirtir.

  SLCRYP
  Windows , UNIX and Linux sistemlerinde, **SSLCryptoHardware** kuyruk yöneticisi özniteliğini ayarlar. Bu öznitelik, sisteminizde sahip olduğunuz şifreleme donanımını yapılandırmak için kullanabileceğiniz parametre dizilimini içerir.

  SSLEV
  TLS ' yi kullanan bir kanal TLS bağlantısı oluşturamazsa TLS olay iletisinin raporlanıp raporlanmayacağını belirler.

  SLFIPS
  Şifreleme donanımında değil, IBM MQ içinde şifreleme gerçekleştiriliyorsa, yalnızca FIPS onaylı algoritmaların kullanılıp kullanılmayacağını belirtir. Şifreleme donanımı yapılandırılmışsa, donanım ürünü tarafından sağlanan şifreleme modülleri kullanılır ve bunlar belirli bir düzey için FIPS onaylı olabilir. Bu, donanımın kullanımında kullanılan ürüne bağlıdır.

  SSLKEYR
  UNIX, Linux, and Windows sistemlerinde, bir anahtar havuzunu kuyruk yöneticisiyle ilişkilendirir. Anahtar veritabanı, bir *GSKit* anahtar veritabanında tutulur. The IBM Global Security Kit (GSKit) enables you to use TLS security on Windows , UNIX and Linux systems.

  SSLRKEYC
  Gizli anahtar yeniden anlaşılmadan önce bir TLS iletişiminde gönderilecek ve alınan bayt sayısı. Bayt sayısı, MCA tarafından gönderilen denetim bilgilerini içerir.

- Aşağıdaki kanal parametreleri TLS ' yi destekler:

  CERTLABEL
  Kullanılacak kişisel sertifika etiketini tanımlar.

  SSLCAUTH
  IBM MQ ' in TLS istemcisinden bir sertifikayı isteyip istemediğinizi ve doğrulayıp doğrulamayacağını tanımlar.

  SSLCIPH
  Şifreleme kalınlığını ve işlevini (CipherSpec) belirtir; örneğin, TLS_RSA_WITH_AES_128_CBC_SHA. CipherSpec , kanal uçlarında eşleşmelidir.

  SSLPEER
  İzin verilen iş ortaklarının ayırt edici adını (benzersiz tanıtıcı) belirtir.

Bu bölümde, kimlik doğrulama bilgileri nesnesini desteklemek için **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg**ve **dspmqfls** komutları ele alınmıştır. It also describes the **runmqckm** (iKeycmd) command for managing certificates on UNIX and Linux systems, and the **runmqakm** tool for managing certificates on UNIX, Linux, and Windows. Aşağıdaki bölümlere bakın:

- setmqaut
- dspmqaut

- dmpmqaut
- rcrmqobj
- rcdmqimg
- dspmqfls
- Anahtarlar ve sertifikaların yönetilmesi

TLS ' yi kullanarak kanal güvenliğine genel bakış için bkz.

- “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22

TLS ile ilişkili MQSC komutlarına ilişkin ayrıntılar için bkz.

- ALTER AUTHORINFO
- DEFINE AUTHINFO
- YAZAR BILGILERINI SIL
- AUTHENTIFO GöRüNTüLE

TLS ile ilişkili PCF komutlarının ayrıntıları için bkz.

- Kimlik Doğrulama Bilgileri Nesnesi Değiştir, Kopyala ve Yarat
- Kimlik Doğrulama Bilgileri nesnesini sil
- Kimlik Doğrulama Bilgileri Nesnesi

z/OS *IBM MQ for z/OS sunucusu bağlantı kanalı*

The IBM MQ for z/OS SVRCONN channel is not secure without implementing channel authentication, or adding a security exit using TLS. SVRCONN kanallarının varsayılan olarak tanımlanmış bir güvenlik çıkışı yoktur.

Güvenlik endişeleri

SVRCONN kanalları başlangıçta tanımlandığı gibi güvenli değildir; örneğin, SYSTEM.DEF.SVRCONN . To secure a SVRCONN channel you must set up channel authentication using the CHLAUTH KüMESI command, or install a security exit and implement TLS.

Kamuya açık bir örnek güvenlik çıkışı kullanmanız, bir güvenlik çıkışı kendiniz yazmanız ya da bir güvenlik çıkışı satın almanız gerekir.

Kendi SVRCONN kanalı güvenlik çıkışınızı yazmak için iyi bir başlangıç noktası olarak kullanabileceğiniz birkaç örnek vardır.

IBM MQ for z/OS' ta, hlq.SCSQC37S kitaplığınızdaki CSQ4BCX3 üyesi, C dilinde yazılmış bir güvenlik çıkışı örneğidir. Örnek CSQ4BCX3 , hlq.SCSQAUTH kitaplığınızda önceden derlenmiş olarak da verilir.

You can implement the CSQ4BCX3 sample exit by copying the compiled member hlq.SCSQAUTH(CSQ4BCX3) into a load library that is allocated to the CSQXLIB DD in your CHIN Proc. CHIN ' in yükleme kitaplığının "Program Denetimli" olarak ayarlanmasını gerektirdiğini unutmayın.

SVRCONN kanalınızı, güvenlik çıkışı olarak CSQ4BCX3 ayarına ayarlayın.

V 9.1.4 Bir istemci, bu SVRCONN kanalını kullanarak bağlandığında, CSQ4BCX3 , MQCD 'den **RemoteUserIdentifier** ve **RemotePassword** çifti kullanılarak kimlik doğrulaması yapacak ya da IBM MQ 9.1.4, **CSPUserIdPtr** ve **CSPPasswordPtr** çiftinden MQCSP' den kimlik doğrulaması gerçekleştirecektir. If authentication is successful it will copy **RemoteUserIdentifier** into **MCAUserIdentifier**, changing the identity context of the thread.

For Long Term Support and Continuous Delivery before IBM MQ 9.1.4, when a client connects using that SVRCONN channel, CSQ4BCX3 will authenticate using the **RemoteUserIdentifier** and **RemotePassword** pair from MQCD. If authentication is successful it will copy **RemoteUserIdentifier** into **MCAUserIdentifier**, changing the identity context of the thread.

Bir IBM MQ Java istemcisi yazıyorsanız, kullanıcıyı sorgulamak için açılan pencereleri kullanabilir ve MQEnvironment.userID ve MQEnvironment.passwordseçeneklerini belirleyebilirsiniz. Bu değerler, bağlantı yapıldığında iletilir.

Artık işlevsel bir güvenlik çıkışa sahip olduğunuz için, bağlantı yapıldığında ağ üzerinden düz metin olarak kullanıcı kimliği ve parolanın iletileceği endişesi vardır. Bu, sonraki tüm IBM MQ iletilerinin içerikleri de olabilir. Bu ilk bağlantı bilgilerini ve herhangi bir IBM MQ iletisinin içeriğini şifrelemek için TLS ' yi kullanabilirsiniz.

Örnek

IBM MQ Explorer SVRCONN kanalının SYSTEM.ADMIN.SVRCONN aşağıdaki adımları tamamlar:

1. hlq.SCSQAUTH(CSQ4BCX3) adlı kopyayı CHINIT Proc içindeki CSQXLIB DD ' ye ayrılan bir yükleme kitaplığına kopyalayın.
2. Yükleme kitaplığının Program Denetimli olduğunu doğrulayın.
3. Alter the SYSTEM ADMIN.SVRCONN to use security exit CSQ4BCX3.
4. IBM MQ Explorer'ta, z/OS Kuyruk Yöneticisi adını sağ tıklatın, **Bağlantı Ayrıntıları** > **Özellikler** > **Kullanıcı Kimliği** ' yi seçin ve z/OS kullanıcı kimliğinizi girin.
5. Bir parola girerek z/OS Kuyruk Yöneticisine bağlanın.

Ek bilgi

CSQ4BCX3 ' un bir Program Denetimli ortamında çalışması için, CHIN adres alanına yüklenen her şey, bir Program Denetimli kitaplığından (örneğin, STEPLIB içindeki tüm kitaplıklar ve CSQXLIB DD adlı kitaplıklarda) yüklenmelidir. Bir yükleme kitaplığını Program Denetimli sorunu RACF komutları olarak ayarlamak için. Aşağıdaki örnekte, yükleme kitaplığı adı MY.TEST.LOADLIB.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

SVRCONN kanalını CSQ4BCX3komutunu uygulamak üzere değiştirmek için, aşağıdaki IBM MQ komutunu verin:

```
ALTER CHANNEL(SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SCYEXIT(CSQ4BCX3)
```

Yukarıdaki örnekte, kullanılmakta olan SVRCONN kanal adı SYSTEM ADMIN.SVRCONN' dir.

Kanal çıkışlarıyla ilgili daha fazla bilgi için bkz. “Kanal çıkış programları” sayfa 99 .

İlgili görevler

Writing channel exit programs on z/OS

SNA LU 6.2 güvenlik hizmetleri

SNA LU 6.2 , oturum düzeyinde şifreleme, oturum düzeyinde kimlik doğrulaması ve etkileşim düzeyinde kimlik doğrulaması sunar.

Not: Bu konu grubu, Sistem Ağ Mimarisi (SNA) ile ilgili temel bir anlayışınız olduğunu varsayar. Bu bölümde atıfta bulunulan diğer belgeler, ilgili kavramlara ve terminolojiye kısa bir giriş sağlar. SNA ' ya daha kapsamlı bir teknik tanıtıma gerek duyuyorsanız bkz. *Systems Network Mimarisi Teknik Genel Bakış*, GC30-3073.

SNA LU 6.2 üç güvenlik hizmeti sağlar:

- Oturum düzeyi şifrelemesi
- Oturum düzeyi kimlik doğrulaması
- Etkileşim düzeyi kimlik doğrulaması

Oturum düzeyinde şifreleme ve oturum düzeyi kimlik doğrulaması için, SNA *Data Encryption Standard (DES)* algoritmasını kullanır. DES algoritması, verileri şifrelemek ve şifrelerini çözmek için simetrik bir anahtar kullanan bir blok şifre algoritmasıdır. Hem blok, hem de anahtar 8 baytlık uzunluğdır.

Oturum düzeyi şifrelemesi
Oturum düzeyi şifrelemesi , DES algoritmasını kullanarak oturum verilerini şifreler ve şifrelerini çözer. Bu nedenle, SNA LU 6.2 kanallarında bağlantı düzeyinde bir gizlilik hizmeti sağlamak için kullanılabilir.

Mantıksal birimler (LU ' lar) zorunlu veri şifrelemesi, seçmeli veri şifrelemesi ya da veri şifrelemesi olmadan zorunlu (ya da zorunlu) veri şifrelemesi sağlayabilir.

Bir *zorunlu şifreleme oturumu*üzerinde, LU tüm giden veri isteği birimlerini şifreler ve tüm gelen veri isteği birimlerinin şifresini çözer.

Bir *seçmeli şifreleme oturumu*üzerinde, LU, yalnızca gönderme işlemi programı (TP) tarafından belirlenen veri isteği birimlerini şifreler. Gönderen LU, istek üstbilgisinde bir gösterge ayarlanarak verilerin şifrelendiğine işaret eder. Bu göstergeyi denetleyerek, alan LU, alma TP ' ye iletilmeden önce, hangi istek birimlerinin şifresini çözeceğini söyleyebilir.

Bir SNA ağında, IBM MQ MCA ' lar hareket programlarıdır. MCA ' lar gönderdikleri veriler için şifreleme isteğinde bulunmaz. Seçmeli veri şifrelemesi bir seçenek değildir; bu nedenle, oturumda yalnızca zorunlu veri şifrelemesi ya da veri şifrelemesi yapılamaz.

Zorunlu veri şifrelemesi uygulamaya ilişkin bilgi için SNA altsisteminize ilişkin belgelere bakın. Altyapınızda kullanılabilir olabilecek daha güçlü şifreleme biçimleriyle ilgili bilgi için aynı belgelere bakın (örneğin, z/OSüzerinde Triple DES 24 byte 'lık şifreleme).

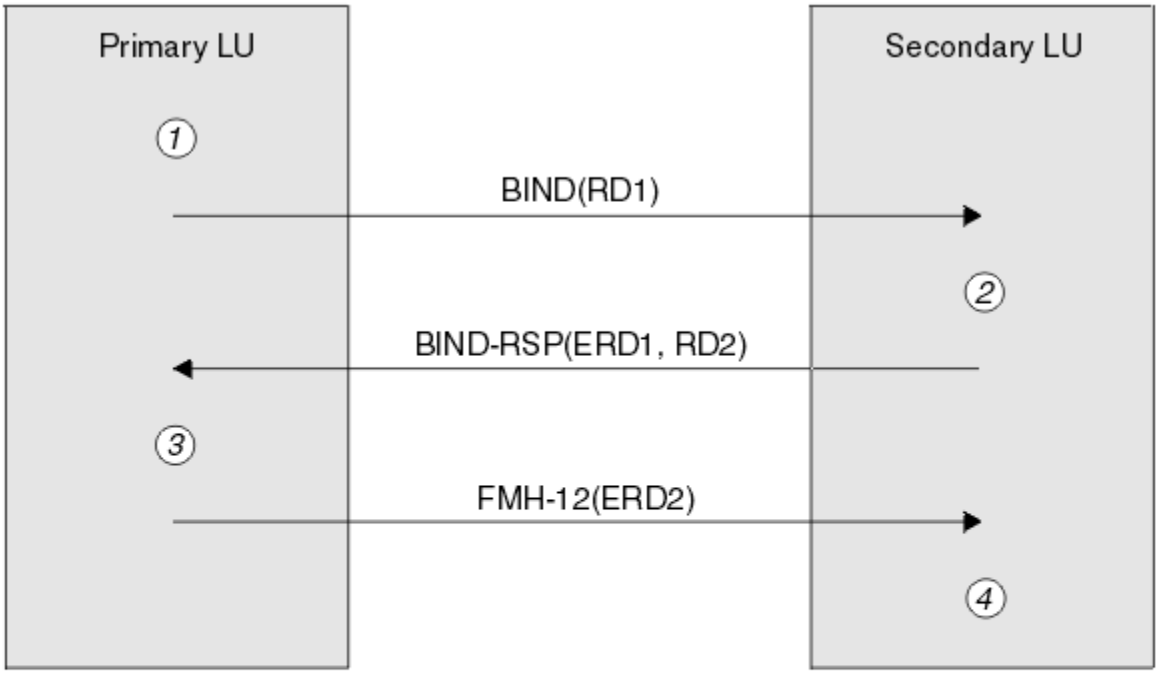
Oturum düzeyi şifrelemesi hakkında daha fazla genel bilgi için bkz. *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Oturum düzeyi kimlik doğrulaması
Oturum düzeyi kimlik doğrulaması , iki LU ' nın bir oturumu etkinleştirirken birbirinin kimliğini doğrulamasına olanak sağlayan bir oturum düzeyi güvenlik protokolüdür. Bu değer, *LU-LU doğrulaması*olarak da bilinir.

Bir LU, ağdan bir sisteme etkin bir şekilde "ağ geçidi" getirdiğinden, bu kimlik doğrulama düzeyini belirli koşullarda yeterli olarak düşünebilirsiniz. Örneğin, kuyruk yöneticinizin denetimli ve güvenilir bir ortamda çalışan bir uzak kuyruk yöneticisiyle ileti alışverişi yapmak gerekiyorsa, LU doğrulandıktan sonra uzak sistemin kalan bileşenlerinin kimliklerine güvenmeye hazır olabilirsiniz.

Her LU, iş ortağının parolasını doğrulayan her LU tarafından oturum düzeyinde kimlik doğrulaması gerçekleştirmektedir. Her bir LU çifti arasında bir parola belirlendiği için, parola *LU-LU parolası* olarak adlandırılır. LU-LU parolasının kurulduğu yol, SNA ' nın kapsamı dışında ve dışında somutlanır.

Şekil 12 sayfa 112 , oturum düzeyinde kimlik doğrulamaya ilişkin akışları gösterir.



Legend:

BIND	=	BIND request unit
BIND-RSP	=	BIND response unit
ERD	=	Encrypted random data
FMH-12	=	Function Management Header 12
RD	=	Random data

Şekil 12. Oturum düzeyi kimlik doğrulamasına ilişkin akışlar

Oturum düzeyinde kimlik doğrulamaya ilişkin protokol aşağıdaki gibidir. Yordamlardaki sayılar, Şekil 12 sayfa 112içindeki sayılara karşılık gelir.

1. Birincil LU rasgele bir veri değeri (RD1) oluşturur ve BIND isteğindeki ikincil LU ' ya gönderir.
2. İkincil LU, BIND isteğini rasgele verilerle aldığında, anahtar olarak LU-LU parolasının kopyasıyla DES algoritmasını kullanarak verileri şifreler. İkincil LU daha sonra ikinci bir rasgele veri değeri (RD2) oluşturur ve bunu, şifrelenmiş verilerle (ERD1), BIND yanıtındaki birincil LU ' ya gönderir.
3. Birincil LU BIND (BIND) yanıtı aldığında, özgün olarak ürettiği rasgele verilerden şifrelenmiş verilerin kendi sürümünü hesaplar. Bunu, anahtar olarak LU-LU parolasının kopyasıyla DES algoritmasını kullanarak yapar. Daha sonra, sürümünü BIND yanıtında aldığı şifrelenmiş verilerle karşılaştırır. İki değer aynıysa, birincil LU, ikincil LU 'un parola ile aynı parolaya sahip olduğunu ve ikincil LU' un kimliğinin doğrulanır olduğunu bilir. İki değer eşleşmezse, birincil LU oturumu sona erdirir.

   Daha sonra birincil LU, BIND yanıtında aldığı rasgele verileri şifreler ve şifrelenmiş verileri (ERD2) bir İşlev Yönetimi Üstbilgisindeki (FMH-12) ikincil LU ' ya gönderir.
4. İkincil LU FMH-12' yi aldığında, oluşturulan rasgele verilerden şifrelenmiş verilerin kendi sürümünü hesaplar. Daha sonra, sürümünü FMH-12içinde aldığı şifrelenmiş verilerle karşılaştırır. İki değer aynıysa, birincil LU ' un kimliği doğrulanır. İki değer eşleşmezse, ikincil LU oturumu sona erdirir.

Orta saldırılarda adama karşı daha iyi koruma sağlayan, protokolün geliştirilmiş bir sürümünde ikincil LU, anahtar olarak LU-LU parolasının kopyasını kullanarak, RD1, RD2ve ikincil LU ' nun tam olarak nitelenmiş adını kullanan bir DES İleti Kimlik Doğrulama Kodu (MAC) hesaplar. İkincil LU, MAC 'i BIND yanıtında ERD1yerine birincil LU' ya gönderir.

Birincil LU, ikincil LU 'nun kimliğini, BIND yanıtında alınan MAC ile karşılaştırdığı MAC' in kendi sürümünü hesaplayarak doğrular. The primary LU then computes a second MAC from RD1 and RD2, and sends the MAC to the secondary LU in the FMH-12 instead of ERD2.

İkincil LU, birincil LU ' nun kimliğini, kendi sürümünü, FMH-12içinde alınan MAC ile karşılaştıran ikinci MAC sürümünü hesaplayarak doğrular.

Oturum düzeyinde kimlik doğrulamasının nasıl yapılandırılacağı hakkında bilgi için, SNA altsisteminize ilişkin belgelere bakın. Oturum düzeyi kimlik doğrulamasına ilişkin daha genel bilgi için bkz. *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Etkileşim düzeyi kimlik doğrulaması
Yerel bir TP, bir iş ortağı TP ile etkileşim ayırmayı denediğinde, yerel LU ortak LU 'ya bir bağlantı isteği gönderir ve bunu iş ortağı TP' yi bağlayacak şekilde gönderir. Belirli koşullar altında, bağlantı isteği, ortak LU 'un yerel TP' yi doğrulamak için kullanabileceği güvenlik bilgilerini içerebilir. Bu, *etkileşim düzeyi kimlik doğrulaması*ya da *son kullanıcı doğrulaması*olarak bilinir.

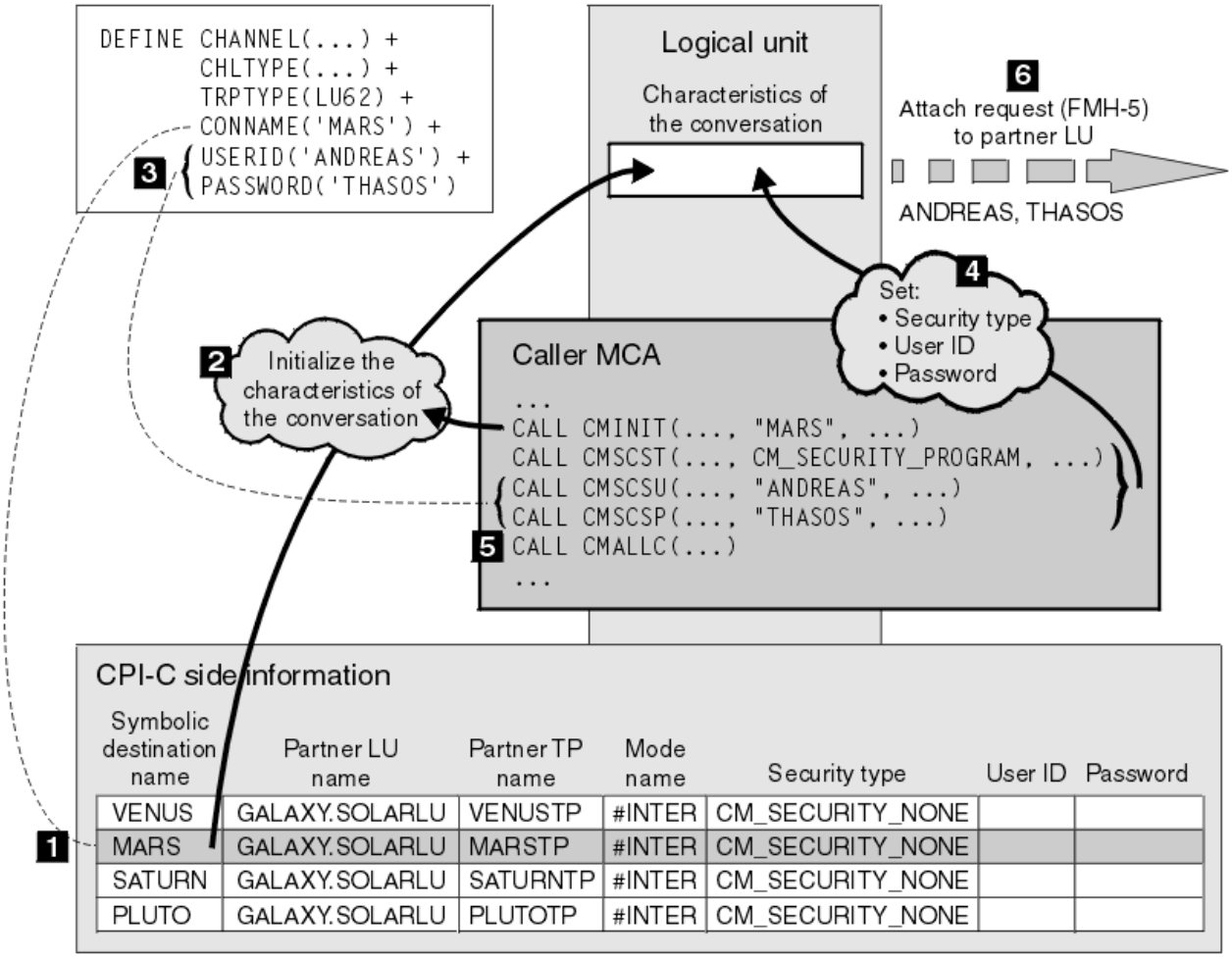
Aşağıdaki konularda, IBM MQ ' in etkileşim düzeyi kimlik doğrulaması için destek sağladığı açıklanmaktadır.

Etkileşim düzeyi kimlik doğrulamasıyla ilgili daha fazla bilgi için bkz. *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808. z/OS' e özgü bilgiler için *z/OS MVS Planning: APPC/MVS Management*, SA22-7599başlıklı konuya bakın.

CPI-C ile ilgili ek bilgi için bkz. *Common Programming Interface Communications CPI-C Specification*, SC31-6180. APPC/MVS TP Conversation Callable Services ile ilgili ek bilgi için *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621başlıklı konuya bakın.

IBM i Windows UNIX *IBM i, UNIXve Windowsüzerinde etkileşim düzeyi kimlik doğrulaması desteği*
Etkileşim düzeyi kimlik doğrulamasının IBM i, UNIXve Windowsüzerinde nasıl çalışacağını genel bir bakış edinmek için bu konuyu kullanın.

IBM i, UNIXve Windows üzerinde etkileşim düzeyi kimlik doğrulaması desteği Şekil 13 sayfa 114' de gösterilmektedir. Şekildeki sayılar, aşağıdaki açıklamadaki sayılara karşılık gelir.



Symbolic destination name	Partner LU name	Partner TP name	Mode name	Security type	User ID	Password
VENUS	GALAXY.SOLARLU	VENUSTP	#INTER	CM_SECURITY_NONE		
MARS	GALAXY.SOLARLU	MARSTP	#INTER	CM_SECURITY_NONE		
SATURN	GALAXY.SOLARLU	SATURNTP	#INTER	CM_SECURITY_NONE		
PLUTO	GALAXY.SOLARLU	PLUTOTP	#INTER	CM_SECURITY_NONE		

Şekil 13. Etkileşim düzeyi kimlik doğrulaması içinIBM MQ desteği

IBM i, UNIXve Windowsüzerinde bir MCA, bir SNA ağı üzerinden ortak MCA ile iletişim kurmak için Common Programming Interface Communications (CPI-C) çağrılarını kullanır. Bir kanalın çağırıcı ucundaki kanal tanımlamasında CONNAME parametresinin değeri, CPI-C yan bilgi girişini (1) tanımlayan simgesel bir hedef adıdır. Bu girdi şunları belirtir:

- Ortak LU ' nun adı
- Yanıt veren MCA olan ortak TP ' nin adı
- Etkileşim için kullanılacak kipin adı

Bir yan bilgi girişi aşağıdaki güvenlik bilgilerini de belirtebilir:

- Bir güvenlik tipi.

  Yaygın olarak uygulanan güvenlik tipleri şunlardır: CM_SECURITY_NONE, CM_SECURITY_PROGRA; ancak diğerleri CPI-C belirtiminde tanımlanmaktadır.
- Bir kullanıcı kimliği.
- Bir parola.

Çağıran MCA, bir yanıtlayıcı MCA ile, CPI-C çağrısı CMINIT adını vererek, çağrıdaki parametrelerden biri olarak CONNAME değerini kullanarak bir etkileşim ayırmayı hazırlar. CMINIT çağrısı, yerel LU 'nun yararı için, MCA' nın etkileşim için kullanmayı amaçladığı yan bilgi girdisinin tanımlanmasını sağlar. Yerel LU, sohbetin özelliklerini başlatmak için bu girişteki değerleri kullanır (2).

Çağıran MCA daha sonra, kanal tanımlamasındaki (3) USERID ve PASSWORD parametrelerinin değerlerini denetler. USERID ayarlandıysa, çağıran MCA şu CPI-C çağrılarını yayınlar (4):

- CMSCST, sohbete ilişkin güvenlik tipini CM_SECURITY_PROGRAY ile ayarlamak için.
- CMSCSU, etkileşmeye ilişkin kullanıcı kimliğini USERID değerine ayarlamak için.
- CMSCSP, parolaya ilişkin parolayı PASSWORD değerine ayarlamak için. CMSCSP, PASSWORD belirlenmedikçe çağrılmaz.

Bu çağrılar tarafından ayarlanan güvenlik tipi, kullanıcı kimliği ve parola, daha önce yan bilgi girdisinden alınan tüm değerleri geçersiz kılar.

Çağıran MCA, daha sonra, konuşmayı ayırmak için CPI-C çağrısı CMALLC ' yi yayınlar (5). Bu çağrıya yanıt olarak, yerel LU ortak LU (6) için bir bağlantı isteği (İşlev Yönetimi Üstbilgisi 5 ya da FMH-5) gönderir.

Ortak LU, bir kullanıcı kimliğini ve parolayı kabul ederse, bağlantı isteğine USERID ve PASSWORD değerleri eklenir. Ortak LU, bir kullanıcı kimliğini ve parolayı kabul etmezse, değerler bağlama isteğine dahil değildir. Yerel LU, bir oturum oluşturmak için LU bağ tanımlandığında, ortak LU ' nun bir bilgi alışverişi parçası olarak bir kullanıcı kimliğini ve parolayı kabul edip etmeyeceğini keşfeder.

Ekleme isteğinin daha sonraki bir sürümünde, parola yerine koyma değeri, temizleme parolası yerine LU ' lar arasında akabilir. Parola yerine koyma değeri, paroladan oluşturulan DES Message Authentication Code (MAC) ya da SHA-1 ileti özetidir. Parola yerine koyma değerleri, yalnızca hem LU 'lar, hem de LU' lar tarafından destekleniyorsa kullanılabilir.

Ortak LU, bir kullanıcı kimliği ve parola içeren bir gelen ekleme isteğini aldığında, kimlik doğrulama ve kimlik doğrulama amacıyla kullanıcı kimliği ve parola kullanabilir. Erişim denetimi listelerine başvurarak, ortak LU, kullanıcı kimliğinin bir etkileşim ayırmayı ve yanıt veren MCA ' yı ekleme yetkisine sahip olup olmadığını da saptayabilir.

Buna ek olarak, yanıt veren MCA, ekleme isteğine dahil edilen kullanıcı kimliği altında çalışabilir.Bu durumda, kullanıcı kimliği, yanıt veren MCA ' nın varsayılan kullanıcı kimliği olur ve MCA kuyruk yöneticisine bağlanma girişiminde bulunduğunda yetki denetimi için kullanılır. MCA, kuyruk yöneticisinin kaynaklarına erişmeyi denediğinde de yetki denetimleri için de kullanılabilir.

Bir kullanıcı kimliğinin ve bağlanma isteğindeki bir parolanın, tanımlama, kimlik doğrulama ve erişim denetimi için kullanılabileceği yol, somutlamaya bağlıdır. SNA altsisteminize özgü bilgi edinmek için uygun belgelere bakın.

USERID belirlenmezse, çağıran MCA ' da CMSCST, CMSCSU ve CMSCSP çağrılmaz. Bu durumda, bir ekleme isteğinde akan güvenlik bilgileri yalnızca, taraf bilgileri girdisinde belirtilenler ve ortak LU ' nın kabul edeceği şey tarafından belirlenir.

Etkileşim düzeyi kimlik doğrulaması ve IBM MQ for z/OS
Sohbet düzeyi kimlik doğrulama çalışmalarının z/OS' ta nasıl çalışacağını genel bir bakış elde etmek için bu konuyu kullanın.

IBM MQ for z/OSüzerinde MCA 'lar CPI-C' yi kullanmaz. Bunun yerine, bazı CPI-C özelliklerine sahip APPC (Advanced Program-to-Program Communication) uygulaması için APPC/MVS TP Conversation Callable Services olanağını kullanırlar. Çağıran MCA bir etkileşimi ayırdığında, çağrıda SAME güvenlik tipi belirtilir. Bu nedenle, bir APPC/MVS LU, giden sohbetler için değil, yalnızca gelen sohbetler için sürekli doğrulamayı destekliyorsa, iki olasılık vardır:

- Ortak LU, APPC/MVS LU ' ya güveniyorsa ve önceden doğrulanmış bir kullanıcı kimliğini kabul ederse, APPC/MVS LU şunları içeren bir bağlantı isteği gönderir:
  - Kanal başlatıcı adres alanı kullanıcı kimliği
  - RACF kullanılırsa, kanal başlatıcı adres alanı kullanıcı kimliğinin yürürlükteki bağlantı grubunun adı olan bir güvenlik tanıtımı adı
  - Önceden doğrulanan bir gösterge
- Ortak LU APPC/MVS LU ' ya güvenmiyorsa ve doğrulanmış bir kullanıcı kimliğini kabul etmezse, APPC/MVS LU, güvenlik bilgisi içermeyen bir bağlantı isteği gönderir.

IBM MQ for z/OSüzerinde, DEFINE CHANNEL komutundaki USERID ve PASSWORD parametreleri bir ileti kanalı için kullanılamaz ve yalnızca bir MQI kanalının istemci bağlantısı sonunda geçerlidir. Bu nedenle, APPC/MVS LU ' dan gelen bir ekleme isteği hiçbir zaman bu parametrelerin belirlediği değerleri içermez.

Kuyruk yöneticisi kümeleri için güvenlik

Kuyruk yöneticisi kümeleri kullanıma uygun olsa da, güvenliklerine özel önem vermelisiniz.

Kuyruk yöneticisi kümesi , mantıksal olarak bir şekilde ilişkili olan bir kuyruk yöneticilerinden oluşan bir ağdır. Bir kümenin üyesi olan bir kuyruk yöneticisine *küme kuyruk yöneticisi*adı verilir.

Bir küme kuyruk yöneticisine ait olan bir kuyruk, kümedeki diğer kuyruk yöneticilerine tanınabilir. Böyle bir kuyruğa *küme kuyruğu*adı verilir. Bir kümedeki kuyruk yöneticisi, aşağıdakilere gerek duymadan küme kuyruklarına ileti gönderebilir:

- Her küme kuyruğu için belirtik bir uzak kuyruk tanımlaması
- Her uzak kuyruk yöneticisinden ve her bir uzak kuyruk yöneticisinden açıkça tanımlanmış kanallar
- Her giden kanal için ayrı bir iletim kuyruğu

İki ya da daha çok kuyruk yöneticisinin klonlar olduğu bir küme yaratabilirsiniz. Başka bir deyişle, bunlar, küme kuyrukları olarak bildirilen yerel kuyruklar da içinde olmak üzere, aynı yerel kuyruklara sahip oldukları ve aynı sunucu uygulamalarının eşgörünümlerini destekleyebildikleri anlamına gelir.

Bir küme kuyruk yöneticisine bağlı bir uygulama, eşkopyalanmış kuyruk yöneticilerinin her birinde bir yönetim ortamı olan bir küme kuyruğuna ileti gönderdiğinde, IBM MQ hangi kuyruk yöneticisinin gönderileceğini karar verir. Birçok uygulama, küme kuyruğuna ileti gönderdiğinde, IBM MQ , iş yükünü kuyruğun bir eşgörünümü olan kuyruk yöneticilerinin her birindeki iş yükünü dengeler. If one of the systems hosting a cloned queue manager fails, IBM MQ continues to balance the workload across the remaining queue managers until the system that failed is restarted.

Kuyruk yöneticisi kümelerini kullanıyorsanız, aşağıdaki güvenlik sorunlarını göz önünde bulundurmanız gerekir:

- Yalnızca seçilen kuyruk yöneticilerinin kuyruk yöneticinize ileti göndermesine izin verilmesi
- Bir uzak kuyruk yöneticisinin yalnızca seçilen kullanıcılarının kuyruk yöneticinizdeki bir kuyruğa ileti göndermesine izin verilmesi
- Kuyruk yöneticinize bağlı uygulamaların yalnızca seçilen uzak kuyruklara ileti göndermesine izin verilmesi

Bu noktalar, kümeleri kullanmasanız bile, ilgili noktaları dikkate almakla birlikte, kümeleri kullanıyorsanız daha önemli hale gelmeleri gerekir.

Bir uygulama, iletileri tek bir küme kuyruğuna gönderebilecekse, başka uzak kuyruk tanımlamalarına, iletim kuyruklarına ya da kanallara gerek duymadan diğer herhangi bir küme kuyruğuna ileti gönderebilir. Bu nedenle, kuyruk yöneticilerinizdeki küme kuyruklarına erişimi kısıtlamak ve uygulamalarınızın ileti gönderebileceği küme kuyruklarını kısıtlamak gerekip gerekmediğini göz önünde bulundurmanız daha önemli hale gelir.

Yalnızca kuyruk yöneticisi kümelerini kullanıyorsanız, bazı ek güvenlik konuları da dikkate alınması gerekir:

- Yalnızca seçilen kuyruk yöneticilerinin bir kümeye katılmalarına izin verilmesi
- İstenmeyen kuyruk yöneticilerinin bir küme bırakması zorlanması

Tüm bu önemli noktalar hakkında daha fazla bilgi için bkz. Kümeleri Güvenli Tutma. z/OS
IBM MQ for z/OS' a özgü dikkat edilmesi gereken noktalar için bkz. “z/OSüzerindeki kuyruk yöneticisi kümelerindeki güvenlik” sayfa 252.

İlgili görevler

“Kuyruk yöneticilerinin ileti alma engellenmesi” sayfa 444
Bir küme kuyruk yöneticisinin çıkış programlarını kullanarak, alma yetkisi olmayan iletileri almasını önleyebilirsiniz.

IBM MQ Yayınlama/Abone Olma Güvenliği

IBM MQ Yayınlama/Abone Olma özelliğini kullanıyorsanız, ek güvenlik konuları da vardır.

Yayınlama/abone olma sisteminde iki tip uygulama vardır: yayınlayıcı ve abone. *Yayınlayıcılar* bilgi kaynağı, IBM MQ iletileri biçiminde bilgi sağlar. Bir yayınlayıcı bir iletiyi yayınladığında, bu ileti, iletinin içindeki bilgilerin konusunu tanımlayan bir *konu*belirtir.

Aboneler , yayınlanan bilgilerin tüketicidir. Abone, ilgilendiği konuları onlara abone olarak belirtir.

Kuyruk yöneticisi , IBM MQ Yayınlama/Abone Olma ile birlikte sağlanan bir uygulamadır. Yayıncılardan ve abonelerden gelen abonelik isteklerinden yayınlanan iletileri alır ve yayınlanan iletileri abonelere yönlendirir. Bir abone, yalnızca abone olduğu ilgili konularda iletiler gönderilir.

Daha fazla bilgi için bkz. Yayınlama/abone olma güvenliği.

Çoklu yayın güvenliği

Use this information to understand why security processes might be needed with IBM MQ Multicast.

IBM MQ Multicast 'ın yerleşik güvenliği yok. Güvenlik denetimleri, MQOPED zamanındaki kuyruk yöneticisinde işlenir ve MQMD alanı ayarı istemci tarafından işlenir. Ağdaki bazı uygulamalar IBM MQ uygulaması olmayabilir (örneğin, LLM uygulamaları, daha fazla bilgi için bkz. IBM MQ Low Latency Messaging ile çoklu yayın birlikte çalışabilirlik), bu nedenle uygulama almak, bağlam alanlarının geçerliğinden emin olamayacağı için kendi güvenlik yordamlarınızı uygulamanız gerekebilir.

Göz önünde bulundurulması gereken üç güvenlik süreci vardır:

Erişim denetimi

IBM MQ içindeki erişim denetimi kullanıcı kimliklerine dayalıdır. Bu konuyla ilgili daha fazla bilgi için bkz. “İstemciler için erişim denetimi” sayfa 93.

Ağ Güvenliği

Yalıtılmış bir ağ, sahte iletileri önlemek için uygun bir güvenlik seçeneği olabilir. Çoklu yayın grubu adresindeki bir uygulama, aynı çoklu yayın grubu adresinde bir uygulamadan gelen, MQ iletilerinden ayırt edilemeyen yerel iletişim işlevlerini kullanarak kötü amaçlı iletileri yayınlayabilirler.

Aynı çoklu yayın grubu adresinde başka istemciler için amaçlanan iletileri almak için çok hedefli grup adresinde bir istemci için de bu olanak mümkündür.

Çok noktaya yayın ağının yalıtılması, yalnızca geçerli istemcilerin ve uygulamaların erişime sahip olmasını sağlar. Bu güvenlik önlemi, kötü niyetli iletilerin gelmesini önleyebilir ve gizli bilgilerin dışarı çıkmalarını engelleyebilir.

Çoklu yayın grubu ağ adreslerine ilişkin bilgi için bkz. Çok noktaya gönderim trafiği için uygun ağın ayarlanması

Dijital imzalar

Dijital imza, bir iletinin gösterimini şifreleyerek oluşturulur. Şifreleme, imzaya ilişkin özel anahtarı kullanır ve verimlilik için genellikle iletinin kendisinden ziyade bir ileti özeti üzerinde çalışır. Bir MQPUT iyi bir güvenlik önlemi olmadan önce bir iletiyi dijital olarak imzalamak, ancak büyük bir ileti hacmi varsa, bu işlemin başarım üzerinde olumsuz etkisi olabilir.

Dijital imzalar imzalanmakta olan verilere göre değişir. İki farklı ileti aynı varlık tarafından dijital olarak imzalanırsa, iki imza farklı olur, ancak her iki imza da aynı genel anahtarla doğrulanabilir; yani, iletileri imzalayan varlığın genel anahtarı.

Bu bölümde daha önce belirtildiği gibi, çok hedefli grup adresindeki bir uygulamanın, MQ iletilerinden ayırt edilemeyen yerli iletişim işlevlerini kullanarak kötü amaçlı iletileri yayınlayabileceği bir uygulama olabilir. Dijital imzalar köken kanıtı sağlar ve sadece gönderen özel anahtarı bilir, bu da gönderenin mesajın kaynağı olduğuna dair güçlü kanıtlar sağlar.

Bu konuyla ilgili daha fazla bilgi için bkz. “Şifreleme kavramları” sayfa 7.

Güvenlik duvarları ve İnternet üzerinden düzgeçiş

Normalde bir güvenlik duvarını kullanarak düşmanca IP adreslerinden erişimi önlemek için kullanabilirsiniz. Örneğin, Hizmet Dışı Bırakma saldırılarında. Ancak, güvenlik duvarı kurallarını

güncelleştirmek için bir güvenlik yöneticisi beklerken, IBM MQiçindeki IP adreslerini geçici olarak engellemeye gerek duyabilirsiniz.

Bir ya da daha çok IP adresini engellemek için, BLOCKADR ya da ADDRESSMAP tipinde bir kanal kimlik doğrulaması kaydı yaratın. Daha fazla bilgi için, bkz. “Belirli IP adreslerinin engellenmesi” sayfa 369.

IBM MQ Internet Pass-Thrugüvenliği

IBM MQ Internet Pass-Thru , bir güvenlik duvarı aracılığıyla iletişimi basitleştirebilir, ancak bunun güvenlik açısından etkileri olur.

IBM MQ Internet Pass-Thru (MQIPT) is an optional component of IBM MQ that can be used to implement messaging solutions between remote sites across the internet.

MQIPT , iki kuyruk yöneticisinin iletileri ya da bir kuyruk yöneticisine bağlanmak için bir IBM MQ istemci uygulamasını, doğrudan TCP/IP bağlantısı gerektirmeden Internet üzerinden değiştirebilmesini sağlar. Bir güvenlik duvarının iki sistem arasında doğrudan TCP/IP bağlantısını engelliyorsa, bu olanak yararlı olur. Bu, HTTP içindeki akışları ya da yetkili sunucu olarak işlev görerek, IBM MQ kanal iletişim kuralının geçişini güvenlik duvarının daha basit ve daha kolay yönetilebilir bir şekilde içine ve dışına aktarıyor. TLS (Transport Layer Security; İletim Katmanı Güvenliği) olanağının kullanılması, Internet üzerinden gönderilen iletileri şifrelemek ve bu iletilerin şifresini çözmek için de kullanılabilir.

When your IBM MQ system communicates with MQIPT, unless you are using SSL proxy mode in MQIPT, ensure that the CipherSpec used by IBM MQ matches the CipherSuite used by MQIPT:

- MQIPT TLS sunucusu olarak hareket ettiğinde ve IBM MQ TLS istemcisi olarak bağlantı kurduğunda, IBM MQ tarafından kullanılan CipherSpec , ilgili MQIPT anahtar halkasında etkinleştirilmiş bir CipherSuite ile karşılık gelmelidir.
- MQIPT TLS istemcisi olarak hareket ederken ve bir IBM MQ TLS sunucusuna bağlandığında, MQIPT CipherSuite , alıcı IBM MQ kanalında tanımlı olan CipherSpec ile eşleşmelidir.

If you migrate from MQIPT to the integrated IBM MQ TLS support, transfer the digital certificates from the MQIPT key ring using either **mqiptKeyman** or **mqiptKeycmd**.

Daha fazla bilgi için bkz. IBM MQ Internet Pass-Thru.

z/OS IBM MQ for z/OS güvenlik somutlaması denetim listesi

This topic gives a step-by-step procedure you can use to work out and define the security implementation for each of your IBM MQ queue managers.

RACF , belirtilen statik Sınıf Tanımlayıcı Tablosuna (CDT) IBM MQ güvenlik sınıflarına ilişkin tanımlar sağlar. Denetim listesinde çalışırken, ayarlarınızın hangi sınıflardan hangilerinin gerektiğini saptayabilirsiniz. Bunların “RACF güvenlik sınıfları” sayfa 176içinde açıklandığı şekilde etkinleştirildiğinden emin olmanız gerekir.

Ayrıntılar için, özellikle “IBM MQ kaynaklarına erişimi denetlemek için kullanılan profiller” sayfa 185' te diğer bölümlere bakın.

Güvenlik denetimi gerekiyorsa, bunu gerçekleştirmek için bu denetim listesini izleyin:

1. RACF MQADMIN (büyük harfli tanıtımlar) ya da MXADMIN (karma vaka tanıtımları) sınıfını etkinleştirin.
   - Kuyruk paylaşım grubu düzeyinde, kuyruk yöneticisi düzeyinde ya da her ikisinin bir birleşiminden güvenlik istiyor musunuz?

     Bkz. “Kuyruk paylaşım grubunu ya da kuyruk yöneticisi düzeyinde güvenliği denetlemek için tanıtımlar” sayfa 181.
2. Bağlantı güvenliğine gerek var mı?
   - **Evet**: MQCONN sınıfını etkinleştirin. MQCONN sınıfındaki kuyruk yöneticisi düzeyinde ya da kuyruk paylaşım grubu düzeyinde uygun bağlantı tanıtımlarını tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin.

Not: İlgili bağlantı tanıtımlarına yalnızca, MQCONN API isteği ya da CICS ya da IMS adres alanı kullanıcı kimliklerinin erişmesi gerekir.

- **Hayır**: Bir hlq.NO.CONNECT.CHECKS tanıtımı, MQADMIN ya da MXADMIN sınıfındaki kuyruk yöneticisi düzeyinde ya da kuyruk paylaşım grubu düzeyinde yer alan bir düzeyden birine sahip.

3. Komutlara ilişkin güvenlik denetimi gerekiyor mu?
   - **Evet**: MQCMDS sınıfını etkinleştirin. MQCMDS sınıfındaki kuyruk yöneticisi düzeyinde ya da kuyruk paylaşım grubu düzeyinde uygun komut tanıtımlarını tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin.

     Bir kuyruk paylaşım grubu kullanıyorsanız, kuyruk yöneticisinin kendisi ve kanal başlatıcı tarafından kullanılan kullanıcı kimliklerini eklemeniz gerekebilir. Bkz. "IBM MQ for z/OS kaynak güvenliğinin ayarlanması" sayfa 243.
   - **Hayır**: Bir hlq.NO.CMD.CHECKS tanıtımı.
4. Komutlarda kullanılan kaynaklar için güvenliğe gereksiniminiz var mı?
   - **Evet**: MQADMIN ya da MXADMIN sınıfının etkin olduğundan emin olun. MQADMIN ya da MXADMIN sınıfındaki kuyruk yöneticisi düzeyindeki ya da kuyruk paylaşım grubu düzeyinde kaynakların korunmasına ilişkin uygun tanıtımları tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin. Set the CMDUSER parameter in CSQ6SYSP to the default user ID to be used for command security checks.

     Bir kuyruk paylaşım grubu kullanıyorsanız, kuyruk yöneticisinin kendisi ve kanal başlatıcı tarafından kullanılan kullanıcı kimliklerini eklemeniz gerekebilir. Bkz. "IBM MQ for z/OS kaynak güvenliğinin ayarlanması" sayfa 243.
   - **Hayır**: Bir hlq.NO.CMD.RESC.CHECKS tanıtımı.
5. Kuyruk güvenliğine gerek var mı?
   - **Evet**: MQQUEUE ya da MXQUEUE sınıfını etkinleştirin. MQQUEUE ya da MXQUEUEclass içinde, gerekli kuyruk yöneticisi ya da kuyruk paylaşım grubu için uygun kuyruk tanıtımlarını tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin.
   - **Hayır**: Bir hlq.NO.QUEUE.CHECKS tanıtımı.
6. Süreç güvenliğine gereksiniminiz var mı?
   - **Evet**: MQPROC ya da MXPROC sınıfını etkinleştirin. Kuyruk yöneticisinde ya da kuyruk paylaşım grubu düzeyinde uygun süreç tanıtımlarını tanımlayın ve uygun kullanıcılara ya da grupların bu tanıtımlara erişmesine izin verin.
   - **Hayır**: Bir hlq.NO.PROCESS.CHECKS tanıtımı.
7. Ad listesi güvenliğine gerek var mı?
   - **Evet**: MQNLIST ya da MXNlistclass öğesini etkinleştirin. MQNLIST ya da MXNLIST sınıfındaki kuyruk yöneticisi düzeyinde ya da kuyruk paylaşım grubu düzeyinde uygun ad listesi tanıtımlarını tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin.
   - **Hayır**: Bir hlq.NO.NLIST.CHECKS tanıtımı.
8. Konu güvenliğine ihtiyacınız var mı?
   - **Evet**: MXKONU sınıfını etkinleştirin. MXTOPIC sınıfındaki kuyruk yöneticisi düzeyinde ya da kuyruk paylaşım grubu düzeyinde uygun konu profillerini tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin.
   - **Hayır**: Bir hlq.NO.TOPIC.CHECKS tanıtımı.
9. Bağlamın kullanımıyla ilgili olarak, kullanıcıların MQOPEN ya da MQPUT1 seçeneklerinin kullanımını korumak zorunda olması gerekir?
   - **Evet**: MQADMIN ya da MXADMIN sınıfının etkin olduğundan emin olun. MQADMIN ya da MXADMIN sınıfındaki kuyrukta, kuyruk yöneticisinde ya da kuyruk paylaşım grubu düzeyinde hlq.CONTEXT.queuename tanıtımlarını tanımlayın. Daha sonra, uygun kullanıcılara ya da grupların bu profillere erişmesine izin verin.

- **Hayır**: Bir hlq.NO.CONTEXT.CHECKS tanıtımı.

10. Diğer kullanıcı kimliklerinin kullanımını korumanız gerekiyor mu?
    - **Evet**: MQADMIN ya da MXADMIN sınıfının etkin olduğundan emin olun. Uygun hlq.ALTERNATE.USER. Gerekli kuyruk yöneticisi ya da kuyruk paylaşım grubu için*alternateuserid* profilleri ve gerekli kullanıcıların ya da grupların bu profillere erişmesine izin verir.
    - **Hayır**: Profili tanımlayın hlq.NO.ALTERNATE.USER.CHECKS , MQADMIN ya da MXADMIN sınıfındaki gerekli kuyruk yöneticisi ya da kuyruk paylaşım grubu için.
11. Kaynak güvenlik denetimleri için kullanılacak kullanıcı kimliklerinin RESDüL yoluyla uyarlanmasına gerek var mı?
    - **Evet**: MQADMIN ya da MXADMIN sınıfının etkin olduğundan emin olun. MQADMIN ya da MXADMIN sınıfındaki kuyruk yöneticisi düzeyinde ya da kuyruk paylaşım grubu düzeyinde bir hlq.RESLEVEL tanıtımı tanımlayın. Daha sonra, gerekli kullanıcılara ya da gruplara tanıtıma erişim izni verin.
    - **Hayır**: hlq.RESLEVELiçin geçerli olacak MQADMIN ya da MXADMIN sınıfında soysal profillerin var olmadığından emin olun. Gerekli kuyruk yöneticisi ya da kuyruk paylaşım grubu için bir hlq.RESLEVEL tanıtımı tanımlayın ve bu tanıtıma hiçbir kullanıcının ya da grubun erişmemesine dikkat edin.
12. Kullanılmayan kullanıcı kimliklerinin IBM MQ 'den' zamanaşımına uğraması ' gerekiyor mu?
    - **Evet**: Hangi zamanaşımı değerlerini kullanmak istediğiniz saptayın ve TIMEOUT ve INTERVAL parametrelerini değiştirmek için MQSC ALTER SECURITY komutunu verin.
    - **Hayır**: INTERVAL değerini sıfır olarak ayarlamak için MQSC ALTER SECURITY komutunu verin.

    Not: Altsistem tarafından kullanılan CSQINP1 başlatma girişi veri kümesini güncelleyin; böylece, kuyruk yöneticisi başlatıldığında MQSC ALTER SECURITY komutunun otomatik olarak yayınını sağlar.
13. Dağıtılmış kuyruklama mı kullanıyorsunuz?
    - **Evet**: Kanal kimlik doğrulama kayıtlarını kullanın. Daha fazla bilgi için bkz “Kanal doğrulama kayıtları” sayfa 47.
    - Ayrıca, her kanal için uygun MCAUSER öznitelik değerini belirleyebilir ya da uygun kanal güvenliği çıkışları sağlayabilirsiniz.
14. TLS (Transport Layer Security; İletim Katmanı Güvenliği) olanağını kullanmak istiyor musunuz?
    - **Evet**: Belirtilen DN ' yi içeren bir TLS kişisel sertifikası sunan herhangi bir kullanıcının belirli bir MCAUSER kullanmasını belirtmek için, SSLPEERMAP tipinde bir kanal kimlik doğrulaması kaydı ayarlayın. Genel arama karakterleri de içinde olmak üzere tek bir ayırt edici ad ya da bir kalıp belirleyebilirsiniz.
    - TLS altyapınızı planlayın. z/OS' ın System SSL özelliğini kurun. RACF'ta sertifika adı süzgeçlerinizi (CNF' ler) ayarlayın, bunları kullanıyorsanız ve dijital sertifikalarınızı ayarlayın. SSL anahtar halkasını ayarlayın. SSLKEYR kuyruk yöneticisi özniteliğinin boş olmadığını ve SSL anahtar halkasına işaret ettiğini doğrulayın. Ayrıca, SSLASKS değerinin en az 2 olduğunu da doğrulayın.
    - **Hayır**: SSLKEYR 'nin boş olduğundan ve SSLASKS' ın sıfır olduğundan emin olun.

    TLS ile ilgili daha fazla ayrıntı için bkz. “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22.
15. Müşteri kullanıyor musunuz?
    - **Evet**: Kanal kimlik doğrulama kayıtlarını kullanın.
    - Ayrıca, her bir sunucu bağlantısı kanalı için uygun MCAUSER özniteliği değerini belirleyebilir ya da gerekirse uygun kanal güvenliği çıkışları sağlayabilirsiniz.
16. Anahtar ayarlarınızı denetleyin.

    IBM MQ , güvenlik ayarlarınızı görüntüleyen kuyruk yöneticisi başlatıldığında iletiler yayınlar. Anahtarlarınızın düzgün şekilde ayarlanıp ayarlanmadığını belirlemek için bu iletileri kullanın.
17. İstemci uygulamalarından parola göndermenizi istiyor musunuz?

- **Evet**: z/OS özelliğinin kurulu olduğundan ve Integrated Cryptographic Service Facility 'nin (Integrated Cryptographic Service Facility) en iyi koruma için başlatıldığından emin olun.
- **Hayır**: ICSF ' nin başlatılamadığını bildiren hata iletisini yoksayabilirsiniz.

ICSF ile ilgili daha fazla bilgi için bkz. “Integrated Cryptographic Service Facility (ICSF) olanağının kullanılması” sayfa 251

Güvenliğin ayarlanması

Bu konu derlemi, farklı işletim sistemlerine ve istemcilerin kullanımına özgü bilgileri içerir.

ULW UNIX, Linux, and Windowsüzerinde güvenliğin ayarlanması

UNIX, Linux, and Windows sistemlerine özgü güvenlik konuları.

IBM MQ kuyruk yöneticileri potansiyel olarak değerli olan bilgileri aktarır; bu nedenle, yetkisiz kullanıcıların kuyruk yöneticilerinize erişememelerini sağlamak için bir yetki sistemi kullanmanız gerekir. Aşağıdaki güvenlik denetimi tiplerini göz önünde bulundurun:

IBM MQ' u yönetebilen
IBM MQ' ı denetlemek için komut alabilen kullanıcılar kümesini tanımlayabilirsiniz.

Who can use IBM MQ objects
Aşağıdaki işlemi yapmak için, hangi kullanıcıların (genellikle uygulamalar) MQI çağrılarını ve PCF komutlarını kullanabileceğini tanımlayabilirsiniz:

- Bir kuyruk yöneticisine kimlerin bağlanabileceği.
- Nesnelere (kuyruklar, süreç tanımlamaları, ad listeleri, kanallar, istemci bağlantı kanalları, dinleyiciler, hizmetler ve kimlik doğrulama bilgileri nesneleri) kimler erişebilir ve bu nesnelere ne tür erişim elde edebilir.
- Who can access IBM MQ messages.
- Bir iletiyle ilişkili bağlam bilgilerine erişebilen kişi.

Kanal güvenliği
Uzak sistemlere ileti göndermek için kullanılan kanalların gerekli kaynaklara erişebilmesi için kanalların kullanılmasını sağlamanız gerekir.

Program kitaplıklarına, MQI bağlantı kitaplıklarına ve komutlara erişim izni vermek için standart işletim olanaklarını kullanabilirsiniz. Ancak, kuyrukları ve diğer kuyruk yöneticisi verilerini içeren dizin IBM MQ' e özeldir; MQI kaynaklarına yetki vermek ya da yetkiyi iptal etmek için standart işletim sistemi komutlarını kullanmaz.

ULW Yetkilendirmeler UNIX, Linux, and Windowsüzerinde nasıl çalışır

Bu bölümdeki konularla ilgili yetki belirtimi tabloları, yetkilerin nasıl çalıştığını ve sınırlamaların nasıl uygulantıldığını tanımlar.

Tablolar bu durumlara uygulanır:

- MQI çağrılarını veren uygulamalar
- Çıkış PCF ' leri olarak MQSC komutlarını veren denetim programları
- PCF komutlarını veren denetim programları

Bu bölümde, bilgiler aşağıdaki özellikleri belirten bir çizelge kümesi olarak sunulur:

Gerçekleştirilecek işlem
MQI seçeneği, MQSC komutu ya da PCF komutu.

Erişim denetimi nesnesi
Kuyruk, süreç, kuyruk yöneticisi, ad listesi, kimlik doğrulama bilgileri, kanal, istemci bağlantı kanalı, dinleyici ya da hizmet.

Yetki gerekiyor
MQZAO_ sabiti olarak ifade edilir.

Çizelgelerde, MQZAO_ öneki olan değişmezler, belirli bir varlık için `setmqaut` komutu yetki listesindeki anahtar sözcüklere karşılık gelir. Örneğin, MQZAO_BROWSE, `+browse`anahtar sözcüğünün karşılığıdır, MQZAO_SET_ALL_CONTEXT, `+setall`anahtar sözcüğünün karşılığıdır ve bu şekilde devam eder. Bu sabitler, ürünle birlikte sağlanan cmqzc.hüstbilgi dosyasında tanımlanır.

ULW *MQI çağrılarına ilişkin yetkiler*

MQCONN, **MQOPEN**, **MQPUT1**ve **MQCLOSE** , yetkilendirme denetimlerini gerektirebilir. Bu konudaki tablolar, her çağrı için gerekli olan yetkileri özetlemektedir.

Bir uygulamanın, belirli bir MQI çağrılarını ve seçeneklerini yalnızca, çalıştığı kullanıcı kimliği (ya da yetkileri varsayabilecek) ilgili yetkiye sahip olması durumunda yayınlanabilir.

Dört MQI çağrısı yetkilendirme denetimlerini gerektirebilir: **MQCONN**, **MQOPEN**, **MQPUT1**, ve **MQCLOSE**.

MQOPEN ve **MQPUT1**için, yetki denetimi, ad ya da ad üzerinde değil, açılmakta olan nesnenin adı üzerinde yapılır ve bir ad çözüldükten sonra bu nesne adı üzerinde değişiklik yapılır. Örneğin, bir uygulamanın, diğer adın çözdüğü temel kuyruğu açma yetkisi olmadan bir diğer ad kuyruğunu açma yetkisi verilmiş olabilir. Kural, kuyruk yöneticisi diğer adı doğrudan açılmadıkça, kuyruk yöneticisi diğer adı olmayan bir adı çözme işlemi sırasında saptanan ilk tanımlamada gerçekleştirilir; yani, nesnenin adı nesne tanımlayıcısının *ObjectName* alanında görüntülenir. Açılmakta olan nesne için her zaman yetki gereklidir. Bazı durumlarda, kuyruk yöneticisi nesnesine ilişkin bir yetki yoluyla elde edilen ek kuyruk-bağımsız yetki gereklidir.

Çizelge 10 sayfa 122, Çizelge 11 sayfa 122, Çizelge 12 sayfa 123ve Çizelge 13 sayfa 124 , her çağrı için gereken yetkileri özetlemektedir. *Uygulanamaz* tablolarında, yetki denetimi bu işlemle ilgili olmadığı anlamına gelir; *Denetim yok* , yetki denetimi yapılmadığı anlamına gelir.

Not: Bu çizelgelerdeki adlardan, kanallardan, istemci bağlantı kanallarından, dinleyicilerden, hizmetlerden ya da kimlik doğrulama bilgileri nesnelerinden herhangi bir söz etmiyorsanız. Bunun nedeni, aynı yetkilerin diğer nesneler için geçerli olduğu MQOO_SORGULAMAK dışında, bu nesnelerle ilgili yetkilerin hiçbirinin uygulanmadığı içindir.

Özel yetki MQZAO_ALL_MQI, denetim yetkileri olarak sınıflanan MQZAO_DELETE ve MQZAO_DISPLAY dışında, nesne tipiyle ilgili tüm yetkilerin içermesini sağlar.

İleti bağlamı seçeneklerinden herhangi birini değiştirmek için, aramayı yayınlamak için gereken yetkilerin olması gerekir. Örneğin, MQOO_SET_IDENTITY_CONTEXT ya da MQPMO_SET_IDENTITY_CONTEXT kullanabilmek için `+setid` iznine sahip olmanız gerekir.

Çizelge 10. MQCONN çağrıları için güvenlik yetkisi gerekli

Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 124)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQCONN	Burada geçerli değil	Burada geçerli değil	MQZAO_CONNECT

Çizelge 11. MQOPEN çağrıları için güvenlik yetkisi gerekli

Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 124)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQOO_SORGULAMA	MQZAO_SORGULAMA	MQZAO_SORGULAMA	MQZAO_SORGULAMA
MQOO_BROWSE	MQZAO_GÖZAT	Burada geçerli değil	Denetim yok
MQOO_INPUT_ *	MQZAO_INPUT	Burada geçerli değil	Denetim yok
MQOO_SAVE_ ALL_CONTEXT **(“2” sayfa 124)**	MQZAO_INPUT	Burada geçerli değil	Burada geçerli değil

Çizelge 11. MQOPEN çağrıları için güvenlik yetkisi gerekli (devamı var)

Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 124)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQOO_OUTPUT (Olağan kuyruk) **("3" sayfa 124)**	MQZAO_OUTPUT	Burada geçerli değil	Burada geçerli değil
MQOO_PASPAS_ IDENTITY_CONTEXT **("4" sayfa 124)**	MQZAO_PASPAS_ IDENTITY_CONTEXT	Burada geçerli değil	Denetim yok
MQOO_PASS_ALL_ CONTEXT **("4" sayfa 124, "5" sayfa 124)**	MQZAO_PASS _ALL_CONTEXT	Burada geçerli değil	Denetim yok
MQOO_SET_ IDENTITY_CONTEXT **("4" sayfa 124, "5" sayfa 124)**	MQZAO_SET_ IDENTITY_CONTEXT	Burada geçerli değil	MQZAO_SET_ IDENTITY_CONTEXT **("6" sayfa 124)**
MQOO_SET_ ALL_CONTEXT **("4" sayfa 124, "7" sayfa 124)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("6" sayfa 124)**
MQOO_OUTPUT (İletim kuyruğu) **("8" sayfa 124)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("6" sayfa 124)**
MQOO_SET	MQZAO_SET	Burada geçerli değil	Denetim yok
MQOO_ALTERNATE_ USER_AUTHORITY	**("9" sayfa 124)**	**("9" sayfa 124)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("9" sayfa 124, "10" sayfa 124)**

Çizelge 12. MQPUT1 çağrıları için güvenlik yetkilendirmesi gerekiyor

Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 124)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQPMO_PASPAS_ IDENTITY_CONTEXT	MQZAO_PASPAS_ IDENTITY_CONTEXT **("11" sayfa 124)**	Burada geçerli değil	Denetim yok
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASPAS_ ALL_CONTEXT **("11" sayfa 124)**	Burada geçerli değil	Denetim yok
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **("11" sayfa 124)**	Burada geçerli değil	MQZAO_SET_ IDENTITY_CONTEXT **("6" sayfa 124)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("11" sayfa 124)**	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("6" sayfa 124)**
(İletim kuyruğu) **("8" sayfa 124)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("6" sayfa 124)**

Çizelge 12. MQPUT1 çağrıları için güvenlik yetkilendirmesi gerekiyor (devamı var)			
Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 124)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQPMO_ALTERNATE_USER_AUTHORITY	**("12" sayfa 124)**	Burada geçerli değil	MQZAO_ALTERNATE_USER_AUTHORITY **("10" sayfa 124)**

Çizelge 13. MQCLOSE çağrıları için güvenlik yetkisi gerekli			
Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 124)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQCO_DELETE	MQZAO_DELETE **("13" sayfa 124)**	Burada geçerli değil	Burada geçerli değil
MQCO_DELETE _PURGE	MQZAO_DELETE **("13" sayfa 124)**	Burada geçerli değil	Burada geçerli değil

Tablolara ilişkin notlar:

1. Bir model kuyruğu açılıyorsa:
   - Model kuyruğu için, açtığınız erişim tipine ilişkin model kuyruğunu açma yetkisine ek olarak, model kuyruğu için MQZAO_DISPLAY yetkisi gereklidir.
   - Devingen kuyruk yaratmak için MQZAO_CREATE yetkisi gerekli değil.
   - Model kuyruğunu açmak için kullanılan kullanıcı kimliği, yaratılan dinamik kuyruk için kuyruğa özgü tüm yetkileri (MQZAO_ALL ile eşdeğer) otomatik olarak kabul edilir.
2. MQOO_INPUT_ * da belirtilmelidir. Bu, yerel, model ya da diğer ad kuyruğu için geçerlidir.
3. Bu denetim, iletim kuyrukları dışında tüm çıkış senaryoları için gerçekleştirilir (bkz. not "8" sayfa 124).
4. MQOO_OUTPUT da belirtilmeli.
5. MQOO_PASS_IDENTITY_CONTEXT, bu seçenek tarafından da örtük olarak belirtilir.
6. Bu yetki, hem kuyruk yöneticisi nesnesi hem de belirli bir kuyruk için gereklidir.
7. MQOO_PASST_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT ve MQOO_SET_IDENTITY_CONTEXT, bu seçenek tarafından da örtük olarak belirtilir.
8. This check is performed for a local or model queue that has a *Kullanım* queue attribute of MQUS_TRANSMISSION, and is being opened directly for output. Bir uzak kuyruk açılırsa (uzak kuyruk yöneticisinin ve uzak kuyruğun adlarını belirterek ya da uzak kuyruğun yerel tanımlamasının adını belirleyerek) bu değer uygulanmaz.
9. En az bir MQOO_SORGULAMASI (herhangi bir nesne tipi için) ya da MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT ya da MQOO_SET (kuyruklar için) da belirtilmelidir. Yapılan denetim, belirtilen diğer seçenekler için, belirtilen nesne yetkisi için sağlanan diğer kullanıcı kimliğini ve MQZAO_ALTERNATE_USER_IDENTIFIER denetim öğesine ilişkin yürürlükteki uygulama yetkisini kullanır.
10. Bu yetki, *AlternateUserTnt* ' in belirtilmesine izin verir.
11. An MQZAO_OUTPUT check is also carried out if the queue does not have a *Kullanım* queue attribute of MQUS_TRANSMISSION.
12. Yapılan denetim, belirtilen diğer seçenekler için, belirtilen kuyruk yetkisi için sağlanan diğer kullanıcı kimliğini ve MQZAO_ALTERNATE_USER_IDENTIFIER denetim öğesine ilişkin yürürlükteki uygulama yetkisini kullanır.
13. Bu denetim yalnızca, aşağıdaki deyimlerin her ikisi de doğru olduğunda gerçekleştirilir:
    - Kalıcı bir dinamik kuyruk kapatılmakta ve silinmektedir.

- Kuyruk, kullanılmakta olan nesne tanıtıcı değeri döndüren MQOPEN çağrısı tarafından yaratılmadı.

Yoksa, kontrol falan yok.

ULW *Çıkış PCF ' lerinde MQSC komutlarına ilişkin yetkiler*

Bu bilgiler, Escape PCF ' de bulunan her MQSC komutu için gereken yetkileri özetler.

Uygulanabilir değil , bu işlemin bu nesne tipiyle ilgili olmadığı anlamına gelir.

Komutu gönderen programın altında çalışmakta olan kullanıcı kimliği, aşağıdaki yetkilerin de geçerli olması gerekir:

- MQZAO_CONNECT yetkisi kuyruk yöneticisi için
- PCF komutlarını gerçekleştirmek için kuyruk yöneticisinde MQZAO_DISPLAY yetkisi
- Escape PCF komutu metninde MQSC komutunu verme yetkisi

ALTER *nesnesi*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	MQZAO_CHANGE
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE
İletişim bilgileri	MQZAO_CHANGE

CLEAR *nesne*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CLEAR
Konu	MQZAO_CLEAR
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	Burada geçerli değil
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil
İletişim bilgileri	Burada geçerli değil

DEFINE *object* NOREPLACE (“1” sayfa 129)

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CREATE **(“2” sayfa 129)**
Konu	MQZAO_CREATE **(“2” sayfa 129)**
Süreç	MQZAO_CREATE **(“2” sayfa 129)**
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CREATE **(“2” sayfa 129)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(“2” sayfa 129)**
Kanal	MQZAO_CREATE **(“2” sayfa 129)**
İstemci bağlantı kanalı	MQZAO_CREATE **(“2” sayfa 129)**
Dinleyici	MQZAO_CREATE **(“2” sayfa 129)**
Hizmet	MQZAO_CREATE **(“2” sayfa 129)**
İletişim bilgileri	MQZAO_CREATE **(“2” sayfa 129)**

DEFINE *nesne* REPLACE (“1” sayfa 129, “3” sayfa 129)

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE
İletişim bilgileri	MQZAO_CHANGE

DELETE *nesnesi*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_DELETE
Konu	MQZAO_DELETE
Süreç	MQZAO_DELETE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_DELETE
Kimlik doğrulama bilgileri	MQZAO_DELETE
Kanal	MQZAO_DELETE

Nesne	Yetki gerekiyor
İstemci bağlantı kanalı	MQZAO_DELETE
Dinleyici	MQZAO_DELETE
Hizmet	MQZAO_DELETE
İletişim bilgileri	MQZAO_DELETE

DISPLAY(***nesne***

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_GÖRÜNTÜLE
Konu	MQZAO_GÖRÜNTÜLE
Süreç	MQZAO_GÖRÜNTÜLE
Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Ad Listesi	MQZAO_GÖRÜNTÜLE
Kimlik doğrulama bilgileri	MQZAO_GÖRÜNTÜLE
Kanal	MQZAO_GÖRÜNTÜLE
İstemci bağlantı kanalı	MQZAO_GÖRÜNTÜLE
Dinleyici	MQZAO_GÖRÜNTÜLE
Hizmet	MQZAO_GÖRÜNTÜLE
İletişim bilgileri	MQZAO_GÖRÜNTÜLE

START ***nesne***

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	MQZAO_CONTROL
Hizmet	MQZAO_CONTROL
İletişim bilgileri	Burada geçerli değil

STOP ***nesne***

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil

Nesne	Yetki gerekiyor
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	MQZAO_CONTROL
Hizmet	MQZAO_CONTROL
İletişim bilgileri	Burada geçerli değil

Kanal Komutları

Komut	Nesne	Yetki gerekiyor
PING KANALI	Kanal	MQZAO_CONTROL
KANALı	Kanal	MQZAO_CONTROL_EXTENDED
KANALıN	Kanal	MQZAO_CONTROL_EXTENDED

Abonelik Komutları

Komut	Nesne	Yetki gerekiyor
ALTER SUB	Konu	MQZAO_CONTROL
ALT	Konu	MQZAO_CONTROL
SUB SIL	Konu	MQZAO_CONTROL
GöRüNTüLE	Konu	MQZAO_GÖRÜNTÜLE

Güvenlik Komutları

Komut	Nesne	Yetki gerekiyor
AUTHREC	Kuyruk yöneticisi	MQZAO_CHANGE
AUTHREC SIL	Kuyruk yöneticisi	MQZAO_CHANGE
YöNETIM	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
YAZAN SAYıSı	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
EKRAN GöRüNTüSü	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
CHLAUTH KüMESI	Kuyruk yöneticisi	MQZAO_CHANGE
CHLAUTH GÖRÜNTÜLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Güvenliği yenileme	Kuyruk yöneticisi	MQZAO_CHANGE

Durum Görüntüler

Komut	Nesne	Yetki gerekiyor
DURUMU GöRüNTüLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE Kanal tipi CLUSSDR ise, iletim kuyruğunda `+inq` yetkisi (ya da eşdeğerde MQZAO_SORT) gerekli olduğunu unutmayın.
LSSTATUS GÖRÜNTÜLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
PUBSUB GÖRÜNTÜLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
SBSTATUS GÖRÜNTÜLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
SVSTATUS GÖRÜNTÜLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
TANıTıM	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE

Küme Komutları

Komut	Nesne	Yetki gerekiyor
CLUSQMGR GöRüNTüLE	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
KüME YENILE	'mqm' grup üyeliği gerekiyor	
KüMEYI Sı	'mqm' grup üyeliği gerekiyor	
QMGR ' YI AS	'mqm' grup üyeliği gerekiyor	
QMGR ' YI Sü	'mqm' grup üyeliği gerekiyor	

Diğer Yönetim Komutları

Komut	Nesne	Yetki gerekiyor
PING QMGR	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
QMGR ' YI YENILE	Kuyruk yöneticisi	MQZAO_CHANGE
QMGR RESET	Kuyruk yöneticisi	MQZAO_CHANGE
GöRüNEN EKRAN	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
-CONN ' I	Kuyruk yöneticisi	MQZAO_CHANGE

Not:

1. DEFE komutları için, MQZAO_DISPLAY yetkisi de belirtildiyse, LIKE nesnesi için ya da uygun SYSTEM.DEFAULT.xxx nesnesi atlanırsa nesne.
2. MQZAO_CREATE yetkisi belirli bir nesne ya da nesne tipine özgü değil. `setmqaut` komutunda QMGR nesne tipi belirtilerek, belirtilen bir kuyruk yöneticisine ilişkin tüm nesneler için yaratma yetkisi verilir.
3. Bu, değiştirilecek nesnenin önceden var olması durumunda geçerlidir. Bu işlem yoksa, denetim DEFINE *object* NOREPLACE için olur.

İlgili bilgiler

Kümeleme: REFRESH CLUSTER en iyi uygulamaları kullanma

ULW *PCF komutlarına ilişkin yetkiler*

Bu bölümde, her PCF komutu için gereken yetkiler özetlenmektedir.

Denetleme yok , yetki denetiminin gerçekleştirilmediği anlamına gelir; *Uygulanamaz* , bu işlemin bu nesne tipiyle ilgili olmadığı anlamına gelir.

Komutu gönderen programın altında çalışmakta olan kullanıcı kimliği, aşağıdaki yetkilerin de geçerli olması gerekir:

- MQZAO_CONNECT yetkisi kuyruk yöneticisi için
- PCF komutlarını gerçekleştirmek için kuyruk yöneticisinde MQZAO_DISPLAY yetkisi

Özel yetki MQZAO_ALL_ADMIN, belirli bir nesneye ya da nesne tipine özgü olmayan MQZAO_CREATE dışında, nesne tipiyle ilgili olan aşağıdaki listedeki tüm yetkileri içerir.

Değişiklik *nesnesi*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
kuyruk yöneticisi	MQZAO_CHANGE
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE
İletişim bilgileri	MQZAO_CHANGE

Clear *nesne*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CLEAR
Konu	MQZAO_CLEAR
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	Burada geçerli değil
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil
İletişim bilgileri	Burada geçerli değil

Copy *nesne* (without replace) (1)

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CREATE **(2)**

Nesne	Yetki gerekiyor
Konu	MQZAO_CREATE **(2)**
Süreç	MQZAO_CREATE **(2)**
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CREATE **(2)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(2)**
Kanal	MQZAO_CREATE **(2)**
İstemci bağlantı kanalı	MQZAO_CREATE **(2)**
Dinleyici	MQZAO_CREATE **(2)**
Hizmet	MQZAO_CREATE **(2)**
İletişim bilgileri	MQZAO_CREATE **(“2” sayfa 135)**

Copy *nesne* (with replace) (1, 4)

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE
İletişim bilgileri	MQZAO_CHANGE

***nesne* yarat (değiştirilmeden) (3)**

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CREATE **(2)**
Konu	MQZAO_CREATE **(2)**
Süreç	MQZAO_CREATE **(2)**
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CREATE **(2)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(2)**
Kanal	MQZAO_CREATE **(2)**
İstemci bağlantı kanalı	MQZAO_CREATE **(2)**
Dinleyici	MQZAO_CREATE **(2)**

Nesne	Yetki gerekiyor
Hizmet	MQZAO_CREATE **(2)**
İletişim bilgileri	MQZAO_CREATE **(2)**

***nesne* yarat (başkasıyla değiştir) (3, 4)**

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE
İletişim bilgileri	MQZAO_CHANGE

Delete *nesne*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_DELETE
Konu	MQZAO_DELETE
Süreç	MQZAO_DELETE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_DELETE
Kimlik doğrulama bilgileri	MQZAO_DELETE
Kanal	MQZAO_DELETE
İstemci bağlantı kanalı	MQZAO_DELETE
Dinleyici	MQZAO_DELETE
Hizmet	MQZAO_DELETE
İletişim bilgileri	MQZAO_DELETE

Inquire *nesne*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_GÖRÜNTÜLE
Konu	MQZAO_GÖRÜNTÜLE
Süreç	MQZAO_GÖRÜNTÜLE
kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE

Nesne	Yetki gerekiyor
Ad Listesi	MQZAO_GÖRÜNTÜLE
Kimlik doğrulama bilgileri	MQZAO_GÖRÜNTÜLE
Kanal	MQZAO_GÖRÜNTÜLE
İstemci bağlantı kanalı	MQZAO_GÖRÜNTÜLE
Dinleyici	MQZAO_GÖRÜNTÜLE
Hizmet	MQZAO_GÖRÜNTÜLE
İletişim bilgileri	MQZAO_GÖRÜNTÜLE

Inquire *nesne* names

Nesne	Yetki gerekiyor
Kuyruk	Denetim yok
Konu	Denetim yok
Süreç	Denetim yok
Kuyruk yöneticisi	Denetim yok
Ad Listesi	Denetim yok
Kimlik doğrulama bilgileri	Denetim yok
Kanal	Denetim yok
İstemci bağlantı kanalı	Denetim yok
Dinleyici	Denetim yok
Hizmet	Denetim yok
İletişim bilgileri	Denetim yok

Başlangıç *nesne*

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	MQZAO_CONTROL
Hizmet	MQZAO_CONTROL
İletişim bilgileri	Burada geçerli değil

Durdur *nesne*

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	MQZAO_CONTROL
Hizmet	MQZAO_CONTROL
İletişim bilgileri	Burada geçerli değil

Kanal Komutları

Komut	Nesne	Yetki gerekiyor
Ping Kanalı	Kanal	MQZAO_CONTROL
İlk Duruma Getir Kanalı	Kanal	MQZAO_CONTROL_EXTENDED
Kanal Çözümle	Kanal	MQZAO_CONTROL_EXTENDED

Abonelik Komutları

Komut	Nesne	Yetki gerekiyor
Aboneliği Değiştir	Konu	MQZAO_CONTROL
Abonelik Yarat	Konu	MQZAO_CONTROL
Aboneliği Sil	Konu	MQZAO_CONTROL
Aboneliği araştır	Konu	MQZAO_GÖRÜNTÜLE

Güvenlik Komutları

Komut	Nesne	Yetki gerekiyor
Yetki Kaydını Ayarla	Kuyruk yöneticisi	MQZAO_CHANGE
Yetki Kaydını Sil	Kuyruk yöneticisi	MQZAO_CHANGE
Yetki Kayıtlarını Sorgulama	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Authoring Authority Service	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Varlık Yetki Sorgusu	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Kanal Doğrulama Kaydını Ayarla	Kuyruk yöneticisi	MQZAO_CHANGE
Kanal Kimlik Doğrulama Kayıtları Sorgula	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Güvenliği Yenile	Kuyruk yöneticisi	MQZAO_CHANGE

Durum Görüntüler

Komut	Nesne	Yetki gerekiyor
Kanal Durumunu Sorgula	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE Kanal tipi CLUSSDR ise, iletim kuyruğunda `+inq` yetkisi (ya da eşdeğerde MQZAO_SORT) gerekli olduğunu unutmayın.
Kanal Dinleyicisi Durumunu Sorgulama	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Bilgi/Alt Durum Sorgula	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Abonelik Durumunu Sorgulama	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Sorgulama Hizmeti Durumu	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Konu Durumunu Sor	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE

Küme Komutları

Komut	Nesne	Yetki gerekiyor
Sorgu Küme Kuyruk Yöneticisi	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Kümeyi Yenile	'mqm' grup üyeliği gerekiyor	'mqm' grup üyeliği gerekiyor
Küme Sıfırlama	'mqm' grup üyeliği gerekiyor	'mqm' grup üyeliği gerekiyor
Kuyruk Yöneticisi Kümesini Askıya Al	'mqm' grup üyeliği gerekiyor	'mqm' grup üyeliği gerekiyor
Sürdürme Kuyruğu Yöneticisi Kümesi	'mqm' grup üyeliği gerekiyor	'mqm' grup üyeliği gerekiyor

Diğer Yönetim Komutları

Komut	Nesne	Yetki gerekiyor
Ping Kuyruğu Yöneticisi	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Kuyruk Yöneticisini Yenile	Kuyruk yöneticisi	MQZAO_CHANGE
Kuyruk Yöneticisini İlk Durumuna Getir	Kuyruk yöneticisi	MQZAO_CHANGE
Kuyruk İstatistiklerini Sıfırla	Kuyruk	MQZAO_DISPLAY ve MQZAO_CHANGE
Bağlantı Sorgula	Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Bağlantıyı Durdur	Kuyruk yöneticisi	MQZAO_CHANGE

Not:

1. Kopyalama komutları için, From nesnesi için MQZAO_DISPLAY yetkisi de gereklidir.
2. MQZAO_CREATE yetkisi belirli bir nesne ya da nesne tipine özgü değil. `setmqaut` komutunda QMGR nesne tipi belirtilerek, belirtilen bir kuyruk yöneticisine ilişkin tüm nesneler için yaratma yetkisi verilir.
3. Create komutları için, uygun SYSTEM.DEFAULT.* nesne.
4. Bu, değiştirilecek nesnenin önceden var olması durumunda geçerlidir. Tersi durumda, bu denetim, kopyaya ya da yaratılmadan yaratılmasına ilişkin olarak olur.

AIX Creating and managing groups on AIX

AIX' ta, NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için SMITTY özelliğini kullanın.

Bu görev hakkında

AIX'ta, bir grup oluşturmak, gruba kullanıcı eklemek, grupta yer alan kullanıcıların listesini görüntülemek ve bir gruptan bir kullanıcıyı kaldırmak için SMITTY' yi kullanabilirsiniz.

Yordam

1. SMITTY ' den **Security and Users** (Güvenlik ve Kullanıcılar) seçeneğini belirleyin ve Enter tuşuna basın.
2. **Gruplar** seçeneğini belirleyin ve Enter tuşuna basın.
3. Bir grup oluşturmak için aşağıdaki adımları tamamlayın:
   a) **Add a Group** (Grup Ekle) seçeneğini belirleyip Enter tuşuna basın.
   b) Gruba eklemek istediğiniz grubun adını ve virgülle ayrılmış olarak, gruba eklemek istediğiniz kullanıcıların adlarını girin.
   c) Grubu oluşturmak için Enter tuşuna basın.
4. Bir gruba kullanıcı eklemek için aşağıdaki adımları tamamlayın:
   a) **Grupların Özelliklerini Değiştir/Göster** seçeneğini belirleyin ve Enter tuşuna basın.
   b) Grup üyelerinin bir listesini göstermek için grubun adını girin.
   c) Gruplara eklemek istediğiniz kullanıcıların adlarını virgüllerle ayırarak ekleyin.
   d) Adları gruba eklemek için Enter tuşuna basın.
5. Bir grupta kimlerin olduğunu görüntülemek için aşağıdaki adımları tamamlayın:
   a) **Grupların Özelliklerini Değiştir/Göster** seçeneğini belirleyin ve Enter tuşuna basın.
   b) Grup üyelerinin bir listesini göstermek için grubun adını girin.
6. Gruptan bir kullanıcıyı kaldırmak için aşağıdaki adımları tamamlayın:
   a) **Grupların Özelliklerini Değiştir/Göster** seçeneğini belirleyin ve Enter tuşuna basın.
   b) Grup üyelerinin bir listesini göstermek için grubun adını girin.
   c) Gruptan kaldırmak istediğiniz kullanıcının adını silin.
   d) Grubu gruptan kaldırmak için Enter tuşuna basın.

Linux Creating and managing groups on Linux

Linux' ta NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için `/etc/group` dosyasını kullanın.

Bu görev hakkında

Linuxüzerinde, grup bilgileri `/etc/group` dosyasında tutulur. Bir grup yaratmak, bir gruba kullanıcı eklemek, grupta yer alan kullanıcıların listesini görüntülemek ve gruptan bir kullanıcıyı kaldırmak için komutları kullanabilirsiniz.

Yordam

1. Yeni bir grup oluşturmak için **groupadd** komutunu kullanın.
   Aşağıdaki komutu yazın:

   ```
   groupadd -g group-ID group-name
   ```

   Burada *grup-tnt* , grubun sayısal tanıtıcısıdır ve *grup-adı* , grubun adıdır.

2. To add a member to a supplementary group, use the **usermod** command to list the supplementary groups that the user is currently a member of, and the supplementary groups that the user is to become a member of.
   Örneğin, kullanıcı zaten `groupa`grubunun bir üyesiyse ve `groupb`üyesi olması durumunda, aşağıdaki komutu kullanın:

   ```
   usermod -G groupa,groupb user-name
   ```

   Burada *kullanıcı-adı* kullanıcı adıdır.
3. Bir grubun üyesi olan kişiyi görüntülemek için **getent** komutunu kullanın.
   Aşağıdaki komutu yazın:

   ```
   getent group group-name
   ```

   Burada *grup-adı* , grubun adıdır.
4. To remove a member from a supplementary group, use the **usermod** command to list the supplementary groups that you want the user to remain a member of.
   Örneğin, kullanıcının birincil grubu `users` ise ve kullanıcı aynı zamanda `mqm`, `groupa` ve `groupb`gruplarının bir üyesiyse, kullanıcıyı `mqm` grubundan kaldırmak için şu komutu kullanın:

   ```
   usermod -G groupa,groupb user-name
   ```

   Burada *kullanıcı-adı* kullanıcı adıdır.

Solaris Creating and managing groups on Solaris

Solaris' ta NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için `/etc/group` dosyasını kullanın.

Bu görev hakkında

Solarisüzerinde, grup bilgileri `/etc/group` dosyasında tutulur. Bir grup yaratmak, bir gruba kullanıcı eklemek, grupta yer alan kullanıcıların listesini görüntülemek ve gruptan bir kullanıcıyı kaldırmak için komutları kullanabilirsiniz.

Yordam

1. Yeni bir grup oluşturmak için **groupadd** komutunu kullanın.
   Aşağıdaki komutu yazın:

   ```
   groupadd -g group-ID group-name
   ```

   Burada *grup-tnt* , grubun sayısal tanıtıcısıdır ve *grup-adı* , grubun adıdır.
2. To add a member to a supplementary group, use the **usermod** command to list the supplementary groups that the user is currently a member of, and the supplementary groups that the user is to become a member of.
   Örneğin, kullanıcı zaten `groupa`grubunun bir üyesiyse ve `groupb`üyesi olması durumunda, aşağıdaki komutu kullanın:

   ```
   usermod -G groupa,groupb user-name
   ```

   Burada *kullanıcı-adı* kullanıcı adıdır.
3. Bir grubun üyesi olan kişiyi bulmak için, `/etc/group` dosyasında bu grubun girişine bakın.
4. To remove a member from a supplementary group, use the **usermod** command to list the supplementary groups that you want the user to remain a member of.
   Örneğin, kullanıcının birincil grubu `users` ise ve kullanıcı aynı zamanda `mqm`, `groupa` ve `groupb`gruplarının bir üyesiyse, kullanıcıyı `mqm` grubundan kaldırmak için şu komutu kullanın:

   ```
   usermod -G groupa,groupb user-name
   ```

Burada *kullanıcı-adı* kullanıcı adıdır.

Windows Creating and managing groups on Windows

Windows' ta, bir iş istasyonundaki ya da üye sunucu makinesinde grupları yönetmek için Bilgisayar Yönetimi özelliğini kullanıyorsunuz.

Bu görev hakkında

Etki alanı denetleyicileri için, kullanıcılar ve gruplar Active Directory(Etkin Dizin) aracılığıyla yönetilir. Active Directory kullanımıyla ilgili daha ayrıntılı bilgi için uygun işletim sistemi yönergelerine bakın.

Bir birincil kullanıcının grup üyeliklerinde yaptığınız değişiklikler, kuyruk yöneticisi yeniden başlatılıncaya kadar tanınmaz ya da **REFRESH SECURITY** MQSC komutunu (ya da PCF eşdeğeri) yayınlayıncaya kadar.

Kullanıcı ve gruplarla çalışmak için Windows Computer Management (Bilgisayar Yönetimi) panosunu kullanın. Oturum açmış olan kullanıcıda yapılan değişiklikler, kullanıcı yeniden oturum açıncaya kadar etkili olmayabilir.

Windows *Windowsüzerinde bir grup oluşturma*

Denetim masasını kullanarak bir grup oluşturun.

Yordam

1. Denetim panosunu aç
2. **Administrative Tools**(Yönetim Araçları) öğesini çift tıklatın
   Yönetim Araçları panosu açılır.
3. **Computer Management**seçeneğini çift tıklatın.
   Bilgisayar Yönetimi panosu açılır.
4. **Yerel Kullanıcılar ve Gruplar**nesnesini açın.
5. **Gruplar**nesnesini farenin sağ düğmesiyle tıklatın ve **Yeni Grup ...**seçeneğini belirleyin.
   Yeni Grup panosu görüntülenir.
6. Grup adı alanına uygun bir ad yazın ve **Yarat**düğmesini tıklatın.
7. **Kapat**'ı tıklatın.

Windows *Windowsüzerinde bir gruba kullanıcı ekleme*

Denetim masasını kullanarak bir kullanıcıyı bir gruba ekleyin.

Yordam

1. Denetim panosunu aç
2. **Administrative Tools**(Yönetim Araçları) öğesini çift tıklatın
   Yönetim Araçları panosu açılır.
3. **Computer Management**seçeneğini çift tıklatın.
   Bilgisayar Yönetimi panosu açılır.
4. Bilgisayar Yönetimi panosundan **Yerel Kullanıcılar ve Gruplar**nesnesini açın.
5. **Kullanıcılar**seçeneğini belirleyin.
6. Bir gruba eklemek istediğiniz kullanıcıyı çift tıklatın.
   Kullanıcı özellikleri panosu görüntülenir.
7. **Üye** sekmesini seçin.
8. Kullanıcıyı eklemek istediğiniz grubu seçin. İstediğiniz grup görünmüyorsa:
   a) **Ekle ...**düğmesini tıklatın.
      Grup Seç panosu görüntülenir.

b) **Konumlar ...**seçeneğini tıklatın.
   Locations (Konumlar) panosu görüntülenir.
c) Kullanıcıyı listeden eklemek istediğiniz grubun yerini seçin ve **Tamam**düğmesini tıklatın.
d) Sağlanan alana grup adını yazın.

   Alternatif olarak, **Gelişmiş ...**düğmesini tıklatın. ve daha sonra, **Şimdi Bul** ' un seçili konumunda bulunan grupları listelemesini sağlar. Buradan, kullanıcıyı eklemek istediğiniz grubu seçin ve **Tamam**' ı tıklatın.
e) **Tamam**'ı tıklatın.
   Kullanıcı özellikleri panosu, eklediğiniz grubun gösterilmesini sağlar.
f) Grubu seçin.

9. **Tamam**'ı tıklatın.
   Computer Management (Bilgisayar Yönetimi) panosu görüntülenir.

Windows *Windows' da bir grupta kimlerin yer aldiğini görüntüleme*

Denetim masasını kullanarak bir grubun üyelerini görüntüler.

Yordam

1. Denetim panosunu aç
2. **Administrative Tools**(Yönetim Araçları) öğesini çift tıklatın
   Yönetim Araçları panosu açılır.
3. **Computer Management**seçeneğini çift tıklatın.
   Bilgisayar Yönetimi panosu açılır.
4. Bilgisayar Yönetimi panosundan **Yerel Kullanıcılar ve Gruplar**nesnesini açın.
5. **Gruplar**seçeneğini belirleyin.
6. Bir grubu çift tıklatın. Grup özellikleri panosu görüntülenir.
   Grup özellikleri panosu görüntülenir.

Sonuçlar

Grup üyeleri görüntülenir.

Windows *Removing a user from a group on Windows*

Denetim panosunu kullanarak bir kullanıcıyı gruptan kaldırın.

Yordam

1. Denetim panosunu aç
2. **Administrative Tools**(Yönetim Araçları) öğesini çift tıklatın
   Yönetim Araçları panosu açılır.
3. **Computer Management**seçeneğini çift tıklatın.
   Bilgisayar Yönetimi panosu açılır.
4. Bilgisayar Yönetimi panosundan **Yerel Kullanıcılar ve Gruplar**nesnesini açın.
5. **Kullanıcılar**seçeneğini belirleyin.
6. Bir gruba eklemek istediğiniz kullanıcıyı çift tıklatın.
   Kullanıcı özellikleri panosu görüntülenir.
7. **Üye** sekmesini seçin.
8. Kullanıcıyı kaldırmak istediğiniz grubu seçin ve **Kaldır**düğmesini tıklatın.
9. **Tamam**'ı tıklatın.
   Computer Management (Bilgisayar Yönetimi) panosu görüntülenir.

Sonuçlar

Şimdi kullanıcıyı gruptan kaldırdınız.

Windows Windowsüzerinde güvenlik için özel dikkat edilmesi gereken noktalar

Bazı güvenlik işlevleri Windows' un farklı sürümlerinde farklı davranır.

IBM MQ güvenliği, kullanıcı yetkileri ve grup üyeliklerine ilişkin bilgi için işletim sistemi API ' larına çağrılara dayanır. Bazı işlevler Windows sistemlerinde aynı şekilde işlev görmez. This collection of topics includes descriptions of how those differences might affect IBM MQ security when you are running IBM MQ in a Windows environment.

Windows *IBM MQ Windows hizmeti için yerel ve etki alanı kullanıcı hesapları*

IBM MQ çalışırken, yalnızca yetkili kullanıcıların kuyruk yöneticilerine ya da kuyruklara erişebildiğini kontrol etmek gerekir. Bu, IBM MQ ' in bu erişimi deneyen herhangi bir kullanıcı hakkında bilgileri sorgulamak için kullanabileceği özel bir kullanıcı hesabı gerektirir.

- “Prepare IBM MQ Wizardile özel kullanıcı hesaplarının yapılandırılması” sayfa 140
- “IBM MQ ile Active Directorykomutunu kullanma” sayfa 140
- “Bir IBM MQ Windows hizmeti için gereken kullanıcı hakları” sayfa 141

Prepare IBM MQ Wizardile özel kullanıcı hesaplarının yapılandırılması

Prepare IBM MQ Wizard , Windows hizmetinin kullanılması gereken süreçlerle paylaşılabilmesi için özel bir kullanıcı hesabı yaratır (bkz. Prepare IBM MQ Wizard ile IBM MQ uygulamasını yapılandırma).

Bir Windows hizmeti, IBM MQ kuruluşu için istemci işlemleri arasında paylaşılır. Her kuruluş için bir hizmet yaratılır. Each service is named `MQ_`*`InstallationName`* , and has a display name of `IBM MQ(`*`InstallationName`*`)`.

Her hizmetin etkileşimli olmayan ve etkileşimli oturum açma oturumları arasında paylaşılması gerektiğinden, her birini özel bir kullanıcı hesabı altında başlatmanız gerekir. Tüm hizmetler için bir özel kullanıcı hesabı kullanabilir ya da farklı özel kullanıcı hesapları oluşturabilirsiniz. Each special user account must have the user right to `Bir hizmet olarak oturum açma`, for more information see Çizelge 14 sayfa 141. Kullanıcı kimliği, hizmeti çalıştırma yetkisine sahip değilse, hizmet başlatılmaz ve Windows sistem olay günlüğünde bir hata döndürür. Tipik olarak, Prepare IBM MQ Wizardkomutunu çalıştırmış ve kullanıcı kimliğini doğru olarak ayarlardınız. Ancak, kullanıcı kimliğini el ile yapılandırdıysanız, çözümlemeniz gereken bir sorun olabilir mi?

IBM MQ 'ı ilk kez kurarken ve Prepare IBM MQ Wizard ' ı ilk kez çalıştırdığınızda, MUSR_MQADMIN adlı hizmet için gerekli ayarlar ve izinlerle (`Bir hizmet olarak oturum açma`de içinde olmak üzere) yerel bir kullanıcı hesabı yaratır.

For subsequent installations, the Prepare IBM MQ Wizard creates a user account named MUSR_MQADMIN*X*, where *X* is the next available number representing a user ID that does not exist. MUSR_MQADMIN*x* için parola, hesap yaratıldığında rasgele oluşturulur ve hizmete ilişkin oturum açma ortamını yapılandırmak için kullanılır. Oluşturulan parolanın süresi dolmaz.

Bu IBM MQ hesabı, belirli bir dönemden sonra hesap parolalarının değiştirilmesini zorunlu kılacak sistemde ayarlanan hesap ilkelerinden etkilenmez.

Parola, bu tek seferlik işlem dışında bilinmez ve kaydın güvenli bir bölümünde Windows işletim sistemi tarafından depolanır.

IBM MQ ile Active Directorykomutunu kullanma

In some network configurations, where user accounts are defined on domain controllers that are using the Active Directory directory service, the local user account that IBM MQ is running under might not have the authority that it requires to query the group membership of other domain user accounts. When you

install IBM MQ, the Prepare IBM MQ Wizard identifies whether this is the case by carrying out tests and asking you questions about the network configuration.

IBM MQ ' in altında çalışmakta olan yerel kullanıcı hesabının gerekli yetkisi yoksa, Prepare IBM MQ Wizard , belirli kullanıcı haklarına sahip bir etki alanı kullanıcı hesabının hesap ayrıntılarını sizden ister. Bir Windows etki alanı hesabı oluşturma ve ayarlama hakkında bilgi için bkz. IBM MQiçin Windows etki alanı hesaplarını oluşturma ve ayarlama. Etki alanı kullanıcı hesabının gerektirdiği kullanıcı hakları için bkz. Çizelge 14 sayfa 141.

When you have entered valid account details for the domain user account into the Prepare IBM MQ Wizard, the wizard configures an IBM MQ Windows service to run under the new account. Hesap ayrıntıları, Kayıt Defterinin güvenli bölümünde tutulur ve kullanıcılar tarafından okunamaz.

Hizmet çalışırken, bir IBM MQ Windows hizmeti başlatılır ve hizmet çalışır durumda olduğu sürece çalışır durumda kalır. Windows hizmeti başlatıldıktan sonra sunucuda oturum açan bir IBM MQ yöneticisi, sunucuda kuyruk yöneticilerini yönetmek için IBM MQ Explorer ' yi kullanabilir. Bu, IBM MQ Explorer ' u var olan Windows hizmet sürecine bağlar. Bu iki işlem, çalışabilmesi için farklı izin düzeylerine gereksinim duyarlar:

- Başlatma işlemi için bir başlatma izni gerekiyor.
- IBM MQ yöneticisi Access izni gerektirir.

Bir IBM MQ Windows hizmeti için gereken kullanıcı hakları

Aşağıdaki tabloda, IBM MQ kuruluşu için Windows hizmetinin altında olduğu yerel ve etki alanı kullanıcı hesapları için gereken kullanıcı hakları listelenir.

Çizelge 14. Bir IBM MQ Windows hizmeti için gereken kullanıcı hakları

İzin	**Tanım**
Toplu iş olarak oturum aç	Bu kullanıcı hesabı altında çalışacak bir IBM MQ Windows hizmetini etkinleştirir.
Hizmet olarak oturum aç	Kullanıcıların, yapılandırılan hesabı kullanarak oturum açmak için IBM MQ Windows hizmetini ayarlamasını sağlar.
Sistemi sona erdirin	Bir hizmetin kurtarılması başarısız olduğunda, IBM MQ Windows hizmetinin sunucuyu yeniden başlatmasına izin verir.
Kotayı büyüt	İşletim sistemi `CreateProcessAsUser` araması için gereklidir.
İşletim sisteminin bir parçası olarak davran	İşletim sistemi `LogonUser` çağrısı için gereklidir.
Geçiş denetimini atla	İşletim sistemi `LogonUser` çağrısı için gereklidir.
Bir işlem düzeyi anahtarını değiştir	İşletim sistemi `LogonUser` çağrısı için gereklidir.

Not: ASP ve IIS uygulamalarının çalışan ortamlarda hata ayıklama programları hakları gerekli olabilir.

Etki alanı kullanıcı hesabınız, Yerel Güvenlik İlkesi uygulamasında listelendiği şekilde, geçerli kullanıcı hakları olarak ayarlanmış bu Windows kullanıcı haklarına sahip olmalıdır. Aksi takdirde, yerel güvenlik ilkesi uygulamasını sunucuda yerel olarak ya da Etki Alanı Güvenlik Uygulaması etki alanını geniş kullanarak ayarlayın.

Windows *Windows Server güvenlik izinleri*

IBM MQ kuruluşu, yerel kullanıcının ya da etki alanı kullanıcısının kuruluşu gerçekleştirmesine bağlı olarak Windows Server 'da farklı bir şekilde davranır.

Bir *yerel* kullanıcı IBM MQkurulursa, Prepare IBM MQ Wizard , IBM MQ Windows hizmeti için oluşturulan yerel kullanıcının kuruluş kullanıcısının grup üyeliği bilgilerini alabileceğini algılar. The Prepare IBM MQ Wizard asks the user questions about the network configuration to determine whether there are other user accounts defined on domain controllers running on Windows 2000 or later. Böyle bir durumda, IBM MQ Windows hizmetinin belirli ayarları ve yetkileri olan bir etki alanı kullanıcı hesabı altında çalışması gerekir. Prepare IBM MQ Wizard , kullanıcıdan bu kullanıcının hesap ayrıntılarını (Prepare IBM MQ Wizard ile IBM MQ uygulamasını yapılandırmaiçinde açıklandığı gibi) ister.

Bir *etki alanı* kullanıcısı IBM MQkurulursa, Prepare IBM MQ Wizard , IBM MQ Windows hizmeti için oluşturulan yerel kullanıcının, kuran kullanıcının grup üyeliği bilgilerini alamıyor olduğunu algılar. Bu durumda, Prepare IBM MQ Wizard her zaman kullanıcıya, kullanılacak IBM MQ Windows hizmeti için etki alanı kullanıcı hesabının hesap ayrıntıları için bilgi isteminde bulunur.

IBM MQ Windows hizmetinin bir etki alanı kullanıcı hesabı kullanması gerektiğinde, IBM MQ , Prepare IBM MQ Wizardkullanılarak yapılandırılıncaya kadar düzgün bir şekilde çalışamaz. Prepare IBM MQ Wizard , Windows hizmeti uygun bir hesapla yapılandırılıncaya kadar, kullanıcının diğer görevlerle devam etmesini sağlar.

Daha fazla bilgi için bkz. IBM MQiçin etki alanı hesaplarını oluşturma ve ayarlama.

Windows *IBM MQ hizmetiyle ilişkili kullanıcı adının değiştirilmesi*

Yeni bir hesap oluşturarak ve ayrıntılarını Prepare IBM MQ Wizardkullanarak girerek IBM MQ hizmetiyle ilişkili kullanıcı adını değiştirebilirsiniz.

Bu görev hakkında

IBM MQ ' ı kurduğunuzda ve Prepare IBM MQ Wizard komutunu ilk kez çalıştırdığınızda, MUSR_MQADMIN adlı hizmet için yerel bir kullanıcı hesabı yaratır. For subsequent installations, the Prepare IBM MQ Wizard creates a user account named MUSR_MQADMIN*X*, where *X* is the next available number representing a user ID that does not exist.

MUSR_MQADMIN ya da MUSR_MQADMIN*x* ' den IBM MQ hizmeti ile ilişkili kullanıcı adını başka bir adla değiştirmeniz gerekebilir. Örneğin, kuyruk yöneticiniz 8 karakterden uzun kullanıcı adlarını kabul etmeyen Db2ile ilişkilendirilmişse, bunu yapmanız gerekebilir.

Yordam

1. Yeni bir kullanıcı hesabı yarat (örneğin, **NEW_NAME**)
2. Yeni kullanıcı hesabının ayrıntılarını girmek için Prepare IBM MQ Wizard değerini kullanın.

İlgili görevler

Prepare IBM MQ Wizard ile IBM MQ uygulamasını yapılandırma

Windows *IBM MQ Windows hizmeti yerel kullanıcı hesabının parolasının değiştirilmesi*

You can change the password of the IBM MQ Windows service local user account by using the Computer Management panel.

Bu görev hakkında

IBM MQ Windows hizmet yerel kullanıcı hesabının parolasını değiştirmek için aşağıdaki adımları gerçekleştirin:

Yordam

1. Hizmetin çalışmakta olduğu kullanıcıyı belirleyin.
2. Stop the IBM MQ service from the Computer Management panel.
3. Gereken parolayı, tek bir kişinin parolasını değiştirdiğiniz şekilde değiştirin.
4. Computer Management (Bilgisayar Yönetimi) panosundan IBM MQ hizmetine ilişkin özelliklere gidin.
5. **Oturum Açma** sayfasını seçin.

6. Belirtilen hesap adının, parolanın değiştirildiği kullanıcıyla eşleştiğini doğrulayın.
7. Type the password into the **Parola** and **Parolayı onayla** fields and click **Tamam**.

Windows *Etki alanı kullanıcı hesabı altında çalışan bir kuruluş için IBM MQ Windows hizmetine ilişkin parolanın değiştirilmesi*

Etki alanı kullanıcı hesabının hesap ayrıntılarını girmek için Prepare IBM MQ Wizard ' yi kullanmaya alternatif olarak, kuruluşa özel IBM MQ Hizmeti için **Oturum Açma** ayrıntılarını değiştirmek üzere Computer Management (Bilgisayar Yönetimi) panosunu kullanabilirsiniz.

Bu görev hakkında

Kuruluş için IBM MQ Windows hizmeti bir etki alanı kullanıcı hesabı altında çalışıyorsa, hesabın parolasını aşağıdaki gibi değiştirebilirsiniz:

Yordam

1. Etki alanı denetleyicide etki alanı hesabına ilişkin parolayı değiştirin. Bunu sizin için etki alanı denetimcinizden sormanız gerekebilir.
2. IBM MQ hizmetine ilişkin **Oturum Açma** sayfasını değiştirmek için aşağıdaki adımları tamamlayın.
   a) Hizmetin altında çalışmakta olduğu kullanıcıyı belirleyin.
   b) Stop the IBM MQ service from the Computer Management panel.
   c) Gereken parolayı, tek bir kişinin parolasını değiştirdiğiniz şekilde değiştirin.
   d) Computer Management (Bilgisayar Yönetimi) panosundan IBM MQ hizmetine ilişkin özelliklere gidin.
   e) **Oturum Açma** sayfasını seçin.
   f) Belirtilen hesap adının, parolanın değiştirildiği kullanıcıyla eşleştiğini doğrulayın.
   g) Type the password into the **Parola** and **Parolayı onayla** fields and click **Tamam**.

   IBM MQ Windows hizmetinin çalıştığı kullanıcı hesabı, kullanıcı arabirimi uygulamaları tarafından yayınlanan ya da sistem başlatma, sona erdirme ya da hizmet kurtarma işlemi sırasında otomatik olarak gerçekleştirilen herhangi bir MQSC komutu yürütür. Bu nedenle, bu kullanıcı hesabının IBM MQ yönetim haklarına sahip olması gerekir. Varsayılan olarak sunucu üzerindeki yerel mqm grubuna eklenir. Bu üyelik kaldırılırsa, IBM MQ Windows hizmeti işe yaramaz. Kullanıcı haklarıyla ilgili daha fazla bilgi için bkz. “Bir IBM MQ Windows hizmeti için gereken kullanıcı hakları” sayfa 141.

   Bir güvenlik sorunu, IBM MQ Windows hizmetinin altında çalıştığı kullanıcı hesabıyla ortaya çıksa, hata iletileri ve tanımlar sistem olay günlüğünde görünür.

İlgili görevler

Prepare IBM MQ Wizard ile IBM MQ uygulamasını yapılandırma

Windows *Windows sunucuları etki alanı denetleyicilerine yükseltilirken dikkat edilmesi gereken noktalar*

Bir Windows sunucusunu bir etki alanı denetleyicisine yükseltiyorsanız, kullanıcı ve grup izinleriyle ilgili güvenlik ayarının uygun olup olmadığını göz önünde bulundurmanız gerekir. When changing the state of a Windows machine between server and domain controller, you should take into consideration that this can affect the operation of IBM MQ because IBM MQ uses a locally-defined mqm group.

Etki alanı kullanıcısı ve grup izinlerine ilişkin güvenlik ayarları

IBM MQ , güvenlik ilkesini uygulamak için grup üyeliği bilgilerine dayanır; bu da, IBM MQ işlemlerini gerçekleştiren kullanıcı kimliğinin diğer kullanıcıların grup üyeliklerini belirleyebilmesi açısından önem gösterir.

When you promote a Windows server to a domain controller, you are presented with an option for the security setting relating to user and group permissions. Bu seçenek, rasgele kullanıcıların etkin dizinden

grup üyeliklerini alabildiğini denetler. Bir etki alanı denetleyicisi ayarlandıysa, yerel hesapların etki alanı kullanıcı hesaplarının grup üyeliğini sorgulama yetkisi varsa, kuruluş işlemi sırasında IBM MQ tarafından yaratılan varsayılan kullanıcı kimliği, diğer kullanıcılara ilişkin grup üyeliklerini gerektiği gibi edinebilir. Ancak, bir etki alanı denetleyicisi, yerel hesapların, etki alanı kullanıcı hesaplarının grup üyeliğini sorgulama yetkisi olmasa da, IBM MQ ' un etki alanında tanımlı olan kullanıcıların kuyruk yöneticilerine ya da kuyruklara erişme yetkisi olan ve erişim başarısız olduğunda denetimlerini tamamlamasını önler. Bu şekilde ayarlanmış bir etki alanı denetleyicisinde Windows kullanıyorsanız, gerekli izinlerin bulunduğu özel bir etki alanı kullanıcısı hesabı kullanılmalıdır.

Bu durumda bilmeniz gerekir:

- Windows sürümünüze ilişkin güvenlik izinlerinin davranışı nasıl davranır?
- Etki alanı mqm grubu üyelerinin grup üyeliklerini okumasına nasıl izin verileceğini.
- How to configure an IBM MQ Windows service to run under a domain user.

Daha fazla bilgi için bakınız: Configuring user accounts for IBM MQ.

Yerel mqm grubunaIBM MQ erişimi

Windows sunucuları, etki alanı denetleyicilerine yükseltildiğinde ya da bu denetleyicilerden indirgendiğinde, IBM MQ yerel mqm grubuna erişimi kaybeder.

Bir sunucu, etki alanı denetleyicisi olarak yükseltildiğinde, kapsam yerel olarak yerel etki alanından etki alanına değişir. Makine sunucuya indirgendiğinde, tüm etki alanı yerel grupları kaldırılır. Bu, bir makineyi sunucudan etki alanı denetleyicisine değiştirmenin ve sunucunun geri sunucuya erişimin yerel bir mqm grubuna erişimi kaybedeceği anlamına gelir. Bu belirti, yerel bir mqm grubunun eksikliğini gösteren bir hatadır; örneğin:

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

Bu sorunu gidermek için, standart Windows yönetim araçlarını kullanarak yerel mqm grubunu yeniden yaratın. Tüm grup üyeliği bilgileri kaybolduğundan, ayrıcalıklı IBM MQ kullanıcılarını yeni oluşturulan yerel mqm grubuna geri getirmeniz gerekir. Makine bir etki alanı üyesiyse, ayrıcalıklı etki alanı IBM MQ kullanıcı kimlikleri için gereken yetki düzeyini vermek için, etki alanı mqm grubunu yerel mqm grubuna da eklemelisiniz.

Windows *Restrictions on nested groups on Windows*

İçiçe yerleşimli grupların kullanımına ilişkin kısıtlamalar vardır. Bu sonuç kısmen etki alanı işlevsel düzeyinden ve kısmen de IBM MQ kısıtlamalarından kaynaklanabilir.

Active Directory , Etki alanı işlevsel düzeyine bağlı olarak bir Etki Alanı bağlamındaki farklı grup tiplerini destekleyebilir. Varsayılan olarak, Windows 2003 etki alanları " Windows 2000 karma " işlevsel düzeyi. (Windows Server 2008 ve Windows Server 2012, Windows 2003 etki alanı modelini izleyin.) Etki alanı işlevsel düzeyi, bir etki alanı ortamında kullanıcı kimlikleri yapılandırılırken, desteklenen grup tiplerini ve içiçe yerleştirme düzeyini belirler. Grup Kapsamı ve içerme ölçütlerine ilişkin ayrıntılar için Active Directory belgelerine bakın.

Active Directory gereksinmelerine ek olarak, IBM MQtarafından kullanılan tanıtıcılar üzerinde daha fazla kısıtlama uygulanır. IBM MQ tarafından kullanılan ağ API ' leri, etki alanı işlevsel düzeyi tarafından desteklenen tüm yapılandırmaları desteklemez. Sonuç olarak, IBM MQ bir Etki Alanı Yerel grubunda bulunan herhangi bir Etki Alanı Tanıtıcılarının grup üyeliklerini sorgulamayamaz ve bu grup, yerel bir grupta içiçe yerleştirilebilir. Ayrıca, genel ve evrensel grupların birden çok içiçe yerleştirilmesi desteklenmez. Ancak, hemen iç içe geçmiş genel gruplar ya da genel gruplar desteklenir.

Windows *Kullanıcılara IBM MQ uzaktan kullanma yetkisi verme*

If you need to create and start queue managers when connected to IBM MQ remotely, you must have the `Genel nesneler yarat` user access.

Bu görev hakkında

Not: Denetimciler varsayılan olarak `Genel nesneler yarat` kullanıcı erişimine sahiptir; bu nedenle, bir yöneticiyseniz, kullanıcı haklarınızı değiştirmeden uzaktan bağlandığında kuyruk yöneticilerini yaratabilir ve başlatabilirsiniz.

Uçbirim Hizmetlerini ya da Uzak Masaüstü Bağlantısını kullanarak bir Windows makinesine bağlanıyorsanız ve bir kuyruk yöneticisini yaratma, başlatma ya da silme sorunları varsa, bu durum `Genel nesneler yarat`kullanıcı erişimine sahip olmadığınız için olabilir.

`Genel nesneler yarat` kullanıcı erişimi, genel ad alanında nesne yaratma yetkisine sahip olan kullanıcıları sınırlar. Bir uygulamanın genel nesne yaratması için, bu uygulamanın genel ad alanında çalıştırılması ya da uygulamanın çalışmakta olduğu kullanıcının, bu nesneye uygulanan `Genel nesneler yarat` kullanıcı erişimi olması gerekir.

Uçbirim Hizmetlerini ya da Uzak Masaüstü Bağlantısını kullanarak bir Windows makinesine uzaktan bağlandığında, uygulamalar kendi yerel ad alanında çalışır. IBM MQ Explorer ya da **crtmqm** komutunu ya da **dltmqm** komutunu kullanarak bir kuyruk yöneticisi yaratma ya da silme girişiminde bulunursanız ya da **strmqm** komutunu kullanarak bir kuyruk yöneticisi başlatmak için yetki başarısızlığı başarısızlıkla sonuçlanır. Bu, Bağlantı Denetimi Tanıtıcısı XY132002olan bir IBM MQ FDC değeri oluşturur.

Starting a queue manager using the IBM MQ Explorer, or using the **amqmdain qmgr start** command works correctly because these commands do not directly start the queue manager. Bunun yerine komutlar, kuyruk yöneticisini genel ad alanında çalışan ayrı bir sürece başlatmak için istek gönderir.

Uçbirim hizmetlerini kullanırken IBM MQ ' un çeşitli yöntemleri işe yaramazsa, `Genel nesneler yarat` öğesini doğru olarak ayarlamayı deneyin.

Yordam

1. Denetim Araçları panosunu açın:

   Windows Server 2008 ve Windows Server 2012
   Bu panoya **Control Panel** > **System and Maintenance** > **Administrative Tools**(Denetim Masası-Sistem ve Bakım-> Yönetim Araçları)

   Windows 8.1
   Bu panoya **Administrative Tools** > **Computer Management**(Yönetim Araçları-Bilgisayar Yönetimi)
2. **Yerel Güvenlik İlkesi**' ne çift tıklatın.
3. **Yerel İlkeler**nesnesini açın.
4. **Kullanıcı Hakları Ataması**seçeneğini tıklatın.
5. Yeni kullanıcıyı ya da grubu `Genel nesneler yarat` ilkesine ekleyin.

Windows *Windows' da SSPI kanal çıkış programı*

IBM MQ for Windows , hem iletisinde hem de MQI kanallarında kullanılabilen bir güvenlik çıkış programı sağlar. Çıkış, kaynak ve nesne kodu olarak sağlanır ve tek yönlü ve iki yönlü kimlik doğrulaması sağlar.

Güvenlik çıkışı, Windows platformlarının tümleşik güvenlik olanaklarını sağlayan Security Support Provider Interface (SSPI) olanağını kullanır.

Güvenlik çıkışı, aşağıdaki tanımlama ve kimlik doğrulama hizmetlerini sağlar:

Bir şekilde kimlik doğrulaması
Bu, Windows NT LAN Manager (NTLM) kimlik doğrulama desteğini kullanır. NTLM, sunucuların istemcilerinin kimliklerini doğrulamasına olanak sağlar İstemcinin, başka bir sunucuyu doğrulamak için bir sunucuyu ya da bir sunucuyu doğrulamasına izin vermez. NTLM, sunucuların orijinal olduğu varsayıldığı bir ağ ortamı için tasarlanmıştır. NTLM, IBM WebSphere MQ 7.0tarafından desteklenen tüm Windows platformlarında desteklenmektedir.

Bu hizmet genellikle bir MQI kanalında, sunucu kuyruk yöneticisinin bir IBM MQ MQI client uygulamasını doğrulamasına olanak sağlamak için kullanılır. Bir istemci uygulaması, çalışmakta olan süreçle ilişkilendirilmiş kullanıcı kimliğiyle tanımlanır.

Kimlik doğrulamayı gerçekleştirmek için, bir kanalın sonundaki güvenlik çıkışı, NTLM ' den bir kimlik doğrulama belirteci edinir ve bir güvenlik iletisinde simgeyi, kanalın diğer ucundaki ortağına gönderir. İş ortağı güvenlik çıkışı, simgenin otantik olduğunu denetleyen simgeyi NTLM ' ye iletir. İş ortağı güvenlik çıkışı, simgenin gerçekliğinden memnun kalmazsa, MCA ' yı kanalı kapatmasını bildirir.

İki yönlü ya da karşılıklı kimlik doğrulama
Bu, Kerberos kimlik doğrulama hizmetlerini kullanır. Kerberos protokolü, bir ağ ortamındaki sunucuların gerçek olduğunu varsaymaz. Sunucular, istemcilerin ve diğer sunucuların kimliklerini doğrulayabilir ve istemciler, sunucuların kimliklerini doğrulayabilir. Kerberos , IBM WebSphere MQ 7.0tarafından desteklenen tüm Windows platformlarında desteklenir.

Bu hizmet hem ileti, hem de MQI kanallarında kullanılabilir. Bir ileti kanalında, iki kuyruk yöneticisi için karşılıklı kimlik doğrulaması sağlar. Bir MQI kanalında, sunucu kuyruk yöneticisi ve IBM MQ MQI client uygulamasının birbirinin kimliğini doğrulamasına olanak sağlar. A queue manager is identified by its name prefixed by the string `ibmMQSeries/`. Bir istemci uygulaması, çalışmakta olan süreçle ilişkilendirilmiş kullanıcı kimliğiyle tanımlanır.

Karşılıklı kimlik doğrulamayı gerçekleştirmek için, başlangıç güvenlik çıkışı, Kerberos güvenlik sunucusundan bir kimlik doğrulama belirteci edinir ve bir güvenlik iletisinde simgeyi iş ortağına gönderir. İş ortağı güvenlik çıkışı, simgeyi Kerberos Server sunucusuna iletir ve bu, özgün olduğunu denetler. Kerberos güvenlik sunucusu, iş ortağının başlatma güvenliği çıkışa bir güvenlik iletisinde gönderdiği ikinci bir belirteç oluşturur. Daha sonra, başlangıç güvenlik çıkışıysa, ikinci simgenin özgün olup olmadığını Kerberos Server 'dan denettir. Bu değiş tokuş sırasında, güvenlik çıkışı, diğerinin gönderdiği simgenin özgünlüğüyle karşılanmazsa, MCA ' yı kanalı kapatmasını bildirir.

Güvenlik çıkışı hem kaynak, hem de nesne biçiminde sağlanır. Kaynak kodu, kendi kanal çıkış programlarınızı yazmak için bir başlangıç noktası olarak kullanabilir ya da nesne modülünü sağlanan şekilde kullanabilirsiniz. Nesne modülünün iki giriş noktası vardır; biri NTLM kimlik doğrulama desteği kullanılarak bir kimlik doğrulaması, diğeri ise Kerberos kimlik doğrulama hizmetleri kullanılarak iki yönlü kimlik doğrulaması içindir.

SSPI kanal çıkış programının nasıl çalıştığından ve nasıl uygulamaya ilişkin yönergeler için Windows sistemlerinde SSPI güvenlik çıkışısının kullanılmasıbaşlıklı konuya ilişkin bilgi için.

Windows *Applying security template files on Windows*

Bir şablonun uygulanması, IBM MQ dosyalarına ve dizinlerine uygulanan güvenlik ayarlarını etkileyebilir. Yüksek düzeyde güvenli şablonu kullanıyorsanız, IBM MQkuruluşundan önce bu şablonu uygulayın.

Windows , Security Configuration and Analysis MMC snap-in ile bir ya da daha çok bilgisayara tek tip güvenlik ayarları uygulamak için kullanabileceğiniz metin tabanlı güvenlik şablonu dosyalarını destekler. Windows , belirli güvenlik düzeylerinin sağlanması amacıyla bir dizi güvenlik ayarı içeren çeşitli şablonlar sağlar. Bu şablonlar şunlardır: Uyumlu, Güvenli ve Yüksek Güvenli.

Bu şablonlardan birinin uygulanması, IBM MQ dosyalarına ve dizinlerine uygulanan güvenlik ayarlarını etkileyebilir. If you want to use the Highly Secure template, configure your machine before you install IBM MQ.

Yüksek düzeyde güvenli şablonu, IBM MQ ' in önceden kurulu olduğu bir makineye uygulıyorsanız, IBM MQ dosyaları ve dizinlerinde ayarladığınız tüm izinler kaldırılır. Bu izinler kaldırıldığı için, *Yönetici*, *mqm*ve uygun olduğunda *Herkes* grup erişimini hata dizinlerinden kaybedersiniz.

Windows *Configuring extra authority for Windows applications connecting to IBM MQ*

Uygulama süreçlerine erişim izni verilebilmesi için, IBM MQ işlemlerinin çalıştırıldığı hesabın ek yetkilendirmeye gereksinim duyabilir.

Bu görev hakkında

You might experience problems if you have Windows applications, for example ASP pages, connecting to IBM MQ that are configured to run at a security level higher than usual.

IBM MQ , belirli eylemleri koordine etmek için uygulama süreçlerine erişim için SENKRONIZE erişimi gerektirir. Bir sunucu uygulaması ilk kez bir kuyruk yöneticisine bağlanmayı denediğinde, IBM MQ , IBM MQ yöneticileri için SENKRONIZE yetkisi verme işlemini değiştirir. However, the account under which IBM MQ processes run might need additional authorization before the requested access can be granted.

IBM MQ işlemlerinin çalıştırıldığı kullanıcı kimliği için ek yetki yapılandırmak için aşağıdaki adımları tamamlayın:

Yordam

1. Yerel Güvenlik İlkesi aracını başlatın, **Güvenlik Ayarları**->**Yerel İlkeler**->**Kullanıcı Sağ Atamaları**seçeneklerini, **Hata Ayıklama Programları**seçeneğini tıklatın.
2. **Hata Ayıklama Programları**seçeneğini çift tıklatın ve daha sonra, IBM MQ kullanıcı kimliğinizi listeye ekleyin

   Sistem bir Windows etki alanıysa ve etkin ilke ayarı hala belirlenmezse, yerel ilke ayarı ayarlansa da, etki alanı güvenlik ilkesi aracı kullanılarak, kullanıcı kimliğinin etki alanı düzeyinde aynı şekilde yetkilendirilmesi gerekir.

IBM i IBM iüzerinde güvenliğin ayarlanması

SecuritySecurity on IBM i , IBM MQ Object Authority Manager (OAM) ve IBM i nesne düzeyinde güvenlik kullanılarak gerçekleştirilir.

IBM MQ nesnelerine erişim yetkisi belirlenirken yapılması gereken güvenlik noktaları.

Kurumunuzdaki kullanıcılara yetki verdiğinizde, aşağıdaki noktaları göz önünde bulundurmanız gerekir:

1. IBM i GRTOBJAUT ve RVKOBJAUT komutlarını kullanarak IBM MQ for IBM i komutlarına yetki verin ve yetkiyi iptal edin.

   In the QMQM library, certain noncommand (*cmd) objects are set to have ***PUBLIC** authority to ***USE**. Bu nesnelerin yetkilerini değiştirmeyin ya da yetki sağlamak için bir yetki listesi kullanın. Herhangi bir yanlış yetki, IBM MQ işlevselliğini tehlikeye atabilir.
2. IBM MQ for IBM ikuruluşu sırasında, aşağıdaki özel kullanıcı tanıtımları yaratılır:

   QMQM
   Birincil olarak yalnızca iç ürün işlevleri için kullanılır. Ancak, MQCNO_FASTPATH_BINBAĞ tanımlarını kullanarak güvenilir uygulamaları çalıştırmak için kullanılabilir. MQCONNX çağrısını kullanarak kuyruk yöneticisine bağlanmabaşlıklı konuya bakın.

   QMQMADM
   IBM MQyöneticileri için bir grup profili olarak kullanılır. Grup tanıtımı, CL komutlarına ve IBM MQ kaynaklarına erişim sağlar.

   SBMJOB ' i kullanarak IBM MQ komutları çağrısı yapan programları sunmak için, USER, QMQMADM için belirtik olarak ayarlanmamalıdır. Bunun yerine, USER 'i QMQM' ye ya da grup olarak belirlenen QMQMADM ' a sahip başka bir kullanıcı tanıtımını ayarlayın.
3. Uzak kuyruk yöneticilerine kanal komutları gönderiyorsanız, kullanıcı tanıtımınızın hedef sistemde QMQMADM grubunun bir üyesi olduğundan emin olun. PCF ve MQSC kanal komutlarının bir listesi için bkz. IBM MQ for IBM i CL komutları.
4. Bir kullanıcıyla ilişkilendirilmiş grup kümesi, grup yetkileri OAM tarafından hesaplandığında önbelleğe alınır.

   Kullanıcı grubu üyeliklerinde, grup kümesi önbelleğe alındıktan sonra yapılan değişiklikler, kuyruk yöneticisini yeniden başlatılıncaya kadar tanınmaz ya da güvenliği yenilemek için RFRMQMAUT komutunu yürütemez.
5. Özellikle hassas komutlarla çalışma yetkisi olan kullanıcıların sayısını sınırlayın. Bu komutlar şunlardır:
   - İleti Kuyruğu Yöneticisi Yarat (CRTMQM)
   - İleti Kuyruğu Yöneticisini Sil (DLTMQM)

- İleti Kuyruğu Yöneticisi 'ni Başlat (STRMQM)
- İleti Kuyruğu Yöneticisi 'ni sona erdir (ENDMQM)
- Komut Sunucusunu Başlat (STRMQMCSVR)
- Komut Sunucusu Sona erdir (ENDMQMCSVR)

6. Kanal tanımları bir güvenlik çıkış programı belirtimi içerir. Kanal oluşturma ve değiştirme özel konuları gerektirir. Güvenlik çıkışlarına ilişkin ayrıntılar “Güvenlik çıkışa genel bakış” sayfa 100içinde verilmiştir.
7. Kanal çıkışı ve tetikleme izleme programları yerine koyulabilir. Bu tür değiştirmenin güvenliği programcının sorumluluğunda.

IBM i IBM iüzerinde nesne yetkisi yöneticisi

Nesne yetkilisi yöneticisi (OAM), kullanıcıların, kuyruklar ve süreç tanımlamaları da içinde olmak üzere IBM MQ nesnelerini işlemek için yetkilendirilmelerini yönetir. Ayrıca, belirli bir kullanıcı grubuna ilişkin bir nesneye erişim yetkisi verebileceğiniz ya da bu nesneye erişim yetkisini iptal edebildiğiniz bir komut arabirimi de sağlar. Bir kaynağa erişilmesine izin verme kararı OAM tarafından yapılır ve kuyruk yöneticisi bu kararı izler. OAM bir karar veremiyorsa, kuyruk yöneticisi o kaynağa erişimi engeller.

OAM boyunca kontrol edebilirsin.

- MQI aracılığıyla IBM MQ nesnelerine erişim. Bir uygulama programı bir nesneye erişmeyi denediğinde OAM, isteği yapan kullanıcı tanıtımının istenen işleme ilişkin yetkiye sahip olup olmadığını denetler.

  Bu, özellikle kuyruklar ve kuyruklar üzerindeki iletilerin yetkisiz erişimden korunabileceği anlamına gelir.
- PCF ve MQSC komutlarını kullanma izni.

Farklı kullanıcı gruplarının aynı nesne için farklı erişim yetkileri olabilir. Örneğin, belirli bir kuyruk için, bir grup hem put, hem de alma işlemleri gerçekleştirebilir; başka bir gruba yalnızca kuyruğa göz atma izni verilebilir (Göz atma seçeneğiyle MQGET). Benzer şekilde, bazı gruplar bir kuyruğa alma ve kuyruğa alma yetkisine sahip olabilir, ancak kuyruğun değiştirilmesine ya da silinmesine izin verilmeyebilir.

IBM MQ for IBM i commands and perform operations on IBM MQ for IBM i objects

IBM i IBM iüzerindekiIBM MQ yetkiler

IBM MQ nesnelerine erişmek için, komutu verme ve gönderme yapılan nesneye erişme yetkisine sahip olun. Yöneticilerin tüm IBM MQ kaynaklarına erişimi vardır.

IBM MQ nesnelerine erişim, yetkililer tarafından aşağıdaki nesnelere erişim denetiminden geçilir:

1. IBM MQ komutunu verin.
2. Komut tarafından gönderme yapılan IBM MQ nesnelerine erişim

Tüm IBM MQ for IBM i CL komutları QMQM ' nin sahibi ile birlikte gönderilir ve denetim tanıtımının (QMQMADM) *USE haklarıyla *EXCLUDE değeri *EXCLUDE değerine ayarlanmış olmalıdır.

Not: The QSRDUPER program is used by the IBM MQ for IBM i licensed program installer to duplicate Command (*CMD) objects in QSYS. IBM i V5R4 ve sonraki yayın düzeylerinde, QSRDUPER programı, varsayılan davranışın özgün komutun yinelemesi yerine bir yetkili sunucu komutu yaratması için değiştirildi. Bir yetkili komut, komutu yürütmeyi başka bir komutla yeniden yönlendirir ve PRX özniteliğine sahiptir. Kopyalanmakta olan komutla aynı ada sahip bir yetkili sunucu QSYS kitaplığında varsa, yetkili sunucu komutuna ilişkin özel yetkiler ürün kitaplığındaki komuta verilemez. QSYS ' de proxy komutunu uygulama ya da çalıştırma girişimleri, ürün kitaplığındaki hedef komutun yetkisini denetler. Bu nedenle, *CMD nesnelerine ilişkin yetkilerde yapılacak değişikliklerin, ürün kitaplığında (QMQM) yapılması ve QSYS ' de yapılması gerekenlerin değiştirilmesi gerekmez. Örneğin:

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

Ürünün CL komutlarından bazılarının yetki yapısında yapılan değişiklikler, bu değişiklikleri yapmak üzere IBM MQ nesnelerine gerekli OAM yetkinizin olması durumunda bu komutların genel kullanımına olanak tanır.

IBM iüzerinde IBM MQ yöneticisi olmak için, *QMQMADM grubu*üyesi olmanız gerekir. Bu grubun özellikleri, UNIX, Linux ve Windows sistemlerinde mqm grubunun özellikleri gibi özellikleri içerir. Özellikle, QMQMADM grubu, IBM MQ for IBM i' u kurduğunuzda yaratılır ve QMQMADM grubunun üyeleri sistemdeki tüm IBM MQ kaynaklarına erişir. Ayrıca, *ALLOBJ yetkiniz varsa tüm IBM MQ kaynaklarına da erişiminiz vardır.

Yöneticiler, IBM MQ' u yönetmek için CL komutlarını kullanabilirler. Bu komutlardan biri, diğer kullanıcılara yetki vermek için kullanılan GRTMQMAUT komutlarından biridir. STRMQMQSC başka bir komut, bir denetimcinin yerel bir kuyruk yöneticisine MQSC komutları yayınlamasını sağlar.

İlgili kavramlar

"IBM iüzerinde IBM MQ yönetimi yetkisi" sayfa 81

IBM i *IBM iüzerindeki IBM MQ nesnelerine erişim yetkileri*

Access authorities required for running IBM MQ CL commands.

IBM MQ for IBM i , ürünün CL komutlarını iki grup halinde kategorilere ayırır:

Grup 1

Bu komutları işlemek için, kullanıcıların QMQMADM kullanıcı grubuna ya da *ALLOBJ yetkisine sahip olması gerekir. Bu yetkilerden herhangi birine sahip olan kullanıcılar, herhangi bir ek yetki gerektirmeden tüm kategorilerdeki tüm komutları işleyebilirler.

Not: Bu yetkiler OAM yetkisini geçersiz kılar.

Bu komutlar aşağıdaki gibi gruplandırılabilir:

- Komut Sunucusu Komutları
  - ENDMQMCSVR, Son IBM MQ Komut Sunucusu
  - STRMQMCSVR, IBM MQ Command Server 'ı Başlat
- Dead-Letter Kuyruk İşleyici Komutu
  - STRMQMDLQ, IBM MQ Dead-Letter Queue Handler 'ı Başlat
- Dinleyici Komutu
  - ENDMQMLSR, Son IBM MQ dinleyicisi
  - STRMQMLSR, Nesne olmayan dinleyiciyi başlat
- Ortam Kurtarma Komutları
  - RCDMQMIMG, Kayıt IBM MQ Nesne Görüntüsü
  - RCRMQMOBJ, IBM MQ Nesnesinin Yeniden Yarat
  - WRKMQMTRN, IBM MQ Q Transactions ile çalışma
- Kuyruk Yöneticisi Komutları
  - CRTMQM, İleti Kuyruğu Yöneticisi Yarat
  - DLTMQM, İleti Kuyruk Yöneticisini Sil
  - ENDMQM, İleti Kuyruğu Yöneticisi Sonu
  - STRMQM, İleti Kuyruğu Yöneticisi 'nin Başlatılması
- Güvenlik Komutları
  - GRTMQMAUT, Ver IBM MQ Nesne Yetkisi
  - RVKMQMAUT, IBM MQ Nesne Yetkiyi İptal Et
- İzleme Komutu
  - TRCMQM, İzleme IBM MQ İşi

- Hareket Komutları
  - RSVMQMTRN, Resolve IBM MQ Transaction
- Tetikleyici İzleme Komutları
  - STRMQMTRM, Tetikleyici İzleyiciyi Başlat
- IBM MQSC Komutları
  - RUNMQSC, Run IBM MQSC Commands
  - STRMQMMQSC, Start IBM MQSC Commands

Grup 2

İki yetki düzeyinin gerekli olduğu geri kalan komutlar şunlardır:

1. Komutu çalıştırabilmek içinIBM i yetkisi. Bir IBM MQ yöneticisi, bir kullanıcı ya da kullanıcı grubu için *PUBLIC (*EXCLUDE) kısıtlamasını geçersiz kılmak için **GRTOBJAUT** komutunu kullanarak bunu ayarlar.

   Örneğin:

   ```
   GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
   ```

2. Adım 1 'de doğru IBM i yetkisi verilmiş olan, komutla ya da komutlarla ilişkili IBM MQ nesnelerini işlemek içinIBM MQ yetkisi.

   Bu yetki, **GRTMQMAUT** komutunu kullanarak bir IBM MQ yöneticisi tarafından ayarlanan gerekli işlem için uygun OAM yetkisine sahip kullanıcı tarafından denetlenir.

   Örneğin:

   ```
   GRTMQMAUT *connect authority to the queue manager + *admchg authority to
           the queue
   ```

Komutlar aşağıdaki gibi gruplanabilir:

- Kanal Komutları
  - CHGMQMCHL, Change IBM MQ Channel

    Bu, kuyruk yöneticisi için * bağlanma yetkisi ve kanala * admchg yetkisi gerektirir.
  - CPYMQMCHL, IBM MQ Kanalını Kopyala

    Bu, kuyruk yöneticisi için * connect ve * admcrt yetkinizin, kopyalanacak varsayılan kanal tipine * admdsp yetkisi ve kanal nesnesi sınıfı için * admcrt yetkisi gerektirir.

    Örneğin, bir gönderen kanalını kopyalamak için, SYSTEM.DEF.SENDER kanalı için * admdsp yetkisine gerek vardır.
  - CRTMQMCHL, IBM MQ Kanalı Oluştur

    Bu, kuyruk yöneticisi için * connect ve * admcrt yetkisini, yaratılacak varsayılan kanal tipine * admdsp yetkisi ve kanal nesnesi sınıfı için * admcrt yetkisine sahip olmalıdır.

    Örneğin, bir gönderen kanalı yaratmak için, SYSTEM.DEF.SENDER kanalı
  - DLTMQMCHL, Delete IBM MQ Channel

    Bu, kanal için kuyruk yöneticisi ve * admdlt yetkisi için * bağlantı yetkisini gerektirir.
  - RSVMQMCHL, Resolve IBM MQ Channel

    Bu, kuyruk yöneticisi için * bağlanma yetkisi ve kanal için * ctrlx yetkisi gerektirir.
- Görüntüleme komutları

  DSP komutlarını işlemek için, kullanıcı `*connect` ve `*admdsp` yetkisini, listelenen belirli bir seçenekle birlikte kuyruk yöneticisine vermeniz gerekir:

- DSPMQM, İleti Kuyruk Yöneticisini Görüntüle
- DSPMQMAUT, IBM MQ Nesne Yetkisini Görüntüle
- DSPMQMAUTI, Display IBM MQ Authentication Information - `*admdsp` to the authentication information object
- DSPMQMCHL, Display IBM MQ Channel - `*admdsp` to the channel
- DSPMQMCSVR, Display IBM MQ Command Server
- DSPMQMNL, Display IBM MQ Namelist - `*admdsp` to the namelist
- DSPMQMOBJN, IBM MQ Nesne Adlarını Görüntüle
- DSPMQMPRC, Display IBM MQ Process - `*admdsp` to the process
- DSPMQMQ, IBM MQ kuyruğunu görüntüle- `*admdsp` kuyrukta
- DSPMQMTOP, Display IBM MQ Topic - `*admdsp` to the topic

- Komutlarla çalış

  WRK komutlarını işlemek ve seçenekler panosunu görüntülemek için, kullanıcı `*connect` ve `*admdsp` yetkisini kuyruk yöneticisine vermeniz ve listelenen belirli bir seçenekle birlikte, aşağıdaki işlemleri gerçekleştirmelisiniz:

  - WRKMQM, İleti Kuyruğu Yöneticileriyle Çalışma
  - WRKMQMAUT, IBM MQ Object Authority ile çalış
  - WRKMQMAUTD, IBM MQ Object Authority Data ile çalış
  - WRKMQMAUTI, IBM MQ Kimlik Doğrulama Bilgileri ile Çalışma
    - `*admchg` for the Change IBM MQ Authentication Information Object command.
    - `*admcrt` for the Create and Copy IBM MQ Authentication Information Object command.
    - `*admdlt` for the Delete IBM MQ Authentication Information Object command.
    - `*admdsp` for the Display IBM MQ Authentication Information Object command.
  - WRKMQMCHL, IBM MQ Kanal ile çalış

    Bu, aşağıdaki yetkilerin kullanılmasını gerektirir:

    - `*admchg` for the Change IBM MQ Channel command.
    - Clear IBM MQ Channel komutu için`*admclr` .
    - `*admcrt` for the Create and Copy IBM MQ Channel command.
    - `*admdlt` for the Delete IBM MQ Channel command.
    - Görüntü IBM MQ Kanal komutu için`*admdsp` .
    - `*ctrl` for the Start IBM MQ Channel command.
    - Uç IBM MQ Kanal komutu için`*ctrl` .
    - Ping IBM MQ Kanal komutu için`*ctrl` .
    - `*ctrlx` for the Reset IBM MQ Channel command.
    - `*ctrlx` for the Resolve IBM MQ Channel command.
  - WRKMQMCHST, IBM MQ Kanal Durumuyla Çalışma

    Bu, kanala `*admdsp` yetkisi gerektirir.
  - WRKMQMCL, IBM MQ Kümeleriyle Çalışma
  - WRKMQMCLQ, IBM MQ Küme Kuyruklarıyla Çalışma
  - WRKMQMCLQM, IBM MQ Küme Kuyruk Yöneticisiyle Çalışma
  - WRKMQMLSR, IBM MQ Listener ile çalışın
  - WRKMQMMSG, IBM MQ iletileriyle çalış

    Bu, kuyruk için `*browse` yetkisi gerektirir.

- WRKMQMNL, IBM MQ Ad listeleriyle çalış

  Bu, aşağıdaki yetkilerin kullanılmasını gerektirir:

  - *admchg for the Change IBM MQ Namelist command.
  - Yarat ve Kopyala IBM MQ Ad listesi komutu için*admcrt .
  - *admdlt for the Delete IBM MQ Namelist command.
  - Görüntüle IBM MQ Ad listesi komutu için*admdsp .
- WRKMQMPRC, IBM MQ Süreçleriyle Çalışma

  Bu, aşağıdaki yetkilerin kullanılmasını gerektirir:

  - *admchg for the Change IBM MQ Process command.
  - Create(Create and Copy ve Copy IBM MQ Process) komutu için*admcrt .
  - *admdlt for the Delete IBM MQ Process command.
  - Display(Display IBM MQ Process) komutu için*admdsp .
- WRKMQMQ, IBM MQ kuyruklarıyla çalış

  Bu, aşağıdaki yetkilerin kullanılmasını gerektirir:

  - ChangeKuyruğu (Change IBM MQ Queue) komutu için*admchg .
  - Clear IBM MQ Queue komutu için*admclr .
  - Create and Copy IBM MQ Queue komutu için*admcrt .
  - *admdlt for the Delete IBM MQ Queue command.
  - Görüntüleme IBM MQ Kuyruk komutu için*admdsp .
- WRKMQMQSTS, IBM MQ kuyruk durumuyla çalış
- WRKMQMTOP, IBM MQ Konularıyla Çalışma

  Bu, aşağıdaki yetkilerin kullanılmasını gerektirir

  - *admchg for the Change IBM MQ Topic command.
  - Create, Create and Copy IBM MQ Topic komutu için*admcrt .
  - *admdlt for the Delete IBM MQ Topic command.
  - *admdsp for the Display IBM MQ Topic command.
- WRKMQMSUB, IBM MQ abonelikleriyle çalış

- Diğer Kanal komutları

  Kanal komutlarını işlemek için kullanıcıya belirli yetkilerin listelenmesini vermeniz gerekir:

  - ENDMQMCHL, Son IBM MQ Kanalı

    Bu, kuyruk yöneticisi için *connect yetkisi ve kanalla ilişkili iletim kuyruğu için *allmqi yetkisi gerektirir.
  - ENDMQMLSR, Son IBM MQ Dinleyicisi

    Bu, kuyruk yöneticisi için *connect yetkisi ve adlandırılmış dinleyici nesnesi için *ctrl yetkisi gerektirir.
  - PNGMQMCHL, Ping IBM MQ Kanalı

    Bu, kuyruk yöneticisi için *connect ve *inq yetkisi ve kanal nesnesi için *ctrl yetkisi gerektirir.
  - RSTMQMCHL, IBM MQ Kanalını İlk Durumuna Getir

    Bu, kuyruk yöneticisine *connect yetkisi gerektirir.
  - STRMQMCHL, IBM MQ Kanalını Başlat

    Bu, kuyruk yöneticisine *connect yetkisi ve kanal nesnesi için *ctrl yetkisi gerektirir.
  - STRMQMCHLI, Start IBM MQ Channel Initiator

Bu, kuyruk yöneticisi için *connect ve *inq yetkisini ve kanalın iletim kuyruğuyla ilişkili başlatma kuyruğuna *allmqi yetkisi gerektirir.

– STRMQMLSR, IBM MQ Listener 'i Başlat

Bu, kuyruk yöneticisi için * bağlanma yetkisi ve adlandırılan dinleyici nesnesi için * ctrl yetkisi gerektirir.

- Diğer komutlar:

Aşağıdaki komutları işlemek için kullanıcıya belirli yetkilerin listelenmesini vermeniz gerekir:

– CCTMQM, İleti Kuyruğu Yöneticisi 'ye Bağlan

Bu, IBM MQ nesne yetkisi gerektirmez.

– CHGMQM, İleti Kuyruk Yöneticisini Değiştir

Bu, kuyruk yöneticisi için *connect ve *admchg yetkisini gerektirir.

– CHGMQMAUTI, Change IBM MQ Authentication Information

Bu, kuyruk yöneticisine *connect yetkisi ve kimlik doğrulama bilgileri nesnesi için *admchg ve *admdsp yetkisi gerektirir.

– CHGMQMNL, Değişiklik IBM MQ Ad listesi

Bu, kuyruk yöneticisi için *connect yetkisi ve ad listesi için *admchg yetkisi gerektirir.

– CHGMQMPRC, Change IBM MQ Process

Bu işlem, kuyruk yöneticisi için *connect yetkisi ve işlem için *admchg yetkisi gerektirir.

– CHGMQMQ, Değişiklik IBM MQ Kuyruğu

Bu, kuyruk yöneticisi ve kuyruk için *admchg yetkisi için *connect yetkisini gerektirir.

– CLRMQMQ, Clear IBM MQ Queue

Bu, kuyruk yöneticisi ve kuyruk için *admclr yetkisi için *connect yetkisini gerektirir.

– CPYMQMAUI, IBM MQ Kimlik Doğrulama Bilgilerini Kopyala

This requires *connect authority to the queue manager and *admdsp authority to the authentication information object and *admcrt authority to the authentication information object class.

– CPYMQMNL, Kopyala IBM MQ Ad Listesi

Bu, kuyruk yöneticisi için *connect ve *admcrt yetkisini gerektirir.

– CPYMQMPRC, IBM MQ İşlemi Kopyala

Bu, kuyruk yöneticisi için *connect ve *admcrt yetkisini gerektirir.

– CPYMQMQ, IBM MQ Kuyruğunu Kopyala

Bu, kuyruk yöneticisi için *connect ve *admcrt yetkisini gerektirir.

– CRTMQMAUTI, IBM MQ Kimlik Doğrulama Bilgileri Oluştur

This requires *connect authority to the queue manager and *admdsp authority to the authentication information object and *admcrt authority to the authentication information object class.

– CRTMQMNL, Create IBM MQ Namelist

Bu, kuyruk yöneticisi için *connect ve *admcrt yetkisi ve varsayılan ad listesi için *admdsp yetkisi gerektirir.

– CRTMQMPRC, IBM MQ İşlemi Oluştur

Bu, kuyruk yöneticisi için *connect ve *admcrt yetkisi ve varsayılan işlem için *admdsp yetkisi gerektirir.

– CRTMQMQ, IBM MQ Kuyruğu Oluştur

Bu, kuyruk yöneticisi için *connect ve *admcrt yetkisi ve varsayılan kuyruk için *admdsp yetkisi gerektirir.

- CVTMQMDTA, IBM MQ Veri Tipi Komutunu Dönüştür

  Bu, IBM MQ nesne yetkisi gerektirmez.

- DLTMQMAUTI, Delete IBM MQ Authentication Information

  Bu, kimlik doğrulama bilgileri nesnesi için kuyruk yöneticisi ve *ctrlx yetkisi için *connect yetkisi gerektirir.

- DLTMQMNL, Silme IBM MQ Ad Listesi

  Bu, kuyruk yöneticisi için *connect yetkisi ve ad listesi için *admdlt yetkisi gerektirir.

- DLTTMQMPRC, IBM MQ Sürecini Sil

  Bu işlem, kuyruk yöneticisi için *connect yetkisi ve işlem için *admdlt yetkisi gerektirir.

- DLTMQMQ, Delete IBM MQ Queue

  Bu, kuyruk yöneticisi ve kuyruk için *admdlt yetkisi için *connect yetkisini gerektirir.

- DSCMQM, İleti Kuyruğu Yöneticisi ile bağlantıyı kes

  Bu, IBM MQ nesne yetkisi gerektirmez.

- RFRMQMAUT, Güvenlik Yenile

  Bu, kuyruk yöneticisine *connect yetkisi gerektirir.

- RFRMQMCL, Kümeyi Yenile

  Bu, kuyruk yöneticisine *connect yetkisi gerektirir.

- RSMMQMCLQM, Küme Kuyruk Yöneticisini Sürdür

  Bu, kuyruk yöneticisine *connect yetkisi gerektirir.

- RSTMQMCL, Küme İlk Durumuna Getir

  Bu, kuyruk yöneticisine *connect yetkisi gerektirir.

- SPDMQMCLQM, Küme Kuyruk Yöneticisini Askıya Al

  Bu, kuyruk yöneticisine *connect yetkisi gerektirir.

IBM i *IBM iüzerindeki erişim yetkileri*

Erişim yetkisi komutlarını anlamak için bu bilgileri kullanın.

GRTMQMAUT ve RVKMQMAUT komutlarında AUT anahtar sözcüğü tarafından tanımlanan yetkiler aşağıdaki gibi kategorilere ayrılabilir:

- MQI çağrılarına ilişkin yetkiler
- Yetkilendirmeyle ilgili yönetim komutları
- Bağlam yetkileri
- MQI çağrılarına, komutlara ya da her ikisine ilişkin genel yetkiler

İzleyen çizelgelerde, MQI çağrıları, bağlam çağrıları, MQSC ve PCF komutları ve soysal işlemler için AUT değiştirgesi kullanılarak farklı yetkiler listelenir.

Çizelge 15. MQI çağrılarına ilişkin yetkiler

AUT	Tanım
*ALTUSR	Başka bir kullanıcının MQOPEN ve MQPUT1 çağrıları için başka bir kullanıcının yetkisinin kullanılmasına izin verin.
*GöZ AT	Bir kuyruktan iletiyi almak için, BROWSE seçeneğiyle bir MQGET çağrısı yayınlayın.

Çizelge 15. MQI çağrılarına ilişkin yetkiler (devamı var)	
AUT	**Tanım**
*CONNECT	Bir MQCONN çağrısı yayınlayarak, uygulamayı belirtilen kuyruk yöneticisine bağlayın.
*GET	Bir MQGET çağrısı yayınlayarak kuyruktan ileti alın.
*INQ	Bir MQINQ çağrısı yayınlayarak, belirli bir kuyrukda sorgu yürütün.
*PUB	MQPUT çağrısını kullanarak bir iletiyi yayınlamak için bir konu açın.
*PUT	Bir MQPUT çağrısı yayınlayarak, iletiyi belirli bir kuyruğa koyun.
*RESUME	MQSUB çağrısı kullanarak bir aboneliği sürdürün.
*SET	Bir MQSET çağrısı yayınlayarak, MQI ' dan bir kuyruktaki öznitelikleri ayarlayın. Birden çok seçenek için bir kuyruk açsanız, kuyruğun her biri için yetkilendirilmiş olmanız gerekir.
*SUB	Bir MQSUB çağrısı kullanarak bir konuya ilişkin aboneliği yaratın, Alter ya da Sürdür.

Çizelge 16. Bağlam çağrılarına ilişkin yetkiler	
AUT	**Tanım**
*PASSALL	Belirtilen kuyruğun tüm bağlamını iletin. Tüm bağlam alanları özgün istekten kopyalanır.
*PASSID	Belirtilen kuyruğun kimlik bağlamını iletin. Kimlik bağlamı, istekle aynı.
*SETALL	Belirtilen kuyruğun tüm bağlamını ayarlar. Bu, özel sistem yardımcı programları tarafından kullanılır.
*SETID	Belirtilen kuyruğun kimlik bağlamını ayarlayın. Bu, özel sistem yardımcı programları tarafından kullanılır.

Çizelge 17. MQSC ve PCF çağrılarına ilişkin yetkiler	
AUT	**Tanım**
*ADMCHG	Belirtilen nesnenin özniteliklerini değiştirin.
*ADMCLR	Belirlenen nesneyi temizleyin (yalnızca PCF Clear object komutu).
*ADMCRT	Belirtilen tipte nesneler yaratın.
*ADMDLT	Belirtilen nesneyi silin.
*ADMDSP	Belirtilen nesneye ilişkin öznitelikleri görüntüler.

Çizelge 18. Soysal işlemlere ilişkin yetkiler	
AUT	**Tanım**
*ALL	Nesne için geçerli olan tüm işlemleri kullanın. `all` authority is equivalent to the union of the authorities `alladm`, `allmqi`, and `system` appropriate to the object type.
*ALLADM	Nesne için geçerli olan tüm yönetim işlemlerini gerçekleştirir.
*ALLMQI	Nesne için geçerli olan tüm MQI çağrılarını kullanın.
*CTRL	Kanalların, dinleyicilerin ve hizmetlerin başlatılması ve kapanması.
*CTRLX	Sıra numarasını ilk durumuna getirin ve belirsiz kanalları çözümleyin.

IBM i *IBM üzerindeki erişim yetkilendirme komutlarının kullanılması*

Erişim yetkilendirme komutları hakkında bilgi edinmek ve komut örneklerini kullanmak için bu bilgileri kullanın.

GRTMQMAUT komutunun kullanılması

Gerekli yetkiniz varsa, bir kullanıcı tanıtımından ya da kullanıcı grubuna belirli bir nesneye erişmesi için yetki vermek üzere GRTMQMAUT komutunu kullanabilirsiniz. Aşağıdaki örneklerde, GRTMQMAUT komutunun nasıl kullanıldığı gösterilmektedir:

1. ```
   GRTMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
             AUT(*BROWSE *PUT) MQMNAME('saturn.queue.manager')
   ```

   Bu örnekte:

   - RED.LOCAL.QUEUE , nesne adıdır.
   - *LCLQ (yerel kuyruk) nesne tipidir.
   - GROUPA , yetkilerin değiştirileceği sistemdeki bir kullanıcı profilinin adıdır. Bu profil, diğer kullanıcılar için bir grup profili olarak kullanılabilir.
   - *BROWSE ve *PUT , belirtilen kuyruğa verilen yetkiler.

     *BROWSE , kuyruktaki iletilere göz atmak için yetki ekler (göz atma seçeneğiyle MQGET komutunu vermek için).

     *PUT , kuyruğa alma (MQPUT) iletileri için yetki ekler.
   - saturn.queue.manager , kuyruk yöneticisi adıdır.
2. Aşağıdaki komut, varsayılan kuyruk yöneticisi için, JAK ve JLL tüm geçerli yetkilendirmeleri tüm süreç tanımlamalarına verir.

   ```
   GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
   ```
3. The following command grants user GEORGE authority to put a message on the queue ORDERS, on the queue manager TRENT.

   ```
   GRTMQMAUT OBJ(TRENT) OBJTYPE(*MQM) USER(GEORGE) AUT(*CONNECT) MQMNAME (TRENT)
   GRTMQMAUT OBJ(ORDERS) OBJTYPE(*Q) USER(GEORGE) AUT(*PUT) MQMNAME (TRENT)
   ```

RVKMQMAUT komutunun kullanılması

Gerekli yetkiniz varsa, belirli bir nesneye erişmek üzere bir kullanıcı tanıtımı ya da kullanıcı grubunun önceden verilmiş yetkisini kaldırmak için RVKMQMAUT komutunu kullanabilirsiniz. Aşağıdaki örneklerde, RVKMQMAUT komutunun nasıl kullanıldığı gösterilmektedir:

1. ```
   RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
   AUT(*PUT) MQMNAME('saturn.queue.manager')
   ```

   Önceki örnekte verildiği belirtilen kuyruğa ileti koyma yetkisi, GROUPAiçin kaldırılır.
2. ```
   RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
   MQMNAME(PAYROLLQM)
   ```

   Authority to get messages from any queue with a name starting with the characters PAY, owned by queue manager PAYROLLQM, is removed from all users of the system unless they, or a group to which they belong, have been separately authorized.
   ```

DSPMQMAUT komutunu kullanma

Görüntülenen MQM yetkisi (DSPMQMAUT) komut, belirtilen nesne ve kullanıcı için, kullanıcının nesne için sahip olduğu yetkilerin listesini gösterir. Aşağıdaki örnek, komutun nasıl kullanıldığını göstermektedir:

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

RFRMQMAUT komutunun kullanılması

MQM güvenliği yenileniyor (RFRMQMAUT) komut, kuyruk yöneticisini durdurma ve yeniden başlatma gerekmeden işletim sistemi düzeyinde yapılan değişiklikleri yansıtarak OAM ' nin yetki grubu bilgilerini hemen güncellemenizi sağlar. Aşağıdaki örnek, komutun nasıl kullanıldığını göstermektedir:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

IBM i IBM iüzerinde yetkilendirme belirtimi tabloları

Belirli API çağrıları ve bu çağrıların belirli seçenekleri, kuyruk nesneleri, süreç nesneleri ve kuyruk yöneticisi nesneleri için hangi yetkilendirmenin gerekli olduğunu belirlemek için bu bilgileri kullanın.

Çizelge 19 sayfa 158 ' ta başlayan yetkilendirme belirtimi tabloları, yetkilerin nasıl çalıştığını ve uygulanan kısıtlamaların nasıl olduğunu tanımlar. Tablolar bu durumlara uygulanır:

- MQI çağrılarını veren uygulamalar
- Çıkış PCF ' leri olarak MQSC komutlarını veren denetim programları
- PCF komutlarını veren denetim programları

Bu bölümde, bilgiler aşağıdaki verileri belirten bir çizelge kümesi olarak sunulur:

Gerçekleştirilecek işlem
MQI seçeneği, MQSC komutu ya da PCF komutu.

Erişim denetimi nesnesi
Kuyruk, süreç tanımlaması, kuyruk yöneticisi, ad listesi, kanal, istemci bağlantı kanalı, dinleyici, hizmet ya da kimlik doğrulama bilgileri nesnesi.

Yetki gerekiyor
MQZAO_ sabiti olarak ifade edilir.

Çizelgelerde, MQZAO_ öneki olan değişmezler, belirli bir varlık için **GRTMQMAUT** ve **RVKMQMAUT** komutlarına ilişkin yetki listesindeki anahtar sözcüklere karşılık gelir. Örneğin, MQZAO_BROWSE, *Browse anahtar sözcüğünün karşılığıdır; Benzer şekilde, MQZAO_SET_ALL_CONTEXT anahtar sözcüğü *SETALLanahtar sözcüğünün karşılığıdır ve bu şekilde devam eder. Bu sabitler, ürünle birlikte sağlanan cmqzc.hüstbilgi dosyasında tanımlanır.

MQI yetkileri

Bir uygulamanın, belirli bir MQI çağrılarını ve seçeneklerini yalnızca, çalıştığı kullanıcı kimliği (ya da yetkileri varsayabilecek) ilgili yetkiye sahip olması durumunda yayınlanabilir.

Dört adet MQI çağrısı yetkilendirme denetimi gerektirir: MQCONN, MQOPEN, MQPUT1, ve MQCLOSE.

MQOPER ve MQPUT1için yetki denetimi, açılmakta olan nesnenin adı ya da ad ya da ad değil, bir ad çözüldükten sonra ortaya çıkar. Örneğin, bir uygulamanın, diğer adın çözümleyeceği temel kuyruğu açma yetkisi olmadan bir diğer ad kuyruğunu açma yetkisi verilebilir. Kural, kuyruk yöneticisi diğer adı doğrudan açılmadıkça, kuyruk yöneticisi diğer adı olmayan ad çözme işlemi sırasında saptanan ilk tanımlamada gerçekleştirilir; yani, nesnenin adı nesne tanımlayıcısının *ObjectName* alanında gösterilir. Açılmakta olan nesne için her zaman yetki gereklidir; bazı durumlarda kuyruk yöneticisi nesnesine ilişkin bir yetki yoluyla elde edilen ek kuyrukta bağımsız yetki gereklidir.

Çizelge 19 sayfa 158, Çizelge 20 sayfa 158, Çizelge 21 sayfa 159ve Çizelge 22 sayfa 159 , her çağrı için gereken yetkileri özetlemektedir.

Not: Bu tablolarda ad listeleri, kanallar, istemci bağlantısı kanalları, dinleyiciler, hizmetler ya da kimlik doğrulama bilgileri nesneleri belirtilmez. Bunun nedeni, aynı yetkilerin diğer nesneler için geçerli olduğu MQOO_SORGULAMAK dışında, bu nesnelerle ilgili yetkilerin hiçbirinin uygulanmadığı içindir.

Çizelge 19. MQCONN çağrıları için güvenlik yetkisi gerekli

Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 159)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQCONN seçeneği	Burada geçerli değil	Burada geçerli değil	MQZAO_CONNECT

Çizelge 20. MQOPEN çağrıları için güvenlik yetkisi gerekli

Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 159)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQOO_SORGULAMA	MQZAO_SORGULA **("2" sayfa 159)**	MQZAO_SORGULA **("2" sayfa 159)**	MQZAO_SORGULA **("2" sayfa 159)**
MQOO_BROWSE	MQZAO_GÖZAT	Burada geçerli değil	Denetim yok
MQOO_INPUT_ *	MQZAO_INPUT	Burada geçerli değil	Denetim yok
MQOO_SAVE_ ALL_CONTEXT **("3" sayfa 159)**	MQZAO_INPUT	Burada geçerli değil	Burada geçerli değil
MQOO_OUTPUT (Olağan kuyruk) **("4" sayfa 159)**	MQZAO_OUTPUT	Burada geçerli değil	Burada geçerli değil
MQOO_PASPAS_ IDENTITY_CONTEXT **("5" sayfa 159)**	MQZAO_PASPAS_ IDENTITY_CONTEXT	Burada geçerli değil	Denetim yok
MQOO_PASS_ALL_ CONTEXT **("5" sayfa 159, "6" sayfa 159)**	MQZAO_PASS _ALL_CONTEXT	Burada geçerli değil	Denetim yok
MQOO_SET_ IDENTITY_CONTEXT **("5" sayfa 159, "6" sayfa 159)**	MQZAO_SET_ IDENTITY_CONTEXT	Burada geçerli değil	MQZAO_SET_ IDENTITY_CONTEXT **("7" sayfa 159)**
MQOO_SET_ ALL_CONTEXT **("5" sayfa 159, "8" sayfa 159)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("7" sayfa 159)**
MQOO_OUTPUT (İletim kuyruğu) **("9" sayfa 160)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("7" sayfa 159)**
MQOO_SET	MQZAO_SET	Burada geçerli değil	Denetim yok
MQOO_ALTERNATE_ USER_AUTHORITY	**("10" sayfa 160)**	**("10" sayfa 160)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("10" sayfa 160, "11" sayfa 160)**

Çizelge 21. MQPUT1 çağrıları için güvenlik yetkilendirmesi gerekiyor			
Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 159)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQPMO_PASPAS_ IDENTITY_CONTEXT	MQZAO_PASPAS_ IDENTITY_CONTEXT **("12" sayfa 160)**	Burada geçerli değil	Denetim yok
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASPAS_ ALL_CONTEXT **("12" sayfa 160)**	Burada geçerli değil	Denetim yok
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **("12" sayfa 160)**	Burada geçerli değil	MQZAO_SET_ IDENTITY_CONTEXT **("7" sayfa 159)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("12" sayfa 160)**	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("7" sayfa 159)**
(İletim kuyruğu) **("9" sayfa 160)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **("7" sayfa 159)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**("13" sayfa 160)**	Burada geçerli değil	MQZAO_ALTERNATE_ USER_AUTHORITY **("11" sayfa 160)**

Çizelge 22. MQCLOSE çağrıları için güvenlik yetkisi gerekli			
Yetki için gerekli yetki:	**Kuyruk nesnesi ("1" sayfa 159)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQCO_DELETE	MQZAO_DELETE **("14" sayfa 160)**	Burada geçerli değil	Burada geçerli değil
MQCO_DELETE _PURGE	MQZAO_DELETE **("14" sayfa 160)**	Burada geçerli değil	Burada geçerli değil

Tablolara ilişkin notlar:

1. Bir model kuyruğu açılıyorsa:
   - Model kuyruğu için, açtığınız erişim tipine ilişkin model kuyruğunu açma yetkisine ek olarak, model kuyruğu için MQZAO_DISPLAY yetkisi gereklidir.
   - Devingen kuyruk yaratmak için MQZAO_CREATE yetkisi gerekli değil.
   - Model kuyruğunu açmak için kullanılan kullanıcı kimliği, yaratılan dinamik kuyruk için kuyruğa özgü tüm yetkileri (MQZAO_ALL ile eşdeğer) otomatik olarak kabul edilir.
2. Açılmakta olan nesnenin tipine bağlı olarak kuyruk, süreç, ad listesi ya da kuyruk yöneticisi nesnesi denetlenir.
3. MQOO_INPUT_ * da belirtilmelidir. Bu seçenek yerel, model ya da diğer ad kuyruğu için geçerlidir.
4. Bu denetim, "9" sayfa 160notunda belirtilen vaka dışında tüm çıkış senaryoları için gerçekleştirilir.
5. MQOO_OUTPUT da belirtilmeli.
6. MQOO_PASS_IDENTITY_CONTEXT, bu seçenek tarafından da örtük olarak belirtilir.
7. Bu yetki, hem kuyruk yöneticisi nesnesi hem de belirli bir kuyruk için gereklidir.
8. MQOO_PASST_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT ve MQOO_SET_IDENTITY_CONTEXT, bu seçenek tarafından da örtük olarak belirtilir.

9. This check is performed for a local or model queue that has a *Kullanım* queue attribute of MQUS_TRANSMISSION, and is being opened directly for output. Bir uzak kuyruk açılırsa (uzak kuyruk yöneticisinin ve uzak kuyruğun adlarını belirterek ya da uzak kuyruğun yerel tanımlamasının adını belirleyerek) bu değer uygulanmaz.
10. En az bir MQOO_SORGULAMASI (herhangi bir nesne tipi için) ya da (kuyruklar için) MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT ya da MQOO_SET belirtilmelidir. Yapılan denetim, belirtilen diğer seçenekler için, belirtilen nesne yetkisi için sağlanan diğer kullanıcı kimliğini ve MQZAO_ALTERNATE_USER_IDENTIFIER denetim öğesine ilişkin yürürlükteki uygulama yetkisini kullanır.
11. Bu yetki, *AlternateUserTnt* ' in belirtilmesine izin verir.
12. An MQZAO_OUTPUT check is also carried out if the queue does not have a *Kullanım* queue attribute of MQUS_TRANSMISSION.
13. Yapılan denetim, belirtilen kuyruk yetkisi için sağlanan diğer kullanıcı kimliğini ve MQZAO_ALTERNATE_USER_IDENTIFIER denetim öğesine ilişkin yürürlükteki uygulama yetkisini kullanarak, belirtilen diğer seçenekler için geçerli olur.
14. Bu denetim yalnızca, aşağıdaki deyimlerin her ikisi de doğru olduğunda gerçekleştirilir:
    - Kalıcı bir dinamik kuyruk kapatılmakta ve silinmektedir.
    - Kuyruk, kullanılmakta olan nesne tanıtıcı değeri döndüren MQOPER tarafından yaratılmadı.

    Yoksa, kontrol falan yok.

Genel notlar:

1. Özel yetki MQZAO_ALL_MQI, nesne tipiyle ilgili aşağıdaki tüm yetkileri içerir:
    - MQZAO_CONNECT
    - MQZAO_SORGULAMA
    - MQZAO_SET
    - MQZAO_GÖZAT
    - MQZAO_INPUT
    - MQZAO_OUTPUT
    - MQZAO_PASS_IDENTITY_CONTEXT
    - MQZAO_PASS_ALL_CONTEXT
    - MQZAO_SET_IDENTITY_CONTEXT
    - MQZAO_SET_ALL_CONTEXT
    - MQZAO_ALTERNATE_USER_AUTHORITY
2. MQZAO_DELETE (bkz. not “14” sayfa 160) ve MQZAO_DISPLAY denetim yetkileri olarak sınıflandırılır. Bu nedenle MQZAO_ALL_MQI içinde yer almıyorlar.
3. *Denetleme yok* , yetkilendirme denetiminin gerçekleştirilmediği anlamına gelir.
4. *Geçerli değil* , yetki denetiminin bu işlemle ilgili olmadığı anlamına gelir. Örneğin, bir süreç nesnesi için MQPUT çağrısı yayınlayamazsınız.

IBM i *Authorizations for MQSC commands in escape PCFs on IBM i*

Bu yetkiler, bir kullanıcının denetim komutlarını kaçış PCF iletisi olarak yayınlamasına olanak sağlar. Bu yöntemler, bir programın, bir kuyruk yöneticisine ileti olarak bir denetim komutu göndermesini, o kullanıcının adına yürütmesini sağlar.

Bu bölümde, Escape PCF ' de bulunan her MQSC komutu için gereken yetkiler özetlenir.

Geçerli değil , yetki denetiminin bu işlemle ilgili olmadığı anlamına gelir.

Komutu gönderen programın altında çalışmakta olan kullanıcı kimliği, aşağıdaki yetkilerin de geçerli olması gerekir:

- MQZAO_CONNECT yetkisi kuyruk yöneticisi için
- PCF komutlarını gerçekleştirmek için kuyruk yöneticisinde GÖRÜNTÜLEME yetkisi
- Escape PCF komutu metninde MQSC komutlarını verme yetkisi

ALTER *nesnesi*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	MQZAO_CHANGE
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE

CLEAR *nesne*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CLEAR
Konu	MQZAO_CLEAR
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	Burada geçerli değil
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

DEFINE *object* NOREPLACE (“1” sayfa 164)

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CREATE **(“2” sayfa 165)**
Konu	MQZAO_CREATE **(“2” sayfa 165)**
Süreç	MQZAO_CREATE **(“2” sayfa 165)**
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CREATE **(“2” sayfa 165)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(“2” sayfa 165)**
Kanal	MQZAO_CREATE **(“2” sayfa 165)**

Nesne	Yetki gerekiyor
İstemci bağlantı kanalı	MQZAO_CREATE **("2" sayfa 165)**
Dinleyici	MQZAO_CREATE **("2" sayfa 165)**
Hizmet	MQZAO_CREATE **("2" sayfa 165)**

DEFINE *nesne* REPLACE ("1" sayfa 164, "3" sayfa 165)

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE

DELETE *nesnesi*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_DELETE
Konu	MQZAO_DELETE
Süreç	MQZAO_DELETE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_DELETE
Kimlik doğrulama bilgileri	MQZAO_DELETE
Kanal	MQZAO_DELETE
İstemci bağlantı kanalı	MQZAO_DELETE
Dinleyici	MQZAO_DELETE
Hizmet	MQZAO_DELETE

DISPLAY(*nesne*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_GÖRÜNTÜLE
Konu	MQZAO_GÖRÜNTÜLE
Süreç	MQZAO_GÖRÜNTÜLE
Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Ad Listesi	MQZAO_GÖRÜNTÜLE

Nesne	Yetki gerekiyor
Kimlik doğrulama bilgileri	MQZAO_GÖRÜNTÜLE
Kanal	MQZAO_GÖRÜNTÜLE
İstemci bağlantı kanalı	MQZAO_GÖRÜNTÜLE
Dinleyici	
Hizmet	

PING KANALI

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

KANALı

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL_EXTENDED
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

KANALıN

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil

Nesne	Yetki gerekiyor
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL_EXTENDED
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

START *nesne*

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	MQZAO_CONTROL
Hizmet	MQZAO_CONTROL

STOP *nesne*

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	MQZAO_CONTROL
Hizmet	MQZAO_CONTROL

Not:

1. DEFE komutları için, MQZAO_DISPLAY yetkisi de belirtildiyse, LIKE nesnesi için ya da uygun SYSTEM.DEFAULT.xxx nesnesi atlanırsa nesne.

2. MQZAO_CREATE yetkisi belirli bir nesne ya da nesne tipine özgü değil. GRTMQMAUT komutunda QMGR nesne tipi belirtilerek, belirtilen bir kuyruk yöneticisine ilişkin tüm nesneler için yetki yaratma yetkisi verilir.
3. Bu seçenek, değiştirilecek nesne önceden varsa geçerlidir. Bu işlem yoksa, denetim DEFINE *object* NOREPLACE için olur.

IBM i *IBM iüzerinde PCF komutlarına ilişkin yetkiler*

Bu yetkiler, bir kullanıcının, denetim komutlarını PCF komutları olarak yayınlamasına olanak sağlar. Bu yöntemler, bir programın, bir kuyruk yöneticisine ileti olarak bir denetim komutu göndermesini, o kullanıcının adına yürütmesini sağlar.

Bu bölümde, her PCF komutu için gereken yetkiler özetlenmektedir.

Denetleme yok , yetki denetiminin gerçekleştirilmediği anlamına gelir; *Uygulanamaz* , yetki denetiminin bu işlemle ilgili olmadığı anlamına gelir.

Komutu gönderen programın altında çalışmakta olan kullanıcı kimliği, aşağıdaki yetkilerin de geçerli olması gerekir:

- MQZAO_CONNECT yetkisi kuyruk yöneticisi için
- PCF komutlarını gerçekleştirmek için kuyruk yöneticisinde GÖRÜNTÜLEME yetkisi

Özel yetki MQZAO_ALL_ADMIN yetkilendirmesi aşağıdaki yetkileri içerir:

- MQZAO_CHANGE
- MQZAO_CLEAR
- MQZAO_DELETE
- MQZAO_GÖRÜNTÜLE
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED

MQZAO_CREATE, belirli bir nesne ya da nesne tipine özgü olmadığı için içerilmedi

Değişiklik *nesnesi*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	MQZAO_CHANGE
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE

Clear *nesne*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CLEAR
Konu	MQZAO_CLEAR

Nesne	Yetki gerekiyor
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	Burada geçerli değil
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

***nesne* kopyala (değiştirilmeden) (“1” sayfa 170)**

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CREATE **(“2” sayfa 170)**
Konu	MQZAO_CREATE **(“2” sayfa 170)**
Süreç	MQZAO_CREATE **(“2” sayfa 170)**
Kuyruk yöneticisi	Burada geçerli değil
AdlistMQZAO_CREATE	MQZAO_CREATE **(“2” sayfa 170)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(“2” sayfa 170)**
Kanal	MQZAO_CREATE **(“2” sayfa 170)**
İstemci bağlantı kanalı	MQZAO_CREATE **(“2” sayfa 170)**
Dinleyici	MQZAO_CREATE **(“2” sayfa 170)**
Hizmet	MQZAO_CREATE **(“2” sayfa 170)**

***nesne* kopyala (değiştir) (“1” sayfa 170, “4” sayfa 171)**

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE

***nesne* yarat (değiştirilmeden) (“3” sayfa 170)**

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CREATE **(“2” sayfa 170)**
Konu	MQZAO_CREATE **(“2” sayfa 170)**
Süreç	MQZAO_CREATE **(“2” sayfa 170)**
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CREATE **(“2” sayfa 170)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(“2” sayfa 170)**
Kanal	MQZAO_CREATE **(“2” sayfa 170)**
İstemci bağlantı kanalı	MQZAO_CREATE **(“2” sayfa 170)**
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE

***nesne* yarat (başkasıyla değiştir) (“3” sayfa 170, “4” sayfa 171)**

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CHANGE
Kimlik doğrulama bilgileri	MQZAO_CHANGE
Kanal	MQZAO_CHANGE
İstemci bağlantı kanalı	MQZAO_CHANGE
Dinleyici	MQZAO_CHANGE
Hizmet	MQZAO_CHANGE

Delete *nesne*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_DELETE
Konu	MQZAO_DELETE
Süreç	MQZAO_DELETE
Kuyruk yöneticisi	MQZAO_DELETE
Ad Listesi	MQZAO_DELETE
Kimlik doğrulama bilgileri	MQZAO_DELETE
Kanal	MQZAO_DELETE
İstemci bağlantı kanalı	MQZAO_DELETE
Dinleyici	MQZAO_DELETE

Nesne	Yetki gerekiyor
Hizmet	MQZAO_DELETE

Inquire *nesne*

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_GÖRÜNTÜLE
Konu	MQZAO_GÖRÜNTÜLE
Süreç	MQZAO_GÖRÜNTÜLE
Kuyruk yöneticisi	MQZAO_GÖRÜNTÜLE
Ad Listesi	MQZAO_GÖRÜNTÜLE
Kimlik doğrulama bilgileri	MQZAO_GÖRÜNTÜLE
Kanal	MQZAO_GÖRÜNTÜLE
İstemci bağlantı kanalı	MQZAO_GÖRÜNTÜLE
Dinleyici	MQZAO_GÖRÜNTÜLE
Hizmet	MQZAO_GÖRÜNTÜLE

Inquire *nesne* names

Nesne	Yetki gerekiyor
Kuyruk	Denetim yok
Konu	Denetim yok
Süreç	Denetim yok
Kuyruk yöneticisi	Denetim yok
Ad Listesi	Denetim yok
Kimlik doğrulama bilgileri	Denetim yok
Kanal	Denetim yok
İstemci bağlantı kanalı	Denetim yok
Dinleyici	Denetim yok
Hizmet	Denetim yok

Ping Kanalı

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL

Nesne	Yetki gerekiyor
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

Kanalı Sıfırla

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL_EXTENDED
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

Kuyruk İstatistiklerini Sıfırla

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_DISPLAY ve MQZAO_CHANGE
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	Burada geçerli değil
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	
Hizmet	

Kanalı Çözümle

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil

Nesne	Yetki gerekiyor
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL_EXTENDED
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

Başlangıç Kanalı

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

Kanalı Durdur

Nesne	Yetki gerekiyor
Kuyruk	Burada geçerli değil
Konu	Burada geçerli değil
Süreç	Burada geçerli değil
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	Burada geçerli değil
Kimlik doğrulama bilgileri	Burada geçerli değil
Kanal	MQZAO_CONTROL
İstemci bağlantı kanalı	Burada geçerli değil
Dinleyici	Burada geçerli değil
Hizmet	Burada geçerli değil

Not:

1. Kopyalama komutları için, From nesnesi için MQZAO_DISPLAY yetkisi de gereklidir.
2. MQZAO_CREATE yetkisi belirli bir nesne ya da nesne tipine özgü değil. GRTMQMAUT komutunda QMGR nesne tipi belirtilerek, belirtilen bir kuyruk yöneticisine ilişkin tüm nesneler için yetki yaratma yetkisi verilir.
3. Create komutları için, uygun SYSTEM.DEFAULT.* nesne.

4. Bu seçenek, değiştirilecek nesne önceden varsa geçerlidir. Tersi durumda, bu denetim, kopyaya ya da yaratılmadan yaratılmasına ilişkin olarak olur.

IBM i IBM iüzerinde genel OAM profilleri

Nesne yetkisi yöneticisi (OAM) soysal profilleri, bir kullanıcının bir kerede birden çok nesneye sahip olduğu yetkiyi ayarlamanızı sağlar; bu, yaratıldığında her bir nesneye ilişkin ayrı **GRTMQMAUT** komutları vermek zorunda kalmaktan çok. **GRTMQMAUT** komutundaki soysal profilleri kullanarak, o tanıtıma uyan tüm gelecekteki nesneler için bir genel yetki ayarlayabilirsiniz.

Bu bölümün geri kalan kısmı, soysal profillerin daha ayrıntılı bir şekilde kullanılmasını açıklar:

- "Joker Karakterlerin Kullanılması" sayfa 171
- "Profil öncelikleri" sayfa 171

Joker Karakterlerin Kullanılması

Bir profil soysal, profil adında özel karakterlerin (genel arama karakterleri) kullanılmasıdır. Örneğin, soru imi (?) genel arama karakteri, bir addaki tek bir karakterle eşleşir. Bu nedenle, `ABC.?EF`belirtirseniz, bu tanıtıma verdiğiniz yetki, `ABC.DEF`, `ABC.CEF`, `ABC.BEF`, vb. adlarla oluşturulan nesneler için geçerlidir.

Kullanılabilir genel arama karakterleri şunlardır:

?

Herhangi bir tek karakter yerine soru işaretini (?) kullanın. Örneğin, `AB.?D` , `AB.CD`, `AB.ED`ve `AB.FD`nesnelerine uygulardı.

*****

Yıldız işaretini (*) aşağıdaki gibi kullanın:

- Profil adındaki bir *niteleyici* , bir nesne adındaki herhangi bir niteleyiciye eşleştirmek için. Niteleyici, bir nokta ile sınırlanmış bir nesne adının parçasıdır. For example, in `ABC.DEF.GHI`, the qualifiers are `ABC`, `DEF`, and `GHI`.

  For example, `ABC.*.JKL` would apply to the objects `ABC.DEF.JKL`, and `ABC.GHI.JKL`. (**değil** için `ABC.JKL` uygulamasına geçeceğine dikkat edin; * bu bağlamda kullanılan her zaman tek bir niteleyici belirtir.)
- Bir nesne adındaki niteleyici içinde sıfır ya da daha fazla karakterle eşleşen bir niteleyici içindeki bir niteleyici.

  Örneğin, `ABC.DE*.JKL` , `ABC.DE.JKL`, `ABC.DEF.JKL`ve `ABC.DEGH.JKL`nesnelerine uygulardı.

******

Profil adında aşağıdaki gibi çift yıldız işaretini (**) ***bir kez*** kullanın:

- Tüm nesne adlarını eşleştirmek için tüm profil adı. Örneğin, süreçleri tanımlamak için `OBJTYPE (*PRC)` anahtar sözcüğünü kullanırsanız, tanıtım adı olarak ** kullanırsanız, tüm süreçlere ilişkin yetkileri değiştirirsiniz.
- Bir profil adındaki başlangıç, orta ya da bitiş niteleyicisini, bir nesne adındaki sıfır ya da daha çok niteleyiciyle eşleşecek şekilde eşleştirin. Örneğin, `**.ABC` , ABC final niteleyicisine sahip tüm nesneleri tanıtır.

Profil öncelikleri

Soysal profilleri kullanırken anlamanın önemli bir noktası, oluşturulmakta olan bir nesneye hangi yetkilerin uygulanana karar verilirken profillerin verilme önceliğidir. Örneğin, komutları yayınladığınızı varsayalım:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

The first gives put authority to all queues for the principal FRED with names that match the profile AB.*; the second gives get authority to the same types of queue that match the profile AB.C*.

Şimdi AB.CD. Genel arama karakteri eşleştirmesine ilişkin kurallara göre, GRTMQMAUT bu kuyruğa başvur. Yani, otoriteyi ortaya koyması mı, yoksa yetki mi?

Yanıtı bulmak için, bir nesneye birden çok profil uygulandığında, **yalnızca en özel geçerli**olan kuralı uygulayabilirsiniz. Bu kuralı uyguladığınız yol, profil adlarını soldan sağa ile karşılaştırarak uygulanır. Farklı bir karakter varsa, soysal olmayan bir karakter soysal bir karakterden daha özgüdür. So, in the previous example, the queue AB.CD has **alma** authority (AB.C* is more specific than AB.*).

Soysal karakterleri karşılaştırırken, *belirtimlilik* sırası şöyledir:

1. ?
2. *
3. **

IBM i IBM iüzerinde kurulu yetkilendirme hizmetini belirtme

Hangi yetki hizmeti bileşenini kullanabileceğini belirtebilirsiniz.

GRTMQMAUT ve **RVKMQMAUT** üzerindeki **Service Component name** parametresi, kurulu yetki hizmeti bileşeninin adını belirtmenizi sağlar.

İlk panoda **F24** öğesinin seçilmesi, komutların sonraki panosunda bulunan **F9=All değiştirgeleri** ise, kurulu yetki bileşenini (*DFT) ya da kuyruk yöneticisinin qm.ini kütüğünün Hizmet kısmında belirtilen gerekli yetki hizmeti bileşenini belirtmenize olanak tanır.

DSPMQMAUT ' da bu ek parametre de vardır. Bu parametre, belirlenen nesne adı, nesne tipi ve kullanıcı için tüm kurulu yetki bileşenlerinde (*DFT) ya da belirtilen yetki hizmeti bileşeni adını aramanıza olanak sağlar.

IBM i IBM iüzerinde yetki profilleri ile ve yetki profilsiz çalışma

Yetki profilleriyle nasıl çalışacağını ve yetki profilleri olmadan nasıl çalışacağını öğrenmek için bu bilgileri kullanın.

You can work with authority profiles, as explained in “Yetki profilleriyle çalışma” sayfa 172, or without them, as explained here:

To work without authority profiles, use *NONE as an Authority parameter on **GRTMQMAUT** to create profiles without authority. Bu, var olan tanıtımların hiçbirini değiştirmeden bırakır.

RVKMQMAUT' ta, var olan bir yetki profilini kaldırmak için Yetki değiştirgesi olarak *REMOVE değiştirgesini kullanın.

Yetki profilleriyle çalışma

Yetki profilleme ile ilişkili iki komut vardır:

- **WRKMQMAUT**
- **WRKMQMAUTD**

Bu komutlara, doğrudan komut satırından ya da WRKMQM panosundan aşağıdaki komutları kullanarak erişebilirsiniz:

1. Typing in the queue manager name and pressing the Enter key to access the **WRKMQM** results panel.
2. Bu panodaki F23=More options öğesini seçin.

Seçenek 24, **WRKMQMAUT** komutu ve seçenek 25 için sonuç panelini seçer. Bu seçenek, SSL bağ tanımları katmanında kullanılan **WRKMQMAUTI** komutunu seçer.

WRKMQMAUT

Bu komut, yetki kuyruğunda tutulan yetki verileri ile çalışmanızı sağlar.

Not: Bu komutu çalıştırmak için kuyruk yöneticisine `*connect` ve `*admdsp` yetkinizin olması gerekir. Ancak, bir tanıtım yaratmak ya da silmek için QMQMADM yetkisine gerek duyarsınız.

Bilgileri ekrana çıkıyorsanız, yetki profili adlarının bir listesi, tipleriyle birlikte görüntülenir. Çıktıyı yazdırırsanız, tüm yetki verilerinin, kayıtlı kullanıcıların ve yetkilerinin ayrıntılı bir listesini alırsınız.

Bu panoda bir nesne ya da profil adı girmek ve ENTER tuşuna basmak sizi **WRKMQMAUT** için sonuç panosuna götürür.

`4=Delete`seçeneğini belirlerseniz, belirlediğiniz genel yetki profili adına kayıtlı tüm kullanıcı adlarını silmek istediğinizi onaylayabileceğiniz yeni bir panoya gidin. Bu seçenek **RVKMQMAUT** ' u tüm kullanıcılar için *REMOVE seçeneğiyle çalıştırır ve soysal profil adlarına **yalnızca** uygulanır.

`12=Work with profile` seçeneğini belirlerseniz, **WRKMQMAUTD** komut sonuçları panosuna gidin (“WRKMQMAUTD” sayfa 173' da açıklandığı gibi).

WRKMQMAUTD

Bu komut, belirli bir yetki tanıtımı adı ve nesne tipi ile kayıtlı tüm kullanıcıları görüntülemenizi sağlar. Bu komutu çalıştırmak için kuyruk yöneticisine `*connect` ve `*admdsp` yetkinizin olması gerekir. Ancak, QMQMADM yetkisine gerek olan bir tanıtımı vermek, çalıştırmak, yaratmak ya da silmek için bu tanıtımı kullanın.

Selecting `F24=More keys` from the initial input panel, followed by option `F9=All Parameters` displays the Service Component Name as for **GRTMQMAUT** and **RVKMQMAUT**.

Not: `F11=Display Object Authorizations` tuşu, aşağıdaki yetki tipleri arasında geçiş yapar:

- Nesne yetkileri
- Bağlam yetkileri
- MQI yetkileri

Ekrandaki seçenekler şunlardır:

2=Grant
Geçerli yetkilerine eklemek için sizi **GRTMQMAUT** panosuna götürür.

3=Revoke
Yürürlükteki tanımların bazılarını kaldırmak için sizi **RVKMQMAUT** panosuna götürür

4=Delete
Belirlenen kullanıcılara ilişkin yetki verilerini silmenizi sağlayan bir panoya götürür. Bu işlem, **RVKMQMAUT** seçeneği ile *REMOVE seçeneğini çalıştırır.

5=Display
Sizi var olan **DSPMQMAUT** komutuna götürür

F6=Create
Bir tanıtım yetkisi kaydı yaratmanıza olanak tanıyan **GRTMQMAUT** panosuna sizi götürür.

IBM i IBM i ile ilgili Nesne Yetkilisi Yöneticisi yönergeleri

Nesne yetki yöneticisini (OAM) kullanmaya ilişkin ek ipuçları

Hassas işlemlere erişimi sınırla

Bazı işlemler hassastır; ayrıcalıklı kullanıcılarla sınırlandırın. Örneğin,

- İletim kuyrukları ya da komut kuyruğu gibi bazı özel kuyruklara erişilmesi `SYSTEM.ADMIN.COMMAND.QUEUE`
- Tam MQI bağlamı seçeneklerini kullanan programların çalıştırılması
- Uygulama kuyruklarının yaratılması ve kopyalanması

Kuyruk yöneticisi dizinleri

Kuyruk ve diğer kuyruk yöneticisi verilerini içeren dizinler ve kitaplıklar ürün için özeldir. MQI kaynaklarına yetki vermek ya da yetkileri iptal etmek için standart işletim sistemi komutlarını kullanmayın.

Kuyruklar

Dinamik bir kuyruk için yetki, türetildiği model kuyruğuyla aynı olmasına karşın mutlaka aynı değildir.

Diğer ad kuyrukları ve uzak kuyruklar için yetki, diğer adın ya da uzak kuyruğun çözüldüğü kuyruk değil, nesnenin kendisi içindir. Bir kullanıcı tanıtımına, kullanıcı tanıtımının erişim izni olmayan bir yerel kuyruğa çözülen bir diğer ad kuyruğuna erişim yetkisi verilebilir.

Ayrıcalıklı kullanıcılar için kuyruk yaratma yetkisini sınırlayın. Bunu yapmazsanız, kullanıcılar bir diğer ad yaratarak normal erişim denetimini atlayabilir.

Diğer kullanıcı yetkisi

Diğer kullanıcı yetkisi, bir kullanıcı tanıtımının bir IBM MQ nesnesine erişirken başka bir kullanıcı tanıtımının yetkisini kullanıp kullanamayacağını denetler. Bu teknik, bir sunucu bir programdan istek alırsa ve sunucu, programın istek için gerekli yetkiye sahip olduğundan emin olmak isterse gereklidir. Sunucu gerekli yetkiye sahip olabilir, ancak programın istediği işlemlere ilişkin yetkiye sahip olup olmadığını bilmesi gerekir.

Örneğin:

- PAYSERV kullanıcı profili altında çalışan bir sunucu programı, USER1kullanıcı profili tarafından kuyruğa konan bir kuyruktan bir istek iletisi alır.
- Sunucu programı istek iletisini aldığında, isteği işler ve yanıtı istek iletisiyle belirlenen yanıt kuyruğuna geri koyar.
- Sunucu, yanıt kuyruğunun açılmasını yetkilendirmek için kendi kullanıcı profilini (PAYSERV) kullanmak yerine, USER1adlı başka bir kullanıcı profili belirtebilir. Bu örnekte, PAYSERV ' nin yanıt kuyruğunu açtığında alternatif kullanıcı profili olarak USER1 belirtip belirtmeyeceğini denetlemek için alternatif kullanıcı yetkisini kullanabilirsiniz.

Diğer kullanıcı tanıtımı, nesne tanımlayıcısının *AlternateUserId* alanında belirtilir.

Not: Herhangi bir IBM MQ nesnesinde diğer kullanıcı tanıtımlarını kullanabilirsiniz. Diğer kullanıcı tanıtımının kullanılması, diğer kaynak yöneticileri tarafından kullanılan kullanıcı tanıtımını etkilemez.

Bağlam yetkisi

Bağlam, belirli bir ileti için geçerli olan ve iletinin bir parçası olan ileti tanımlayıcısı MQMD ' de bulunan bilgilerdir.

Bağlamla ilgili ileti tanımlayıcı alanlarının açıklamaları için MQMD ' ye genel bakışbaşlıklı konuya bakın.

Bağlam seçenekleri hakkında bilgi için bkz. İleti bağlamı.

Uzak güvenlikle ilgili dikkat edilmesi gereken noktalar

Uzak güvenlik için şunları göz önünde bulundurun:

Yetki koy
Kuyruk yöneticileri arasında güvenlik için, bir kanal başka bir kuyruk yöneticisinden gönderilen bir iletiyi aldığında kullanılacak koyma yetkisini belirtebilirsiniz.

Bu parametre yalnızca RCVR, RQSTR ya da CLUSRCVR kanal tipleri için geçerlidir. PUTAUT kanal özniteliğini aşağıdaki gibi belirtin:

DEF
Varsayılan kullanıcı profili. Bu, ileti kanalı aracısının altında çalıştığı QMQM kullanıcı profilidir.

CTX
İleti bağlamındaki kullanıcı profili.

İletim kuyrukları
Kuyruk yöneticileri uzak iletileri otomatik olarak bir iletim kuyruğuna yerleştirir; özel bir yetki gerekmez. Ancak, iletiyi doğrudan bir iletim kuyruğuna koymak için özel yetki gerekir.

Kanal çıkışları
Kanal çıkışları, ek güvenlik için kullanılabilir.

Kanal kimlik doğrulama kayıtları
Kanal düzeyinde bağlanan sistemlere verilen erişim üzerinde daha kesin denetim sağlamak için kullanılır.

Uzak güvenlikle ilgili daha fazla bilgi için bkz. "Kanal yetkisi" sayfa 103.

SSL/TLS ile kanalları koruma

TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolü, gizlice dinleme, kurcalama ve taklit edilmeye karşı koruma ile kanal güvenliği sağlar. TLS için IBM MQ desteği, kanal tanımında belirli bir kanalın TLS güvenliğini kullandığını belirtmenize olanak sağlar. Kullanmak istediğiniz şifreleme algoritması gibi, istediğiniz güvenliğin ayrıntılarını da belirleyebilirsiniz.

IBM MQ içindeki TLS desteği, kuyruk yöneticisi *kimlik doğrulama bilgileri nesnesini* ve çeşitli CL ve MQSC komutlarını ve kuyruk yöneticisi ve kanal parametrelerini kullanır.

Aşağıdaki CL komutları TLS ' yi destekler:

WRKMQMAUTI
Bir kimlik doğrulama bilgileri nesnesinin öznitelikleriyle çalışabilmenizi sağlar.

CHGMQMAUTI
Bir kimlik doğrulama bilgileri nesnesinin özniteliklerini değiştirin.

CRTMQMAUTI
Bir kimlik doğrulama bilgileri nesnesi oluşturun.

CPYMQMAUTI
Var olan bir kimlik doğrulama bilgisi nesnesini kopyalayarak bir kimlik doğrulama bilgisi nesnesi oluşturun.

DLTMQMAUTI
Bir kimlik doğrulama bilgileri nesnesini silin.

DSPMQMAUTI
Belirli bir kimlik doğrulama bilgileri nesnesine ilişkin öznitelikleri görüntüler.

TLS kullanan kanal güvenliğine genel bakış için bkz.

- TLS ile kanalları koruma

TLS ile ilişkili PCF komutlarının ayrıntıları için bkz.

- Kimlik Doğrulama Bilgileri Nesnesini Değiştir, Kopyala ve Oluştur
- Kimlik Doğrulama Bilgileri Nesnesini Sil
- Kimlik Doğrulama Bilgileri Nesnesi

z/OS z/OSüzerinde güvenliğin ayarlanması

z/OS' a özgü güvenlik konuları.

IBM MQ for z/OS içindeki güvenlik RACF kullanılarak ya da eşdeğer bir dış güvenlik yöneticisi (ESM) kullanılarak denetlenir.

Aşağıdaki yönergelerde RACFkomutunu kullandığınız varsayılır.

İlgili başvurular

Güvenlik senaryosu: z/OSüzerinde iki kuyruk yöneticisi

Güvenlik senaryosu: z/OSüzerinde kuyruk paylaşım grubu

z/OS RACF güvenlik sınıfları

RACF classes are used to hold the profiles required for IBM MQ security checking. Üye sınıflarının çoğu, eşdeğer grup sınıflarına sahiptir. Sınıfları etkinleştirmeli ve soysal profilleri kabul etmelerine olanak tanımalısınız

Each RACF class holds one or more profiles used at some point in the checking sequence, as shown in Çizelge 23 sayfa 176.

Çizelge 23. IBM MQtarafından kullanılanRACF sınıfları

Üye sınıfı	Grup sınıfı	İçindekiler
MQADMIN	GMQADMIN	Tanıtımlar: Daha çok yönetim tipi işlevlere ilişkin profilleri tutmak için kullanılır. Örneğin: • IBM MQ güvenlik anahtarlarına ilişkin profiller • RESVELL güvenlik profili • Diğer kullanıcı güvenliği için profiller • Bağlam güvenliği tanıtımı • Komut kaynağı güvenliği için tanıtımlar
MXADMIN	GMXADMIN	Tanıtımlar: Daha çok yönetim tipi işlevlere ilişkin profilleri tutmak için kullanılır. Örneğin: • IBM MQ güvenlik anahtarlarına ilişkin profiller • RESVELL güvenlik profili • Diğer kullanıcı güvenliği için profiller • Bağlam güvenliği tanıtımı • Komut kaynağı güvenliği için tanıtımlar Bu sınıf hem büyük, hem de karışık büyük/küçük harf RACF tanıtımlarını tutabilir.
MQCONN		Bağlantı güvenliği için kullanılan tanıtımlar
MQCMDS		Komut güvenliği için kullanılan tanıtımlar
MQQUEUE	GMQQUEUE	Kuyruk kaynağı güvenliğinde kullanılan tanıtımlar
MXQU	GMXQUEUE	Kuyruk kaynağı güvenliğinde kullanılan büyük/küçük harf ve büyük tanıtımlar
MQPROC	GMQPROC	Süreç kaynağı güvenliğinde kullanılan tanıtımlar
MXPROC	GMXPROC	Süreç kaynağı güvenliğinde kullanılan büyük/küçük harf ve büyük tanıtımlar
MQNLIST	GMQNLIST	Ad listesi kaynak güvenliğinde kullanılan tanıtımlar
MXNLIST	GXNLIST	Ad listesi kaynak güvenliğinde kullanılan büyük/küçük harf ve büyük harf tanıtımlar

Çizelge 23. IBM MQtarafından kullanılanRACF sınıfları (devamı var)		
Üye sınıfı	**Grup sınıfı**	**İçindekiler**
MXKONUSU	GMXKONUSU	Konu güvenliğinde kullanılan büyük/küçük harf ve büyük harf tanıtımlar

Bazı sınıfların, benzer erişim gereksinimlerine sahip olan kaynak gruplarını bir araya getirebilmenizi sağlayan ilgili bir *grup sınıfı* vardır. Üye ve grup sınıfları arasındaki farklılığı ve bir üye ya da grup sınıfını ne zaman kullanabilmeye ilişkin ayrıntılar için z/OS Security Server RACF Security Administrator's Guideadlı yayına bakın.

Güvenlik denetimlerinin yapılabilmesi için önce sınıfların etkinleştirilmesi gerekir. Tüm IBM MQ sınıflarını etkinleştirmek için bu RACF komutunu kullanabilirsiniz:

```
SETROPTS CLASSACT(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                  MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

Ayrıca, sınıfların soysal profilleri kabul edebilmeleri için ayarladığınızdan emin olmanız gerekir. You also do this with the RACF command SETROPTS, for example:

```
SETROPTS GENERIC(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                 MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

z/OS RACF profiller

IBM MQ tarafından kullanılan tüm RACF tanıtımlarının bir önek (kuyruk yöneticisi adı ya da kuyruk paylaşım grubu adı) vardır. Genel arama karakteri olarak yüzde işaretini kullanırken dikkatli olun.

IBM MQ tarafından kullanılan tüm RACF profilleri bir önek içerir. Kuyruk paylaşım grubu düzeyinde güvenlik için bu, kuyruk paylaşım grubu adıdır. Kuyruk yöneticisi düzeyinde güvenlik için önek, kuyruk yöneticisi adıdır. Kuyruk yöneticisi ve kuyruk paylaşımı grubu düzeyinde güvenlik karışımı kullanıyorsanız, her iki önek tipiyle de tanıtımları kullanırsınız. (Kuyruk paylaşımı grubu ve kuyruk yöneticisi düzeyi güvenliği IBM MQ for z/OS concepts: securitybaşlıklı konularda açıklanmaktadır.)

Örneğin, kuyruk paylaşım grubu düzeyinde QSG1 kuyruk paylaşım grubunda QUEUE_FOR_SUBSCRIBER_LIST adlı bir kuyruğu korumak istiyorsanız, uygun profil şu şekilde RACF olarak tanımlanacaktı:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Kuyruk yöneticisi düzeyindeki kuyruk yöneticisi STCD ' ye ait olan QUEUE_FOR_LOST_CARD_LIST adlı bir kuyruğu korumak istiyorsanız, uygun tanıtım RACF olarak tanımlanacak:

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

Bu, farklı kuyruk yöneticilerinin ve kuyruk paylaşım gruplarının aynı RACF veritabanını paylaşabileceği ve henüz farklı güvenlik seçeneklerine sahip olduğu anlamına gelir.

Beklenmeyen kullanıcı erişimini önlemek için profillerde soysal kuyruk yöneticisi adlarını kullanmayın.

IBM MQ , nesne adlarında yüzde işaretinin (%) kullanımına izin verir. Ancak, RACF tek karakterli bir joker karakter olarak% karakterini kullanır. Bu, adında bir% karakteri olan bir nesne adı tanımladığınızda, ilgili profili tanımlarken bunu göz önünde bulundurmanız gerektiği anlamına gelir.

Örneğin, kuyruk yöneticisi CRDP ' de CREDIT_CARD_ %_rate_rectrk kuyruk için, profil RACF olarak aşağıdaki gibi tanımlanacaktı:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Bu kuyruk, CRDP * * gibi soysal bir tanıtım tarafından korunamaz.

IBM MQ , nesne adlarında karışık büyük harf karakterlerinin kullanılmasına izin verir. Şunları tanımlayarak bu nesneleri koruyabilirsiniz:

1. Uygun karma vaka RACF sınıflarında karma vaka profilleri ya da
2. Uygun büyük harfli RACF sınıflarındaki soysal tanıtımlar.

Karma vaka profillerini ve karma case RACF sınıflarını kullanmak için, “z/OS Kuyruk yöneticisinin büyük ve küçük harfe karışık olarak geçirilmesi” sayfa 256içinde açıklanan adımları izlemeniz gerekir.

Yalnızca değerler IBM MQtarafından sağlandığı için büyük harf olarak kalan bazı profiller ya da profillerin bölümleri vardır. Bu bilgiler şunlardır:

- Profilleri değiştirin.
- Altsistem ve kuyruk paylaşım grubu tanıtıcıları da içinde olmak üzere tüm üst düzey niteleyiciler (HLQ).
- SYSTEM nesnelerine ilişkin tanıtımlar.
- Varsayılan nesnelere ilişkin tanıtımlar.
- **MQCMDS** sınıfı, tüm komut tanıtımları yalnızca büyük harflerdir.
- **MQCONN** sınıfı, bu nedenle tüm bağlantı tanıtımları yalnızca büyük harflerdir.
- **RESLEVEL** profilleri.
- Komut kaynağı tanıtımlarındaki `'object'` niteliği; örneğin, `hlq.QUEUE.queuename`. Kaynak adı yalnızca büyük/küçük harf karışık olur.
- Dinamik kuyruk profilleri `hlq.CSQOREXX.*`, `hlq.CSQUTIL.*`ve `CSQXCMD.*`.
- `'CONTEXT'` `hlq.CONTEXT.resourcename`kısmı.
- `hlq.ALTERNATE.USER.userid'` in `'ALTERNATE.USER'` kısmı.

For example, if you have a queue called `PAYROLL.Dept1` on Queue Manager `QM01` and you are using:

- Karma vaka profilleri; IBM MQ RACF sınıfında bir profil tanımlayabilir `MXQUEUE`

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- Uppercase profiles; you can define a profile in the IBM MQ RACF class `MQQUEUE`

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

İlk örnek, karma vaka tanıtımlarını kullanarak, kaynağa erişim yetkisi verilmesine ilişkin daha ayrıntılı denetim sağlar.

z/OS Tanıtımları değiştir

To control the security checking performed by IBM MQ, you use *anahtar profilleri*. Anahtar tanıtımı, IBM MQiçin özel bir anlamı olan olağan bir RACF tanıtımdır. Anahtar profillerindeki erişim listesi IBM MQtarafından kullanılmaz.

IBM MQ , çizelgelerde gösterilen her anahtar tipi için bir iç anahtar sağlar. Altsistem düzeyinde güvenlik için anahtar profilleri, Kuyruk paylaşımı grubu ya da kuyruk yöneticisi düzeyi güvenliği için profiller değiştirve Kaynak denetiminde anahtar profilleri. Anahtar tanıtımları kuyruk paylaşımı grubu düzeyinde ya da kuyruk yöneticisi düzeyinde ya da her ikisinin bir birleşimiyle sağlanabilir. Tek bir kuyruk paylaşım grubu güvenlik anahtarı profillerini kullanarak, bir kuyruk paylaşım grubu içindeki tüm kuyruk yöneticilerindeki güvenliği denetleyebilirsiniz.

Bir güvenlik anahtarı ayarlandığında, anahtarla ilişkili güvenlik denetimleri gerçekleştirilir. Bir güvenlik anahtarı ayarlandığında, anahtarla ilişkili güvenlik denetimleri atlanır. Varsayılan değer, tüm güvenlik anahtarlarının üzerinde ayarlanandır.

z/OS *Anahtarlar ve sınıflar*

Bir kuyruk yöneticisi başlattığınızda ya da güvenliği yenilediğinizde IBM MQ , anahtarları çeşitli RACF sınıflarının durumuna göre ayarlar.

Bir kuyruk yöneticisi başlatıldığında (ya da IBM MQ REFRESH SECURITY komutu tarafından MQADMIN ya da MXADMIN sınıfı yenilendiğinde), IBM MQ öncelikle RACF durumunu ve uygun sınıfı denetler:

- Büyük harf tanıtımlar kullanıyorsanız, MQADMIN sınıfı
- Karma vaka profili kullanıyorsanız, MXADMIN sınıfı.

Bu koşullardan herhangi biri doğruysa, altsistem güvenlik anahtarını kapalı olarak ayarlar:

- RACF etkin değil ya da kurulu değil.
- MQADMIN ya da MXADMIN sınıfı tanımlanmadı (sınıf tanımlayıcı çizelgesine (CDT) dahil oldukları için bu sınıflar her zaman RACF için tanımlıdır).
- MQADMIN ya da MXADMIN sınıfı etkinleştirilmedi.

Hem RACF hem de MQADMIN ya da MXADMIN sınıfı etkinse, IBM MQ , anahtar profillerinden herhangi birinin tanımlanıp tanımlanmadığını görmek için MQADMIN ya da MXADMIN sınıfını denetler. İlk olarak, “Altsistem güvenliğini denetlemek için profiller” sayfa 180içinde açıklanan tanıtımları denetler. Altsistem güvenliği gerekmiyorsa, IBM MQ , iç altsistem güvenlik anahtarını kapalı olarak ayarlar ve başka bir denetleme işlemi gerçekleştirmez.

Tanıtımlar, ilgili IBM MQ anahtarının açık mı, yoksa kapalı mı olduğunu belirler.

- Anahtar kapalıysa, bu tip bir güvenlik devre dışı bırakılır.
- Herhangi bir IBM MQ anahtarı ayarlanmışsa, IBM MQ , IBM MQ anahtarına karşılık gelen güvenlik türüyle ilişkilendirilen RACF sınıfının durumunu denetler. Sınıf kurulmamışsa ya da etkin değilse, IBM MQ anahtarı kapatılır. Örneğin, MQPROC ya da MXPROC sınıfı etkinleştirilmediyse, süreç güvenliği denetimlerinin gerçekleştirilmemesi gerekir. Etkin olmayan sınıf, NO.PROCESS.CHECKS , bu RACF veritabanını kullanan her kuyruk yöneticisi ve kuyruk paylaşım grubu için bir tanıtım sağlar.

z/OS *İşin çalışma şekli*

Bir güvenlik anahtarını kapatmak için bir NO.* tanımlayın. Bunun için anahtar profili değiştirin. Bir NO.* ' ı geçersiz kılabilirsiniz. Bir YES.* tanımlayarak kuyruk paylaşım grubu düzeyinde profil kümesi bir kuyruk yöneticisine ilişkin tanıtım.

Bir güvenlik anahtarını kapatmak için, bir NO.* tanımlamanız gerekir. Bunun için anahtar profili değiştirin. Bir NO.* ' nın varlığı. tanıtım, belirli bir kuyruk yöneticisindeki bir kuyruk paylaşım grubu düzeyi ayarını geçersiz kılamayı seçmediğiniz sürece, o kaynak tipi için güvenlik denetimlerinin **gerçekleştirilmediğini** belirtir. Bu, “Geçersiz kılma kuyruğu paylaşım grubu düzeyi ayarları” sayfa 180içinde açıklanmaktadır.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesi değilse, herhangi bir kuyruk paylaşım grubu düzey tanıtımı ya da herhangi bir geçersiz kılma profili tanımlamanıza gerek yoktur. Ancak, kuyruk yöneticisi daha sonraki bir tarihte bir kuyruk paylaşım grubuna katılırsa, bu tanıtımları tanımlamayı unutmamalısınız.

Her NO.* IBM MQ ' in algıladığı anahtar profili, bu kaynak tipini denetleyerek kapatır. Anahtar tanıtımları kuyruk yöneticisinin başlatılması sırasında etkinleştirilir. If you change the switch profiles while any affected queue managers are running, you can get IBM MQ to recognize the changes by issuing the IBM MQ REFRESH SECURITY command.

Anahtar tanıtımlarının her zaman MQADMIN ya da MXADMIN sınıfında tanımlanması gerekir. Bunları GMQADMIN ya da GMXADMIN sınıfından tanımlamayın. Tables Altsistem düzeyinde güvenlik için anahtar profilleri and Kaynak denetimi için profilleri değiştir show the valid switch profiles and the security type they control.

Geçersiz kılma kuyruğu paylaşım grubu düzeyi ayarları

Belirli bir kuyruk yöneticisine ilişkin kuyruk paylaşım grubu düzeyi güvenlik ayarlarını, o grubun üyesi olan bir kuyruk yöneticisine geçersiz kılabilirsiniz. Kuyruk yöneticisi, gruptaki diğer kuyruk yöneticilerinde gerçekleştirilmeyen bir kuyruk yöneticisini denetleyerek, (qmgr-name.YES. *) öğesini kullanın. anahtar profilleri.

Tersi durumda, bir kuyruk paylaşım grubu içindeki belirli bir kuyruk yöneticisinden belirli bir denetimi gerçekleştirmek istemiyorsanız, bir (qmgr-name.NO. *) değerini tanımlayın. Kuyruk yöneticisininde o belirli kaynak tipine ilişkin tanıtım olup olmadığını ve kuyruk paylaşım grubu için tanıtım tanımlamadığını belirtin. (IBM MQ , kuyruk yöneticisi düzeyinde bir tanıtım bulamazsa, kuyruk paylaşım grubu düzeyinde tanıtım olup olmadığını denetler.)

z/OS *Altsistem güvenliğini denetlemek için profiller*

IBM MQ , altsistem güvenlik denetimlerinin altsistem için, kuyruk yöneticisi için ve kuyruk paylaşım grubu için gerekli olup olmadığını denetler.

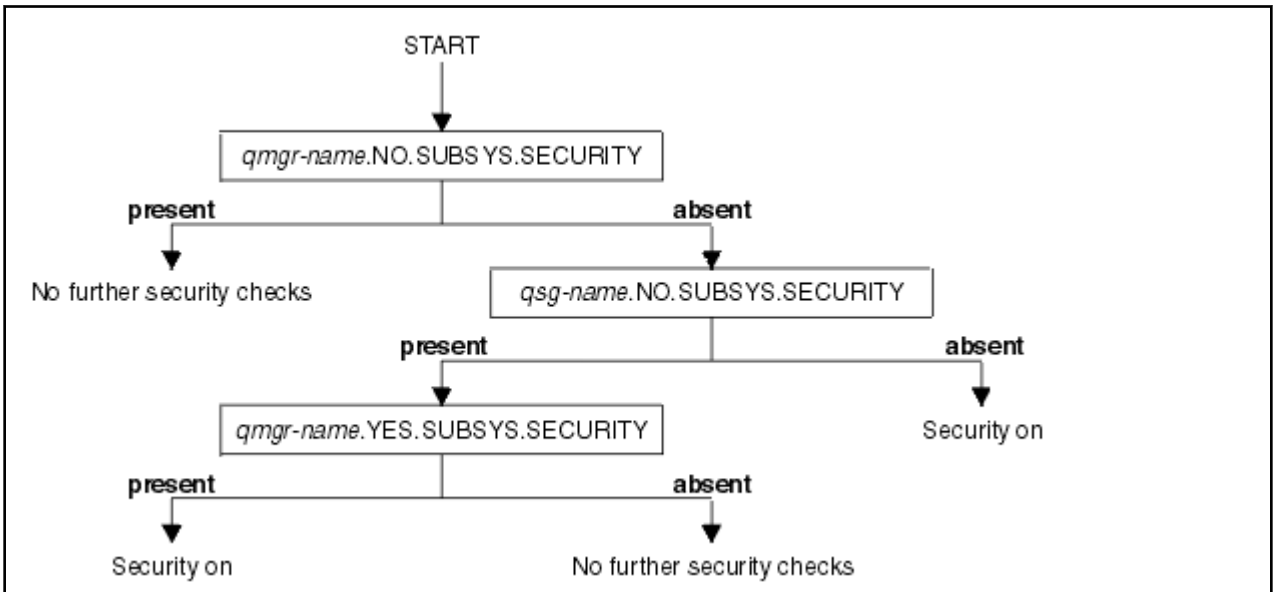
IBM MQ tarafından yapılan ilk güvenlik denetimi, tüm IBM MQ altsistemi için güvenlik denetlerinin gerekli olup olmadığını belirlemek için kullanılır. Altsistem güvenliğini istemiyorsanız, başka denetim yapılmadığını da belirtiyorsanız.

Altsistem güvenliğinin gerekli olup olmadığını belirlemek için aşağıdaki anahtar profilleri imlenir. Şekil 14 sayfa 180 , işaretlendikleri sırayı gösterir.

Çizelge 24. Altsistem düzeyinde güvenlik için anahtar profilleri

Anahtar profili adı	**Denetlenmiş kaynağın ya da denetmenin tipi**
qmgr-name.NO.SUBSYS.SECURITY	Bu kuyruk yöneticisine ilişkin altsistem güvenliği
qsg-name.NO.SUBSYS.SECURITY	Bu kuyruk paylaşım grubu için altsistem güvenliği
qmgr-name.YES.SUBSYS.SECURITY	Bu kuyruk yöneticisine ilişkin altsistem güvenliği geçersiz kılma değeri

Kuyruk yöneticinizin bir kuyruk paylaşım grubunun üyesi değilse, IBM MQ yalnızca qmgr-name.NO.SUBSYS.SECURITY anahtar profilini denetler.



Şekil 14. Altsistem güvenliği denetleniyor

z/OS *Kuyruk paylaşım grubunu ya da kuyruk yöneticisi düzeyinde güvenliği denetlemek için tanıtımlar*

Altsistem güvenliği denetimi gerekiyorsa, IBM MQ , kuyruk paylaşım grubunda ya da kuyruk yöneticisi düzeyinde güvenlik denetiminin gerekli olup olmadığını denetler.

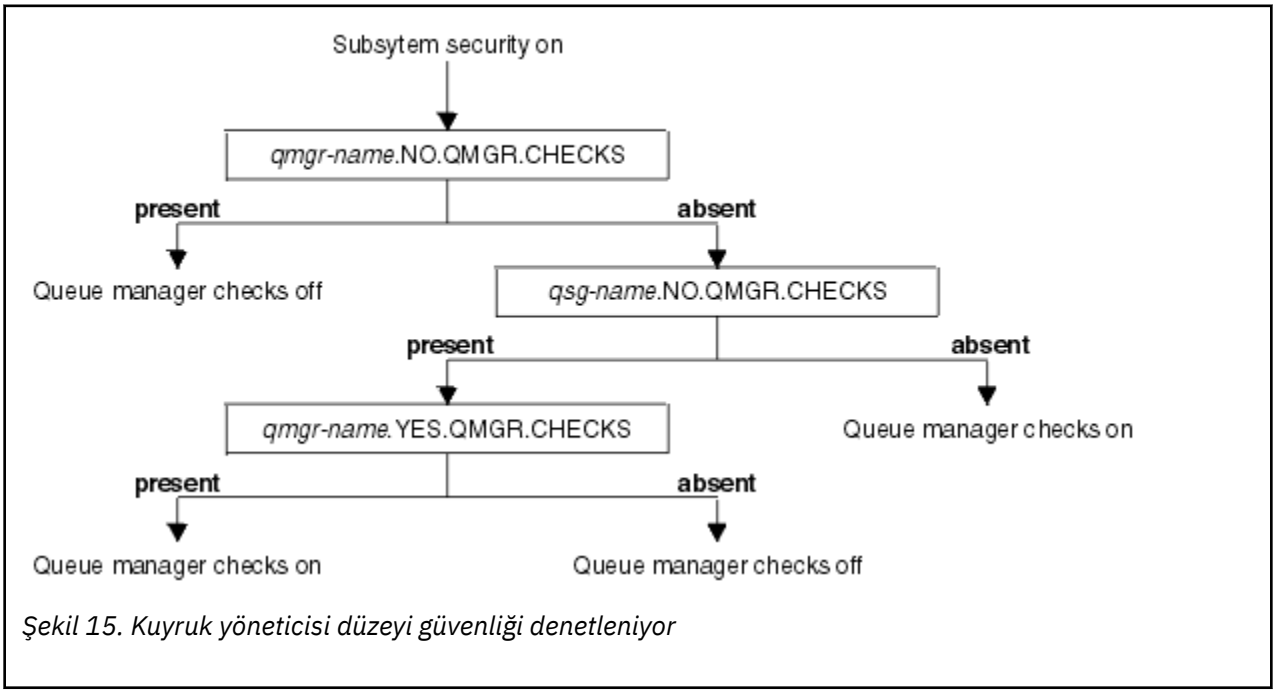
IBM MQ , güvenlik denetiminin gerekli olduğunu belirlediğinde, bu onay denetiminin kuyruk paylaşım grubunda mı, kuyruk yöneticisi düzeyinde mi, yoksa her ikisi için mi gerekli olup olmadığını belirler. Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesi değilse, bu denetimler gerçekleştirilmez.

Gereken düzeyi belirlemek için aşağıdaki anahtar tanıtımları imlenir. Şekil 15 sayfa 181 ve Şekil 16 sayfa 182 , işaretlendikleri sırayı gösterir.

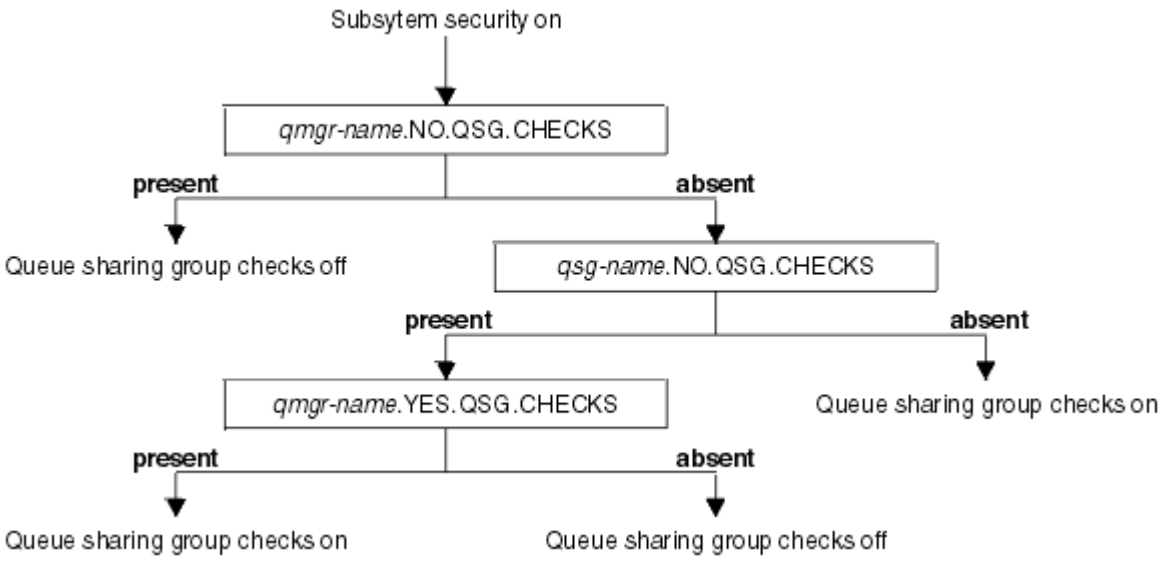
Çizelge 25. Kuyruk paylaşım grubu ya da kuyruk yöneticisi düzeyi güvenliği için tanıtımları değiştir

Anahtar profili adı	**Denetlenmiş kaynağın ya da denetmenin tipi**
qmgr-name.NO.QMGR.CHECKS	Bu kuyruk yöneticisi için kuyruk yöneticisi düzeyi denetimi yok
qsg-name.NO.QMGR.CHECKS	Bu kuyruk paylaşım grubu için kuyruk yöneticisi düzeyi denetimi yok
qmgr-name.YES.QMGR.CHECKS	Kuyruk yöneticisi düzeyinde bu kuyruk yöneticisi için geçersiz kılma denetimi var
qmgr-name.NO.QSG.CHECKS	Bu kuyruk yöneticisi için kuyruk paylaşımı grubu düzeyi denetimi yok
qsg-name.NO.QSG.CHECKS	Bu kuyruk paylaşım grubu için kuyruk paylaşımı grubu düzeyi denetimi yok
qmgr-name.YES.QSG.CHECKS	Kuyruk paylaşım grubu düzeyinde bu kuyruk yöneticisi için geçersiz kılma değeri var

Altsistem güvenliği etkinse, hem kuyruk paylaşım grubunu hem de kuyruk yöneticisi düzeyinde güvenliği kapatamazsınız. Bunu yapmaya çalışırsanız, IBM MQ her iki düzeyde de güvenlik denetimini ayarlar.



Şekil 15. Kuyruk yöneticisi düzeyi güvenliği denetleniyor



Şekil 16. Kuyruk paylaşımı grubu düzeyinde güvenlik olup olmadığını denetleniyor

z/OS *Geçerli güvenlik anahtarları birleşimleri*

Yalnızca belirli anahtarların birleşimleri geçerlidir. If you use a combination of switch settings that is not valid, message CSQH026I is issued and security checking is set on at both queue sharing group and queue manager level.

Çizelge 26 sayfa 182, Çizelge 27 sayfa 182, Çizelge 28 sayfa 183ve Çizelge 29 sayfa 183 , her güvenlik düzeyi tipi için geçerli olan anahtar ayarları birleşimlerini gösterir.

Çizelge 26. Kuyruk yöneticisi düzeyi güvenliği için geçerli güvenlik anahtarı birleşimleri

Birleşikler
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

Çizelge 27. Kuyruk paylaşım grubu düzeyi güvenliği için geçerli güvenlik anahtarı birleşimleri

Birleşikler
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

Çizelge 27. Kuyruk paylaşım grubu düzeyi güvenliği için geçerli güvenlik anahtarı birleşimleri (devamı var)
Birleşikler
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS

Çizelge 28. Kuyruk yöneticisi ve kuyruk paylaşımı grubu düzeyi güvenliği için geçerli güvenlik anahtarı birleşimleri
Birleşikler
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS Hayır, QSG.* tanımlı tanıtımlar
Hayır QMGR.* tanımlı tanıtımlar 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
Anahtar tanımlı olan herhangi bir anahtar için profil yok

Çizelge 29. Other valid security switch combinations that switch both levels of checking **-**.
Birleşikler
qmgr-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS

z/OS *Kaynak düzeyi denetimleri*

Kaynaklara erişimi denetlemek için bir dizi anahtar profili kullanılır. Bir kuyruk yöneticisinde ya da bir kuyruk paylaşım grubunda gerçekleştirilmekte olan bazı durdurma denetimi. Bunlar, belirli kuyruk yöneticileri olup olmadığını denetleyebilen tanıtımlar tarafından geçersiz kılınabilir.

Çizelge 30 sayfa 184 , IBM MQ kaynaklarına erişimi denetlemek için kullanılan anahtar profillerini gösterir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun bir parçasıysa ve kuyruk yöneticisi ve kuyruk paylaşım grubu güvenliği etkinse, bir YES.* kullanabilirsiniz. Kuyruk paylaşım grubu düzeyi profillerini geçersiz kılmak için anahtar profili ve belirli bir kuyruk yöneticisi için özel olarak güvenliği açın.

Bazı tanıtımlar hem kuyruk yöneticileri hem de kuyruk paylaşım grupları için geçerlidir. Bunlar önekli *hlq* dizgisidir ve uygulanabilir olduğu şekilde kuyruk paylaşım grubunuzun ya da kuyruk yöneticinizin adını değiştirmelisiniz. *qmgr-adı* başında önek olarak gösterilen tanıtım adları, kuyruk yöneticisi tarafından geçersiz kılınan tanıtımlardır; kuyruk yöneticinizin adının yerine geçmeniz gerekir.

Çizelge 30. Kaynak denetimi için profilleri değiştir

Denetlenen kaynak denetimi tipi	**Anahtar profili adı**	**Belirli bir kuyruk yöneticisine ilişkin tanıtımı geçersiz kıl**
Bağlantı güvenliği	hlq.NO.CONNECT.CHECKS	qmgr-name.YES.CONNECT.CHECKS
Kuyruk güvenliği	hlq.NO.QUEUE.CHECKS	qmgr-name.YES.QUEUE.CHECKS
Süreç güvenliği	hlq.NO.PROCESS.CHECKS	qmgr-name.YES.PROCESS.CHECKS
Ad listesi güvenliği	hlq.NO.NLIST.CHECKS	qmgr-name.YES.NLIST.CHECKS
Bağlam güvenliği	hlq.NO.CONTEXT.CHECKS	qmgr-name.YES.CONTEXT.CHECKS
Diğer kullanıcı güvenliği	hlq.NO.ALTERNATE.USER.CHECKS	qmgr-name.YES.ALTERNATE.USER.CHECKS
Komut güvenliği	hlq.NO.CMD.CHECKS	qmgr-name.YES.CMD.CHECKS
Komut kaynağı güvenliği	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS
Konu güvenliği	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
Not: hlq.NO. * * gibi genel anahtar profilleri. * * IBM MQtarafından yoksayılır		

Örneğin, QSG3 kuyruk yöneticisinde bulunan QM01kuyruk yöneticisinde süreç güvenlik denetimlerini gerçekleştirmek istiyorsanız, ancak gruptaki diğer kuyruk yöneticilerinden herhangi birinde süreç güvenliği denetimlerini gerçekleştirmek istemiyorsanız, aşağıdaki anahtar profillerini tanımlayın:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Kuyruk paylaşım grubundaki tüm kuyruk yöneticilerinde (QM02dışında) gerçekleştirilen kuyruk güvenliği denetimlerine sahip olmak istiyorsanız, aşağıdaki anahtar tanıtımını tanımlayın:

```
QM02.NO.QUEUE.CHECKS
```

(Bir tanıtım tanımlanmadıysa, denetimler otomatik olarak etkinleştirildiğinden, kuyruk paylaşım grubu için bir profil tanımlamanız gerekmez.)

z/OS *Anahtarların tanımlanmasını gösteren bir örnek*

Farklı IBM MQ altsistemlerinin farklı güvenlik gereksinimleri vardır. Bu gereksinimler, farklı anahtar profilleri kullanılarak uygulanabilir.

Dört IBM MQ altsistemi tanımlanmıştır:

- MQP1 (üretim sistemi)
- MQP2 (bir üretim sistemi)
- MQD1 (bir geliştirme sistemi)
- MQT1 (bir sınama sistemi)

Tüm dört kuyruk yöneticisi, QS01kuyruk paylaşım grubu üyesidir. Tüm IBM MQ RACF sınıfları tanımlanmıştır ve etkinleştirilir.

Bu altsistemlerde farklı güvenlik gereksinimleri vardır:

- Üretim sistemleri, her iki sistemde de kuyruk paylaşımı grubu düzeyinde etkin olmak için tam IBM MQ güvenlik denetimi gerektirir.

  Bu işlem, aşağıdaki profili belirterek gerçekleştirilir:

  ```
  RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
  ```

  Kuyruk paylaşımı grubu, kuyruk paylaşım grubundaki tüm kuyruk yöneticilerine ilişkin kuyruk paylaşımı grubu düzeyini belirler. Bu sistemler için her şeyi denetlemek istediğinizde, üretim kuyruğu yöneticileri için diğer anahtar profillerini tanımlamanıza gerek yoktur.
- Test kuyruğu yöneticisi MQT1 aynı zamanda tam güvenlik denetimi gerektirir. Ancak, bu durumu daha sonra değiştirmek isteyebileceğiniz için, kuyruk yöneticisi düzeyinde güvenlik tanımlanabilir; böylece, kuyruk paylaşım grubunun diğer üyelerini etkilemeden bu kuyruk yöneticisine ilişkin güvenlik ayarlarını değiştirebilirsiniz.

  Bu, MQT1 için NO.QSG.CHECKS tanıtımının aşağıdaki gibi tanımlanarak gerçekleştirilir:

  ```
  RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
  ```
- Geliştirme kuyruk yöneticisi MQD1 , kuyruk paylaşım grubunun geri kalanından farklı güvenlik gereksinimlerine sahiptir. Yalnızca bağlantı ve kuyruk güvenliğinin etkin olmasını gerektirir.

  Bu işlem, bu kuyruk yöneticisi için bir `MQD1.YES.QMGR.CHECKS` tanıtımı tanımlanarak ve sonra denetlenmesi gerekmeyen kaynaklara ilişkin güvenlik denetimini kapatmak için aşağıdaki tanıtımları tanımlayarak gerçekleştirilir:

  ```
  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
  ```

Kuyruk yöneticisi etkin olduğunda, DISPLAY SECURITY MQSC komutunu kullanarak yürürlükteki güvenlik ayarlarını görüntüleyebilirsiniz.

MQADMIN sınıfındaki uygun anahtar tanıtımını tanımlayarak ya da silerek kuyruk yöneticisi çalışırken anahtar ayarlarını da değiştirebilirsiniz. Anahtar ayarlarında yapılan değişiklikleri etkin kılmak için, MQADMIN sınıfı için REFRESH SECURITY komutunu vermelisiniz.

DISPLAY SECURITY ve REFRESH SECURITY komutlarının kullanılmasıyla ilgili ayrıntılar için “z/OSüzerinde kuyruk yöneticisi güvenliği yenileniyor” sayfa 238 konusuna bakın.

z/OS IBM MQ kaynaklarına erişimi denetlemek için kullanılan profiller

Tanımlanmış olabilecek anahtar profillerine ek olarak, IBM MQ kaynaklarına erişimi denetlemek için RACF profillerini tanımlamalısınız. Bu konu derlemi, farklı IBM MQ kaynağı tiplerine ilişkin RACF tanıtımlarıyla ilgili bilgileri içerir.

Belirli bir güvenlik denetimi için tanımlanmış bir kaynak tanıtımınız yoksa ve bir kullanıcı, bu denetimi yapmayı gerektirecek bir istek yayınlarsa, IBM MQ erişimi reddeder. Devre dışı bıraktığınız güvenlik anahtarlarıyla ilgili güvenlik tipleri için profilleri tanımlamanıza gerek yoktur.

z/OS *Bağlantı güvenliği için tanıtımlar*

If connection security is active, you must define profiles in the MQCONN class and permit the necessary groups or user IDs access to those profiles, so that they can connect to IBM MQ.

Bir bağlantının yapılabilmesini sağlamak için, kullanıcılara uygun tanıtıma RACF READ erişimi vermeniz gerekir. (Kuyruk yöneticisi düzeyi tanıtımı yoksa ve kuyruk yöneticinizin bir kuyruk paylaşım grubunun üyesi olması durumunda, güvenlik bunu yapmak üzere ayarlanmışsa, kuyruk paylaşım grubu düzeyinde tanıtımlara karşı denetimler yapılmış olabilir.)

Bir kuyruk yöneticisi adı ile nitelenmiş bir bağlantı tanıtımı, belirli bir kuyruk yöneticisine erişimi denetler ve bu tanıtıma erişim yetkisi verilen kullanıcılar o kuyruk yöneticisine bağlanabilir. Kuyruk paylaşım grubu adına sahip bir bağlantı tanıtımı, o bağlantı tipine ilişkin kuyruk paylaşım grubu içindeki tüm kuyruk yöneticilerine erişimi denetler. Örneğin, `QS01.BATCH` erişimi olan bir kullanıcı, kuyruk yöneticisi düzeyi tanıtımı tanımlanmamış QS01 kuyruk paylaşım grubundaki herhangi bir kuyruk yöneticisiyle toplu iş bağlantısı kullanabilir.

Not:

1. Farklı güvenlik istekleri için denetlenen kullanıcı kimlikleriyle ilgili bilgi için bkz. “z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri” sayfa 227.
2. Bağlantı sırasında kaynak düzeyinde güvenlik (RESEFIL) denetimleri de yapılır. Ayrıntılar için bkz. “RESVELL güvenlik profili” sayfa 221.

IBM MQ güvenliği aşağıdaki farklı bağlantı tiplerini tanır:

- Toplu (ve toplu iş tipi) bağlantılarda şunlar yer alır:
  - z/OS toplu işleri
  - TSO uygulamaları
  - USS oturum açma bilgileri
  - Db2 saklı yordamlar
- CICS bağlantılar
- Denetim ve uygulama işleme bölgelerindenIMS bağlantıları
- IBM MQ kanalı başlatıcısı

z/OS *Toplu iş bağlantıları için bağlantı güvenliği profilleri*

Toplu iş tipi bağlantılarını denetlemek için kullanılan tanıtımlar, kuyruk yöneticisi ya da kuyruk paylaşım grubu adından ve ardından *BATCH*sözcüğünün izlediği bir gruplardan oluşur. Bağlantı tanıtımıyla ilişkilendirilen bağlantı adresi alanı READ (Okuma) erişimiyle ilişkili kullanıcı kimliğini verin.

Toplu iş ve toplu iş tipi bağlantılarını denetlemek için kullanılan profiller şu formu alır:

```
hlq.BATCH
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir. Hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ , önekli bir profil için kuyruk yöneticisi adı önekli olarak denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar. Her iki profili de bulamazsa, bağlantı isteği başarısız olur.

Toplu ya da toplu iş tipi bağlantı istekleri için, bağlantı tanıtımıyla ilişkili kullanıcı kimliğinin bağlantı tanıtımlarına erişmesine izin vermelisiniz. Örneğin, aşağıdaki RACF komutu, CONNTQM1 grubundaki kullanıcıların kuyruk yöneticisine bağlanmalarına izin verir TQM1; bu kullanıcı kimliklerinin toplu ya da toplu iş tipi bağlantılarını kullanmalarına izin verilir.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

z/OS *Yerel olarak bağlı uygulamalarda **CHCKLOCL** ' in kullanılması*

CHCKLOCL yalnızca, BATCH bağlantıları yoluyla yapılan ve CICS ya da IMS' tan yapılan bağlantılar için geçerli olmayan bağlantılara uygulanır. Kanal başlatıcısından yapılan bağlantılar **CHCKCLNT**tarafından denetlenir.

Genel Bakış

If you want to configure your z/OS queue manager to mandate user ID and password checking for some, but not all, of your locally bound applications, you need to do some additional configuration.

Bunun nedeni, **CHCKLOCL** (*REQUIREND*) yapılandırıldıktan sonra, MQCONN API çağrısını kullanan eski toplu iş uygulamalarının kuyruk yöneticisine bağlanmayışıdır.

Yalnızca z/OS için, özel olarak tanımlanmış kullanıcı kimlikleri için genel CHCKLOCL (REQUIRALLY) yapılandırmasını CHCKLOCL (isteğe bağlı) olarak indirgemek için bir adres alanının bağlantı güvenliği temel alınarak daha büyük bir mekanizma kullanılabilir. Kullanılan mekanizma, aşağıdaki metinde bir örn. örnek olarak tanımlanır.

CHCKLOCL 'ta (*REQUIREMVE*) yalnızca HERKESTEN daha fazla ayrıntı düzeyine izin vermek için,connectingbağlantı tanıtımlarıyla ilişkili kullanıcı kimliğinin erişim düzeyini, MQCONN sınıfındaki `hlq.batch` bağlantı tanıtımlarıyla değiştirdiğiniz şekilde, **CHCKLOCL** ' u aynı şekilde değiştirdiniz.

Adres alanı kullanıcı kimliğinin yalnızca okuma erişimi varsa, bu değer, bağlanmak için gereken en küçük değer olan **CHCKLOCL** yapılanışındaki yazıldığı gibi geçerlidir.

Adres alanı kullanıcı kimliğinin UPDATE erişimi (ya da üstü) varsa, **CHCKLOCL** yapılandırması *İSTEKLERI* kipiyle çalışır. Yani, bir kullanıcı kimliği ve parola belirtmeniz gerekmez, ancak bu durumda, kullanıcı kimliği ve parola geçerli bir çift olmalıdır.

Connection security already configured for your z/OS queue manager

z/OS kuyruk yöneticiniz için yapılandırılmış bağlantı güvenliğiniz varsa ve **CHCKLOCL** (*REQUIREND*) WAS ' ı yerel olarak bağlı olan uygulamalara uygulamak istiyorsanız ve başka bir kullanıcı yoksa, aşağıdaki adımları gerçekleştiriniz:

1. Yapılanışınız olarak **CHCKLOCL** (*OPTIONAL*) ile başlayın. Bu, sağlanan herhangi bir kullanıcı kimliği ve parolasının geçerlilik için denetlendiği, ancak zorunlu olmadığı anlamına gelir.
2. Şu komutu vererek bağlantı güvenliği profillerine erişimi olan tüm kullanıcıları listele:

   ```
   RLIST MQCONN MQ23.BATCH AUTHUSER
   ```

   Bu komut görüntülenir; örneğin:

   ```
   CLASS    NAME
   -----    ----
   MQCONN   MQ23.BATCH

   USER     ACCESS  ACCESS COUNT
   ----     ------  ------ -----
   JOHNDOE  READ    000009
   JDOE1    READ    000003
   WASUSER  READ    000000
   ```

3. Okuma erişimine sahip olarak listelenen her kullanıcı kimliği için erişimi değiştirin.

   ```
   UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
   ```

4. IBM MQ yapılandırmasını **CHCKLOCL** olarak güncelleyin (*REQUIREND*).

   `MQ23.BATCH` ' a UPDATE erişimi birleşimi ve yürürlükteki ayar, **CHCKLOCL** (*ISTISEL*) kullandığınız anlamına gelir.
5. Şimdi, **CHCKLOCL** (*REQUIREND*) davranışını belirli bir kullanıcı kimliğine (örneğin, WASUSER) uygulayın; böylece, o bölgeden gelen tüm bağlantıların bir kullanıcı kimliği ve parola sağlaması gerekir.

   Bu işlemi, aşağıdaki komutu girerek, daha önce yaptığınız değişikliği tersine çevirerek gerçekleştirin:

   ```
   PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
   ```

z/OS kuyruk yöneticiniz için bağlantı güvenliği yapılandırılmadı

Bu durumda, aşağıdakileri yapmak gerekir:

1. MQCONN sınıfında `hlq.BATCH` için bağlantı tanıtımları yaratın ve şu komutu verin:

```
RDEFINE MQCONN MQ23.BATCH UACC(NONE)
```

2. Kuyruk yöneticisine toplu bağlantı oluşturan tüm kullanıcı kimliklerini, bu tanıtıma ilişkin UPDATE (güncelleme) erişimine sahip olacak şekilde yetkilendirin. Bu işlem, bağlantı sırasında kullanıcı kimliği ve parola için **CHCKLOCL** (*REQUIREND*) gereksinimini atlıyor.

   Komutu şu komutu vererek yapın:

```
PERMIT MQ23.BATCH CLASS(MQCONN)ID(JOHNDOE) ACCESS(UPDATE)
```

   Bunlar arasında kullanıcı kimlikleri bulunur:

   a. CSQUTIL, ISPF panoları ve yerel olarak bağlı diğer araçlar için kullanılır.

   b. Kuyruk yöneticisiyle bağlantı gibi toplu iş ile ilişkilendirilir. Örneğin, Advanced Message Security, IBM Integration Bus, Db2 saklanmış yordamları, USS ve TSO kullanıcıları ve Java uygulamaları gibi düşünün.

3. Aşağıdaki komutu girerek, kuyruk yöneticisine ilişkin anahtar tanıtımını silin:

```
hlq.NO.CONNECT.CHECKS
```

4. Şimdi, **CHCKLOCL** (*REQUIREND*) davranışını belirli bir kullanıcı kimliğine (örneğin, WASUSER) uygulayın; böylece, o bölgeden gelen tüm bağlantıların bir kullanıcı kimliği ve parola sağlaması gerekir.

   Bu işlemi, aşağıdaki komutu girerek, daha önce yaptığınız değişikliği tersine çevirerek gerçekleştirin:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS *CICS bağlantıları için bağlantı güvenliği profilleri*

CICS bağlantılarını denetleme profilleri, kuyruk yöneticisi ya da kuyruk paylaşım grubu adından ve ardından *CICS* sözcüğünün ardından oluşturulur. Give the user ID associated with the CICS address space READ access to the connection profile.

Profiles for checking connections from CICS take the form:

```
hlq.CICS
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir. Hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ , önekli bir profil için kuyruk yöneticisi adı önekli olarak denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar. Herhangi bir tanıtım bulamazsa, bağlantı isteği başarısız olur

CICSile bağlantı istekleri için, bağlantı tanıtımına yalnızca CICS adres alanı kullanıcı kimliği erişimine izin vermeniz gerekir.

Örneğin, aşağıdaki RACF komutları CICS adres alanı kullanıcı kimliği KCBCICS ' in kuyruk yöneticisine (TQM1:) bağlanmasına olanak sağlar.

```
RDEFINE MQCONN TQM1.CICS UACC(NONE)
PERMIT TQM1.CICS CLASS(MQCONN) ID(KCBCICS) ACCESS(READ)
```

z/OS *IMS bağlantıları için bağlantı güvenliği profilleri*

IMS bağlantılarını denetleme profilleri, kuyruk yöneticisi ya da kuyruk paylaşım grubu adından ve ardından *IMS* sözcüğünün ardından oluşturulur. IMS denetim olanağına ve bağımlı bölge kullanıcı kimliklerini, bağlantı tanıtımına okuma erişimi verin.

Profiles for checking connections from IMS take the form:

```
hlq.IMS
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir. Hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ , önekli bir profil için kuyruk yöneticisi adı önekli olarak denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar. Herhangi bir tanıtım bulamazsa, bağlantı isteği başarısız olur

IMStarafından yapılan bağlantı istekleri için, IMS denetimi ve bağımlı bölge kullanıcı kimliklerine ilişkin bağlantı tanıtılmasına erişim izni verin.

Örneğin, aşağıdaki RACF komutları aşağıdaki komutlara izin verir:

- Kuyruk yöneticisine (TQM1) bağlanmak için IMS bölgesi kullanıcı kimliği (IMSREG).
- BMPGRP grubundaki kullanıcılar BMP işlerini göndersin.

```
RDEFINE MQCONN TQM1.IMS UACC(NONE)
PERMIT TQM1.IMS CLASS(MQCONN) ID(IMSREG,BMPGRP) ACCESS(READ)
```

z/OS *Kanal başlatıcısı için bağlantı güvenliği profilleri*

Kanal başlatıcısından gelen bağlantıları denetlemek için kullanılan tanıtımlar, kuyruk yöneticisi ya da kuyruk paylaşım grubu adından ve ardından *CHIN*sözcüğünün izlediği bir tanıtımdan oluşur. Kanal başlatıcı tarafından kullanılan kullanıcı kimliğine, bağlantı tanıtımına görev adresi alanı okuma erişimi başlatmasını sağlar.

Kanal başlatıcısından gelen bağlantıları denetlemek için kullanılan tanıtımlar aşağıdaki formu alır:

```
hlq.CHIN
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir. Hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ , önekli bir profil için kuyruk yöneticisi adı önekli olarak denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar. Herhangi bir tanıtım bulamazsa, bağlantı isteği başarısız olur

Kanal başlatıcı tarafından yapılan bağlantı istekleri için, kanal başlatıcısı tarafından kullanılan kullanıcı kimliğine ilişkin bağlantı tanıtılmasına ilişkin erişim tanımlamayı tanımlayın.

Örneğin, aşağıdaki RACF komutları, kullanıcı kimliği DQCTRL ile çalışan kanal başlatıcı adres alanının kuyruk yöneticisine (TQM1:) bağlanmasına olanak sağlar.

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

z/OS *Kuyruk güvenliğine ilişkin profiller*

Kuyruk güvenliği etkinse, uygun sınıflarda tanıtımlar tanımlamanız ve bu tanıtımlara gereken grupların ya da kullanıcı kimliklerinin erişmesine izin vermeniz gerekir. Kuyruk güvenliği tanıtımları, kuyruk yöneticisi ya da kuyruk paylaşım grubunun ve açılacak kuyruğun adını taşır.

Kuyruk güvenliği etkinse, aşağıdakileri yapmanız gerekir:

- Büyük harfli tanıtımlar kullanılıyorsa, tanıtımları **MQQUEUE** ya da **GMQQUEUE** sınıflarında tanımlayın.
- Büyük ve küçük harf karışık tanıtımlar kullanılıyorsa, **MXQUEUE** ya da **GMXQUEUE** sınıflarındaki tanıtımları tanımlayın.
- Gerekli grupların ya da kullanıcı kimliklerinin, kuyrukları kullanan IBM MQ API isteklerini yayınlayabilmesi için bu profillere erişmesine izin verin.

Kuyruk güvenliğine ilişkin profiller şu formu alır:

```
hlq.queuename
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir ve `queuename` , `MQOPEN` ya da `MQPUT1` çağrısındaki nesne tanımlayıcısında belirtildiği şekilde, açılmakta olan kuyruğun adıdır.

Kuyruk yöneticisi adı öneki eklenen bir tanıtım, o kuyruk yöneticisindeki tek bir kuyruğa erişimi denetler. Kuyruk paylaşım grubu adı öneki eklenen bir tanıtım, kuyruk paylaşım grubu içindeki tüm kuyruk yöneticilerine bir ya da daha fazla kuyruk adı içeren bir ya da daha fazla kuyruğa erişimi ya da grup içindeki herhangi bir kuyruk yöneticisi tarafından paylaşılan bir kuyruğa erişimi denetler. Bu erişim, söz konusu kuyruk yöneticisinde o kuyruk için bir kuyruk yöneticisi düzeyi tanıtımı tanımlanarak, tek bir kuyruk yöneticisinde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adının öneki olan bir tanıtımı denetler. Bir tanıtım bulamazsa, kuyruk paylaşım grubu adının öneki olan bir tanıtımı arar.

Paylaşılan kuyruklar kullanıyorsanız, kuyruk paylaşım grubu düzeyinde güvenlik kullanmanız önerilir.

Kuyruk adı bir diğer adla ya da model kuyruğuyla aynı olduğunda kuyruk güvenliğinin nasıl çalıştığına ilişkin ayrıntılar için z/OS, bkz. “Diğer ad kuyruklarına ilişkin dikkat” sayfa 192 ve “Model kuyruklarında dikkate alınması gerekenler” sayfa 193 .

Bir kuyruğu açmak için gereken RACF erişimi, belirtilen `MQOPEN` ya da `MQPUT1` seçeneklerine bağlıdır. Birden çok `MQOO_ *` ve `MQPMO_ *` seçeneği kodlanmışsa, kuyruk güvenliği denetimi gereken en yüksek RACF yetkisi için gerçekleştirilir.

Çizelge 31. MQOPEN ya da MQPUT1 çağrılarını kullanarak kuyruk güvenliği için erişim düzeyleri

MQOPEN ya da MQPUT1 seçeneği	**RACF hlq.queuename için gereken erişim düzeyi**
MQOO_GÖZ AT	READ
MQOO_INQUIRE	READ
MQOO_BIND_ *	GÜNCELLE
MQOO_INPUT_ *	GÜNCELLE
MQOO_OUTPUT ya da MQPUT1	GÜNCELLE

Çizelge 31. MQOPEN ya da MQPUT1 çağrılarını kullanarak kuyruk güvenliği için erişim düzeyleri (devamı var)

MQOPEN ya da MQPUT1 seçeneği	**RACF hlq.queuename için gereken erişim düzeyi**
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	GÜNCELLE
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	GÜNCELLE
MQOO_SAVE_ALL_CONTEXT	GÜNCELLE
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	GÜNCELLE
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	GÜNCELLE
MQOO_SET	Çeviri

Örneğin, IBM MQ kuyruk yöneticisi QM77'de, RACF PAYGRP grubundaki tüm kullanıcı kimliklerine, adları' PAY ' ile başlayan tüm kuyruklardan ileti alma ya da tüm kuyruklara ileti gönderme erişimi verilir. Bunu şu RACF komutlarını kullanarak yapabilirsiniz:

```
RDEFINE MQQUEUE QM77.PAY.** UACC(NONE)
PERMIT QM77.PAY.** CLASS(MQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Ayrıca, PAYGRP grubundaki tüm kullanıcı kimliklerinin, PAY adlandırma kuralına uymayan iletileri kuyruklara koymak için erişimi olmalıdır. Örneğin:

```
REQUEST_QUEUE_FOR_PAYROLL
SALARY.INCREASE.SERVER
REPLIES.FROM.SALARY.MODEL
```

GMQQUEUE sınıfında bu kuyruklar için profiller tanımlayarak ve bu sınıfa aşağıdaki gibi erişim vererek bunu yapabilirsiniz:

```
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)
```

Not:

1. Bir uygulamanın bir kuyruk güvenliği tanıtımına ilişkin RACF erişim düzeyi değiştirilirse, değişiklikler yalnızca o kuyruk için elde edilen yeni nesne tanıtıcıları (yeni MQOPEN ' ler) için geçerli olur. Değişiklik sırasında var olan bu tanıtıcıları, kuyruğa var olan erişimlerini korur. Bir uygulamanın, varolan erişim düzeyi yerine, kuyrukta değiştirilen erişim düzeyini kullanması gerekiyorsa, değişikliği gerektiren her nesne tanıtıcısı için kuyruğu kapatıp yeniden açması gerekir.
2. Örnekte, QM77 kuyruk yöneticisi adı bir kuyruk paylaşım grubunun adı da olabilir.

Belirlenen açma seçeneklerine ve etkin güvenlik tiplerine bağlı olarak, kuyruk açıldığında diğer güvenlik denetimi tipleri de oluşabilir. z/OS Ayrıca bkz. “Bağlam güvenliğine ilişkin profiller” sayfa 206 ve “Diğer kullanıcı güvenliği için profiller” sayfa 205. Kuyruk, bağlam ve diğer kullanıcı güvenliğinin tümü

etkin olduğunda gereken açma seçeneklerini ve güvenlik yetkisini gösteren bir özet tablo için bkz. Çizelge 36 sayfa 197.

Yayınlama/abone olma özelliğini kullanıyorsanız, aşağıdakileri göz önünde bulundurmanız gerekir. Bir MQSUB isteği işlendiğinde, isteği yapan kullanıcı kimliğinin iletileri hedef IBM MQ kuyruğuna koymak için gerekli erişime ve IBM MQ konusuna abone olmak için gerekli erişime sahip olduğundan emin olmak için bir güvenlik denetimi gerçekleştirilir.

Çizelge 32. MQSUB çağrısı kullanılarak kuyruk güvenliği için erişim düzeyleri

MQSUB seçeneği	**RACF hlq.queuename için gereken erişim düzeyi**
MQSO_ALTER, MQSO_CREATE ve MQSO_RESUME	GÜNCELLE

Not:

1. `hlq.queuename` , yayınların hedef kuyruğudur. Bu bir yönetilen kuyruk olduğunda, yönetilen kuyruk ve yaratılan dinamik kuyruk için kullanılacak uygun model kuyruğuna erişmeniz gerekir.
2. Abonelikleri yapan kullanıcılar ile hedef kuyruktan yayınları alan kullanıcılar arasında ayrım yapmak istiyorsanız, MQSUB API çağrısında sağladığınız hedef kuyruk için bu tür bir teknik kullanabilirsiniz.

z/OS *Diğer ad kuyruklarına ilişkin dikkat*

Bir diğer ad kuyruğu için bir MQOPEN ya da MQPUT1 çağrısı yayınlarken, IBM MQ , çağrıdaki nesne tanımlayıcısında (MQOD) belirtilen kuyruk adına karşı bir kaynak denetimi yapar. Kullanıcının hedef kuyruk adına erişmesine izin verilip verilmediğini denetmez.

For example, an alias queue called PAYROLL.REQUEST resolves to a target queue of PAY.REQUEST. If queue security is active, you need only be authorized to access the queue PAYROLL.REQUEST. No check is made to see if you are authorized to access the queue PAY.REQUEST.

z/OS *MQGET ve MQPUT isteklerini ayırt etmek için diğer ad kuyruklarının kullanılması*

Bir erişim düzeyinde kullanılabilir MQI çağrıları aralığı, bir kuyruğa erişimi yalnızca **MQPUT** çağrısına ya da yalnızca **MQGET** çağrısına izin verecek şekilde kısıtlamak istiyorsanız soruna neden olabilir. Bir kuyruk, bu kuyruğa çözülecek iki diğer ad tanımlanarak korunabilir: biri, uygulamaların kuyruktan ileti almasını, diğeri de uygulamaların kuyruğa ileti koymasını sağlar.

Aşağıdaki metin, kuyruklarınızı IBM MQiçin nasıl tanımlayabileceğinize ilişkin bir örnek sağlar:

```
DEFINE QLOCAL(MUST_USE_ALIAS_TO_ACCESS) GET(ENABLED)
       PUT(ENABLED)

DEFINE QALIAS(USE_THIS_ONE_FOR_GETS) GET(ENABLED)
       PUT(DISABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)

DEFINE QALIAS(USE_THIS_ONE_FOR_PUTS) GET(DISABLED)
       PUT(ENABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)
```

Aşağıdaki RACF tanımlamalarını da yapmalısınız:

```
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)
```

Daha sonra, hiçbir kullanıcının hlq.MUST_USE_ALIAS_TO_ACCESSkuyruğuna erişimi olmadığından emin olun ve diğer ada uygun kullanıcılara ya da gruplara erişim verin. Bunu aşağıdaki RACF komutlarını kullanarak yapabilirsiniz:

```
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)
```

Bu, GETGRP grubundaki kullanıcı kimliği GETUSER ve kullanıcı kimliklerinin yalnızca USE_THIS_ONE_FOR_GETS; diğer ad kuyruğu aracılığıyla MUST_USE_ALIAS_TO_ACCESS ile ilgili iletileri almasına ve PUTGRP grubundaki kullanıcı kimlikleri ve PUTUSER kullanıcı kimliklerinin iletileri yalnızca USE_THIS_ONE_FOR_PUTS kuyruğuna yerleştirmesine izin verildiği anlamına gelir.

Not:

1. Böyle bir teknik kullanmak istiyorsanız, uygulama geliştiricilerinizi bilgilendirmelisiniz, böylece programlarını uygun şekilde tasarlayabilirler.
2. Abonelikleri yapan kullanıcılar ile yayınları hedef kuyruktan alan kullanıcılar arasında ayrım yapmak istiyorsanız, MQSUB API isteğinde sağladığınız hedef kuyruk için bu tür bir teknik kullanabilirsiniz.

z/OS *Model kuyruklarında dikkate alınması gerekenler*

Bir model kuyruğunu açmak için, hem model kuyruğunu hem de çözdüğü dinamik kuyruğu açabilmelisiniz. Dinamik kuyruklar için, IBM MQ yardımcı programları tarafından kullanılan dinamik kuyruklar da içinde olmak üzere soysal RACF tanıtımlarını tanımlayın.

Bir model kuyruğunu açtığınızda, IBM MQ güvenliği iki kuyruk güvenliği denetimi yapar:

1. Model kuyruğuna erişme yetkiniz var mı?
2. Model kuyruğunun çözümlediği dinamik kuyruğa erişme yetkiniz var mı?

Dinamik kuyruk adı sondaki bir yıldız işareti (*) içeriyorsa, bu * benzersiz bir adla dinamik bir kuyruk yaratmak için IBM MQtarafından oluşturulan bir karakter dizgisiyle değiştirilir. Ancak, bu üretilmiş dizgi de içinde olmak üzere tüm ad, yetki denetlemek için kullanıldığından, bu kuyruklar için soysal profilleri tanımlamanız gerekir.

Örneğin, bir MQOPEN çağrısı, CREDIT.CHECK.REPLY.MODEL ve dinamik kuyruk adı olarak CREDIT.REPLY.* kuyruk yöneticisininde (ya da kuyruk paylaşım grubu) MQSP.

Bunu yapmak için, gereken kuyruk profillerini tanımlamak için aşağıdaki RACF komutlarını yayınlamanız gerekir:

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Ayrıca, bu tanıtımlara kullanıcı erişimine izin vermek için karşılık gelen RACF PERMIT komutlarını da yayınlamanız gerekir.

A typical dynamic queue name created by an MQOPEN is something like CREDIT.REPLY.A346EF00367849A0. Son niteleyicinin kesin değeri tahmin edilemez; bu nedenle, bu tür kuyruk adları için soysal profilleri kullanmanız gerekir.

Bir dizi IBM MQ yardımcı programı, iletileri dinamik kuyruklara yerleştirdi. Aşağıdaki dinamik kuyruk adlarına ilişkin tanıtımları tanımlamanız ve ilgili kullanıcı kimliklerine RACF UPDATE erişimi sağlamanız gerekir (doğru kullanıcı kimlikleri için “z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri” sayfa 227 konusuna bakın):

```
SYSTEM.CSQUTIL.*  (used by CSQUTIL)
SYSTEM.CSQOREXX.* (used by the operations and control panels)
SYSTEM.CSQXCMD.*  (used by the channel initiator when processing CSQINPX)
CSQ4SAMP.*        (used by the IBM MQ supplied samples)
```

Ayrıca, uygulama programlama kopyası üyelerinde varsayılan olarak kullanılan dinamik kuyruk adının kullanımını denetlemek için bir profil tanımlamayı da düşünebilirsiniz. IBM MQtarafından sağlanan kopya defterleri, CSQ. * olan varsayılan bir *DynamicQName*(sayfa adı) içeriyor. Bu, uygun bir RACF tanıtımının oluşturulabilmesini sağlar.

Not: Uygulama programcılarının dinamik kuyruk adı için tek bir * belirlemesine izin verme. Eğer bunu yaparsan, bir Hlq. * * * tanımlamanız gerekir. * MQqueue sınıfındaki tanıtıma ve ona geniş kapsamlı erişim vermeniz gerekir. Bu, bu profilin, daha belirli bir RACF profili olmayan diğer dinamik olmayan kuyruklar için de kullanılabileceği anlamına gelir. Bu nedenle, kullanıcılarınız, erişmelerini istemediğiniz kuyruklara erişim elde edebilirmiş.

z/OS *Kalıcı dinamik kuyruklardaki seçenekleri kapat*

Bir uygulama, başka bir uygulama tarafından yaratılmış kalıcı bir dinamik kuyruk açıyorsa ve daha sonra bu kuyruğu bir MQCLOSE seçeneğiyle silme girişiminde bulunursa, bu girişim yapıldığında fazladan bazı ek güvenlik denetimleri uygulanır.

Çizelge 33. Kalıcı dinamik kuyruklara ilişkin kapatma seçeneklerine ilişkin erişim düzeyleri

MQCLOSE seçeneği	**hlq.queuenameiçin gerekenRACF erişim düzeyi**
MQCO_DELETE	ALTER
MQCO_DELETE_PURGE	ALTER

z/OS *Güvenlik ve uzak kuyruklar*

Bir ileti uzak bir kuyruğa konduğunda, yerel kuyruk yöneticisi tarafından uygulanan kuyruk güvenliği, açıldığı sırada uzak kuyruğun nasıl belirtildiğine bağlıdır.

Aşağıdaki kurallar uygulanır:

1. Uzak kuyruk yerel kuyruk yöneticisininde IBM MQ DEFINE QREMOTE komutu kullanılarak tanımlandıysa, denetlenen kuyruk uzak kuyruğun adıdır. Örneğin, kuyruk yöneticisi MQS1 üzerinde bir uzak kuyruk aşağıdaki gibi tanımlandıysa:

   ```
   DEFINE QREMOTE(BANK7.CREDIT.REFERENCE)
          RNAME(CREDIT.SCORING.REQUEST)
          RQMNAME(BNK7)
          XMITQ(BANK1.TO.BANK7)
   ```

   Bu durumda, BANK7.CREDIT.REFERENCE , MQQUEUE sınıfında tanımlanmalıdır.
2. İsteğe ilişkin *ObjectQMgrName* , yerel kuyruk yöneticisine çözülmezse, denetim, küme kuyruğu adına karşı yapılan denetmenin yapıldığı bir küme kuyruğu dışında, çözülen (uzak) kuyruk yöneticisi adına ilişkin bir güvenlik denetimi gerçekleştirilir.

   For example, the transmission queue BANK1.TO.BANK7 is defined on queue manager MQS1. An MQPUT1 request is then issued on MQS1 specifying *ObjectName* as BANK1.INTERBANK.TRANSFERS and an *ObjectQMgrAd* of BANK1.TO.BANK7. Bu durumda, isteği gerçekleştiren kullanıcının BANK1.TO.BANK7.
3. Bir kuyruğa ilişkin bir MQPUT isteği yapıp yerel kuyruk yöneticisinin diğer adı olarak *ObjectQMgrName* değerini belirtirseniz, güvenlik için yalnızca kuyruk adı denetlenmez, kuyruk yöneticisininse bu adı belirtmez.

İleti uzak kuyruk yöneticisine vardığında, bu ileti ek güvenlik işlemeye tabi olabilir. Daha fazla bilgi için bkz “Uzaktan ileti sistemine ilişkin güvenlik” sayfa 91.

z/OS *Ölü-mektup kuyruğu güvenliği*

Çok sayıda kullanıcının bu kuyruğa ileti koyabilmesi, ancak iletilerin alınması için erişim çok sıkı bir şekilde kısıtlanmış olması gerektiğinden, ölü-mektup kuyruğunda özel noktalar geçerlidir. Bunu, farklı RACF yetkilerine, ölü-mektup kuyruğuna ve bir diğer ad kuyruğuna uygulayarak bunu başarabilirsiniz.

Teslim edilmeyen iletiler, ölü-mektup kuyruğu adı verilen özel bir kuyruğa konabilir. Bu kuyruğun sonunda sona erdirilebilecek hassas verileriniz varsa, yetkisiz kullanıcıların bu verileri almasını istemediğiniz için bunun güvenlik etkilerini dikkate almanız gerekir.

İletilerin her birinin, iletileri ölü harf kuyruğuna yerleştirmesine izin verilmelidir:

- Uygulama programları.
- Kanal başlatıcı adres alanı ve herhangi bir MCA kullanıcı kimliği. (RESLEVEL tanıtımı yoksa ya da kanal kullanıcı kimliklerinin denetleneceği şekilde tanımlandıysa, kanal kullanıcı kimliğinin de, iletileri ölü-mektup kuyruğuna koyma yetkisi de gerekir.)
- CKTI, CICStarafından sağlanan CICS görev başlatıcısı.
- CSQQTRMN, IBM MQtarafından sağlanan IMS tetikleyicisi izleyicisi.

İleti kuyruğundan ileti alabilen tek uygulama, bu iletileri işleyen 'özel' bir uygulama olmalıdır. However, a problem arises if you give applications RACF UPDATE authority to the dead-letter queue for MQPUT s because they can then automatically retrieve messages from the queue using MQGET calls. İşlemleri almak için, 'özel' uygulamalar bile iletileri alamıyorsa, bu kuyruk-çıkış kuyruğunu geçersiz kılamazsınız.

Bu soruna bir çözüm, ölü-mektup kuyruğuna iki düzeyli bir erişim olarak ayarlanıyor. CKTI, ileti kanalı aracısı işlemleri ya da kanal başlatıcı adres alanı ve 'özel' uygulamaların doğrudan erişimi vardır; diğer uygulamalar yalnızca bir diğer ad kuyruğundan yalnızca ölü-mektup kuyruğuna erişebilir. Bu diğer ad, uygulamaların, iletileri ölüme ya da kuyruğa göndermesine izin verecek şekilde tanımlıdır, ancak ileti almalarını sağlar.

Bu, iş şeklinin nasıl çalışacağını.

1. Define the real dead-letter queue with attributes PUT(ENABLED) and GET(ENABLED), as shown in the sample thlqual.SCSQPROC(CSQ4INYG).
2. Ölü-mektup kuyruğu için RACF UPDATE yetkisini aşağıdaki kullanıcı kimliklerine verin:
   - CKTI 'nın ve MCA' ların ya da kanal başlatıcı adres alanının altında çalıştırıldığı kullanıcı kimlikleri.
   - 'Özel' ölü harf kuyruğu işleme uygulaması ile ilişkili kullanıcı kimlikleri.
3. Gerçek ölü harf kuyruğuna çözülen bir diğer ad kuyruğu tanımlayın, ancak diğer ad kuyruğunu şu öznitelikleri verin: PUT (ENABLED) ve GET (DEVRE Dışı). Diğer ad kuyruğuna, ölü harf kuyruğu adıyla aynı kök adını taşıyan bir ad verin, ancak ". PUT" karakterlerini bu sapta ekleyin. Örneğin, ölü-harfli kuyruk adı hlq.DEAD.QUEUE, diğer ad kuyruğu adı hlq.DEAD.QUEUE.PUT.
4. Bir ileti, diğer ad kuyruğunu kullanan bir uygulamaya ileti koymak için kullanılır. Uygulamanızın yapması gereken budur:
   - Gerçek ölü harf kuyruğunun adını alın. To do this, it opens the queue manager object using MQOPEN and then issues an MQINQ to get the dead-letter queue name.
   - Bu ada '.PUT' karakterleri ekleyerek, diğer ad kuyruğunun adını oluşturun; bu durumda, hlq.DEAD.QUEUE.PUT.
   - Diğer ad kuyruğunu açın, hlq.DEAD.QUEUE.PUT.
   - Diğer ad kuyruğuna karşı bir MQPUT komutu vererek, iletiyi gerçek ölü harf kuyruğuna yerleştirin.
5. Uygulama RACF UPDATE yetkisiyle ilişkili kullanıcı kimliğini diğer ad için verin, ancak gerçek ölü harf kuyruğunda erişim (YOK yetkisi) yok. Bu da şu anlama gelir:
   - Uygulama, diğer ad kuyruğunu kullanarak iletileri ölü-mektup kuyruğuna yerleştirebilir.
   - Diğer ad kuyruğu, alma işlemleri için geçersiz kılındığından, uygulama diğer ad kuyruğunu kullanarak iletileri alamıyor ya da başka bir adla ileti alınamıyor.

   Uygulama, doğru RACF yetkisine sahip olduğu için, gerçek ölü harf kuyruğundan ileti alamıyor.

Çizelge 34 sayfa 195 , bu çözümdeki çeşitli katılımcılar için gerekli olan RACF yetkisini özetler.

Çizelge 34. Ölü-mektup kuyruğu ve diğer adı içinRACF yetkisi

İlişkili kullanıcı kimlikleri	**Gerçek ölü harf kuyruğu (hlq.DEAD.QUEUE)**	**Diğer ad ölü harf kuyruğu (hlq.DEAD.QUEUE.PUT)**
MCA ya da kanal başlatıcı adres alanı ve CKTI	GÜNCELLE	YOK

Çizelge 34. Ölü-mektup kuyruğu ve diğer adı içinRACF yetkisi (devamı var)		
İlişkili kullanıcı kimlikleri	**Gerçek ölü harf kuyruğu (hlq.DEAD.QUEUE)**	**Diğer ad ölü harf kuyruğu (hlq.DEAD.QUEUE.PUT)**
'Özel' uygulama (kuyruk-kuyruk işleme için)	GÜNCELLE	YOK
Kullanıcı tarafından yazılan uygulama kullanıcı kimlikleri	YOK	GÜNCELLE

Bu yöntemi kullanırsanız, uygulama, ölü-mektup kuyruğunun ileti uzunluğu üst sınırını (MAXMSGL) belirleyemez. Bunun nedeni, MAXMSGL özniteliğinin bir diğer ad kuyruğundan alınamaması olabilir. Bu nedenle, uygulamanızın ileti uzunluğu üst sınırı 100 MB olduğunu, IBM MQ for z/OS ' un büyüklük üst sınırının desteklendiğini varsaymalıdır. Gerçek ölü-mektup kuyruğu, 100 MB ' lik bir MAXMSGL öznitelikle de tanımlanmalıdır.

Not: Kullanıcı tarafından yazılan uygulama programları olağan durumda, iletileri ölüler kuyruğuna yerleştirmek için diğer kullanıcı yetkisini kullanmaz. Bu, ölü-mektup kuyruğuna erişimi olan kullanıcı kimliklerinin sayısını azaltır.

z/OS *Sistem kuyruğu güvenliği*

Belirli kullanıcı kimliklerinin belirli sistem kuyruklarına erişmesine izin vermek için RACF erişimini ayarlamanız gerekir.

Sistem kuyruklarına IBM MQ' un yan kısımlarından erişilir:

- CSQUTIL yardımcı programı
- İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)
- İşlemler ve denetim panoları
- Kanal başlatıcı adres alanı (Kuyruğa Alınmış Pub/Alt Yardımcı Program da içinde olmak üzere)
- V 9.1.0 MQ Console ve REST APItarafından kullanılan mqweb sunucusu.

Bu çalıştırmanın altındaki kullanıcı kimliklerinin bu kuyruklara RACF erişimi verilmesi gerekir; Çizelge 35 sayfa 196içinde gösterildiği şekilde.

Çizelge 35. IBM MQtarafından sistem kuyruklarına erişmek için gereken erişim					
Sistem kuyruğu	**CSQUTIL**	**CSQ0UTIL**	**mqweb sunucusu**	**İşlemler ve denetim panoları**	**Dağıtılmış kuyruklama için kanal başlatıcısı**
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	-	GÜNCELLE
SYSTEM.ADMIN.COMMAND.QUEUE	-	-	GÜNCELLE	-	-
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	-	ALTER
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	-	GÜNCELLE
SYSTEM.CHANNEL.INITQ	-	-	-	-	GÜNCELLE
SYSTEM.CHANNEL.SYNCQ	-	-	-	-	GÜNCELLE
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	-	ALTER
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	-	GÜNCELLE

Çizelge 35. IBM MQtarafından sistem kuyruklarına erişmek için gereken erişim (devamı var)					
Sistem kuyruğu	**CSQUTIL**	**CSQ0UTIL**	**mqweb sunucusu**	**İşlemler ve denetim panoları**	**Dağıtılmış kuyruklama için kanal başlatıcısı**
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	-	ALTER
SYSTEM.COMMAND.INPUT	GÜNCELLE	-	-	GÜNCELLE	GÜNCELLE
SYSTEM.COMMAND.REPLY.*	-	-	-	-	GÜNCELLE
SYSTEM.COMMAND.REPLY.MODEL	GÜNCELLE	-	-	GÜNCELLE	GÜNCELLE
SYSTEM.CSQOREXX.*	-	-	-	GÜNCELLE	-
SYSTEM.CSQUTIL.*	GÜNCELLE	-	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	-	GÜNCELLE
SYSTEM.HIERARCHY.STATE	-	-	-	-	GÜNCELLE
SYSTEM.INTER.QMGR.CONTROL	-	-	-	-	GÜNCELLE
SYSTEM.INTER.QMGR.PUBS	-	-	-	-	GÜNCELLE
SYSTEM.INTER.QMGR.FANREQ	-	-	-	-	GÜNCELLE
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	GÜNCELLE
SYSTEM.PROTECTION.POLICY.QUEUE	-	Güncelle“ 1” sayfa 197	-	-	READ
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	GÜNCELLE
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	GÜNCELLE
SYSTEM.REST.REPLY.QUEUE	-	-	GÜNCELLE	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	GÜNCELLE

Notlar:

1. Advanced Message Security adres alanı kullanıcısı da bu kuyruk için okuma erişimi gerektirir.

z/OS *API-kaynak güvenliği erişimi için hızlı başvuru*

MQOPEN, **MQPUT1**, **MQSUB**ve **MQCLOSE** seçeneklerinin bir özeti ve farklı kaynak güvenlik tipleri tarafından gerekli erişim.

Çizelge 36. MQOPEN, MQPUT1, MQSUB ve MQCLOSE seçenekleri ve gereken güvenlik yetkisi. Bu **(1)** gibi gösterilen Callouts, bu tabloyu izleyen notlara başvurmaya devam eder.				
	En az RACF erişim düzeyi gerekli			
RACF Sınıf:	**MXKONUSU**	**MQQUEUE ya da MXQUEUE (1)**	**MQADMIN YA DA MXADMIN**	**MQADMIN YA DA MXADMIN**
RACF profili:	**(15 ya da 16)**	**(2)**	**(3)**	**(4)**
MQOPEN seçeneği				
MQOO_SORGULAMA		OKUMA **(5)**	Denetim yok	Denetim yok

Çizelge 36. MQOPEN, MQPUT1, MQSUB ve MQCLOSE seçenekleri ve gereken güvenlik yetkisi. Bu **(1)** gibi gösterilen Callouts, bu tabloyu izleyen notlara başvurmaya devam eder. *(devamı var)*

	En az RACF erişim düzeyi gerekli			
RACF Sınıf:	**MXKONUSU**	**MQQUEUE ya da MXQUEUE (1)**	**MQADMIN YA DA MXADMIN**	**MQADMIN YA DA MXADMIN**
RACF profili:	**(15 ya da 16)**	**(2)**	**(3)**	**(4)**
MQOO_BROWSE		READ	Denetim yok	Denetim yok
MQOO_INPUT_ *		GÜNCELLE	Denetim yok	Denetim yok
MQOO_SAVE_ALL_CONTEXT **(6)**		GÜNCELLE	Denetim yok	Denetim yok
MQOO_OUTPUT (USAGE = NORMAL) **(7)**		GÜNCELLE	Denetim yok	Denetim yok
MQOO_PASS_IDENTITY_CONTEXT **(8)**		GÜNCELLE	READ	Denetim yok
MQOO_PASS_ALL_CONTEXT **(8) (9)**		GÜNCELLE	READ	Denetim yok
MQOO_SET_IDENTITY_CONTEXT **(8) (9)**		GÜNCELLE	GÜNCELLE	Denetim yok
MQOO_SET_ALL_CONTEXT **(8) (10)**		GÜNCELLE	CONTROL	Denetim yok
MQOO_OUTPUT (KULLANIM (XMITQ) **(11)**		GÜNCELLE	CONTROL	Denetim yok
MQOO_OUTPUT (konu nesnesi)	GüNCELLE **(16)**			
MQOO_OUTPUT (diğer ad kuyruğu konu nesnesi)	GüNCELLE **(16)**	GÜNCELLE		
MQOO_SET		ALTER	Denetim yok	Denetim yok
MQOO_ALTERNATE_USER_AUTHORITY		**(12)**	**(12)**	GÜNCELLE
MQPUT1 seçeneği				
Normal bir kuyruk yerleştirin **(7)**		GÜNCELLE	Denetim yok	Denetim yok
MQPMO_PASS_IDENTITY_CONTEXT		GÜNCELLE	READ	Denetim yok
MQPMO_PASS_ALL_CONTEXT		GÜNCELLE	READ	Denetim yok
MQPMO_SET_IDENTITY_CONTEXT		GÜNCELLE	GÜNCELLE	Denetim yok
MQPMO_SET_ALL_CONTEXT		GÜNCELLE	CONTROL	Denetim yok
MQOO_OUTPUT İletim kuyruğuna konun **(11)**		GÜNCELLE	CONTROL	Denetim yok
MQOO_OUTPUT (konu nesnesi)	GüNCELLE **(16)**			
MQOO_OUTPUT (diğer ad kuyruğu konu nesnesi)	GüNCELLE **(16)**	GÜNCELLE		
MQPMO_ALTERNATE_USER_AUTHORITY		**(13)**	**(13)**	GÜNCELLE
MQCLOSE seçeneği				
MQCO_DELETE **(14)**		ALTER	Denetim yok	Denetim yok
MQCO_DELETE_PURGE **(14)**		ALTER	Denetim yok	Denetim yok

Çizelge 36. MQOPEN, MQPUT1, MQSUB ve MQCLOSE seçenekleri ve gereken güvenlik yetkisi. Bu **(1)** gibi gösterilen Callouts, bu tabloyu izleyen notlara başvurmaya devam eder. *(devamı var)*

	En az RACF erişim düzeyi gerekli			
RACF Sınıf:	**MXKONUSU**	**MQQUEUE ya da MXQUEUE (1)**	**MQADMIN YA DA MXADMIN**	**MQADMIN YA DA MXADMIN**
RACF profili:	**(15 ya da 16)**	**(2)**	**(3)**	**(4)**
MQCO_REMOVE_SUB	ALTER **(15)**			
MQSUB seçeneği				
MQSO_CREATE	ALTER **(15)**	**(17)**	**(18)**	
MQSO_ALTER	ALTER **(15)**	**(17)**	**(18)**	
MQSO_RESUME	OKUMA **(15)**	**(17)**	Denetim yok	
MQSO_ALTERNATE_USER_AUTHORITY				GÜNCELLE
MQSO_SET_IDENTITY_CONTEXT			**(18)**	

Not:

1. Bu seçenek kuyruklar için sınırlandırılmaz. Ad listeleri için MQNLIST ya da MXNLIST sınıfını ve süreçlere ilişkin MQPROC ya da MXPROC sınıfını kullanın.
2. RACF profilini kullanın: hlq.resourcename
3. RACF profilini kullanın: hlq.CONTEXT.queuename
4. RACF profilini kullanın: hlq.ALTERNATE.USER. `alternateuserid`

   `alternateuserid` , nesne tanımlayıcısının *AlternateUserId* alanında belirtilen kullanıcı kimliğidir. Bir kullanıcı kimliğinin yalnızca ilk 8 karakterinin kullanıldığı diğer denetimlerden farklı olarak, bu denetim için en çok 12 karakterlik bir *AlternateUserId* alanının kullanıldığını unutmayın.
5. Sorgular için kuyruk yöneticisi açılırken herhangi bir denetim yapılmadı.
6. MQOO_INPUT_ * belirtilmeli olarak belirlenmelidir. Bu, yerel, model ya da diğer ad kuyruğu için geçerlidir.
7. Bu denetim, **Usage** kuyruk özniteliği MQUS_NORMAL ve aynı zamanda bir diğer ad ya da uzak kuyruk için (bağlı kuyruk yöneticisininde tanımlı) bir yerel ya da model kuyruğu için yapılır. If the queue is a remote queue that is opened specifying an *ObjectQMgrName* (not the name of the connected queue manager) explicitly, the check is carried out against the queue with the same name as *ObjectQMgrName* (which must be a local queue with a **Usage** queue attribute of MQUS_TRANSMISSION).
8. MQOO_OUTPUT da belirtilmeli.
9. MQOO_PASS_IDENTITY_CONTEXT, bu seçeneğin yanı sıra örtük olarak da belirtilir.
10. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT VE MQOO_SET_IDENTITY_CONTEXT, bu seçeneğin yanı sıra örtük olarak da belirtilir.
11. This check is done for a local or model queue that has a **Usage** queue attribute of MQUS_TRANSMISSION, and is being opened directly for output. Uzak bir kuyruk açılıyorsa, bu değer uygulanmaz.
12. En az bir MQOO_SORGULAMASI, MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT ya da MQOO_SET belirtilmeli. Yapılan denetim, belirtilen diğer seçenekler için de aynı şekilde gerçekleştirilir.
13. Yapılan denetim, belirtilen diğer seçenekler için de aynı şekilde gerçekleştirilir.

14. Bu, yalnızca doğrudan açılan kalıcı dinamik kuyruklar için geçerlidir, yani, bir model kuyruğu üzerinden açılmaz. Geçici bir dinamik kuyruğu silmek için güvenlik gerekli değildir.
15. RACF profilini hlq.SUBSCRIBE.topicnamekullanın.
16. RACF profilini hlq.PUBLISH.topicnamekullanın.
17. MQSUB isteğinde, yayınların gönderileceği hedef kuyruğu belirlediyseniz, o kuyruğa ilişkin yetkiye sahip olmadığınızdan emin olmak için o kuyruğa ilişkin bir güvenlik denetimi gerçekleştirilir.
18. MQSUB isteğinde, MQSO_CREATE ya da MQSO_ALTER seçenekleri belirtilirse, MQSD yapısındaki tanıtıcı bağlamı alanlarının herhangi birini ayarlamak istiyorsanız, MQSO_SET_IDENTITY_CONTEXT seçeneğini de belirtmeniz ve hedef kuyruğa ilişkin bağlam tanıtımı için uygun yetkiye de ihtiyacınız olduğunu da belirtmeniz gerekir.

z/OS *Konu güvenliğine ilişkin profiller*

Konu güvenliği etkinse, uygun sınıflarda tanıtımlar tanımlamanız ve bu tanıtımlara gereken grupların ya da kullanıcı kimliklerinin erişmesine izin vermeniz gerekir.

Bir konu ağacındaki konu güvenliği kavramı Yayınla/abone ol güvenliğikonusunda açıklanmıştır.

Konu güvenliği etkinse, aşağıdaki işlemleri gerçekleştirmeniz gerekir:

- **MXTOPIC** ya da **GMXTOPIC** sınıflarındaki tanıtımları tanımlayın.
- Konuları kullanan IBM MQ API isteklerini yayınlayabilmeleri için gerekli grupların ya da kullanıcı kimliklerinin bu profillere erişmesine izin verin.

Konu güvenliğine ilişkin profiller şu formu alır:

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

burada:

- `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir.
- `topicname` , konu ağacındaki konu denetim düğümünün adıdır; MQSUB çağrısı yoluyla abone olunan ya da MQOPEN çağrısıyla yayınlanmakta olan konuyla ilişkilidir.

Kuyruk yöneticisi adı öneki eklenmiş bir tanıtım, o kuyruk yöneticisindeki tek bir konuya erişimi denetler. Kuyruk paylaşım grubu adı öneki eklenmiş bir tanıtım, kuyruk paylaşım grubu içindeki tüm kuyruk yöneticilerine o konu adını taşıyan bir ya da daha çok konuya erişimi denetler. Bu erişim, söz konusu kuyruk yöneticisinde ilgili konu için kuyruk yöneticisi düzeyinde bir tanıtım tanımlanarak, tek bir kuyruk yöneticisinde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adının öneki olan bir tanıtımı denetler. Bir tanıtım bulamazsa, kuyruk paylaşım grubu adının öneki olan bir tanıtımı arar.

Abone olun

Bir konuya abone olmak için, abone olmaya çalıştığınız konuya ve yayınlara ilişkin hedef kuyruğa erişmeniz gerekir.

Bir MQSUB isteği yayınladığınızda aşağıdaki güvenlik denetimleri gerçekleşmiş:

- Bu konuya abone olmak için uygun erişim düzeyine sahip olup olmadığınızı ve çıkış için hedef kuyruğun (belirtildiyse) açılıp açılmadığını belirler
- Hedef kuyruğa uygun erişim düzeyine sahip olup olmadığınızı belirler.

Çizelge 37. Konu güvenliğinin abone olması için gereken erişim düzeyi	
MQSUB seçeneği	**MXTOPIC sınıfındaki `hlq.SUBSCRIBE.topicname` profili için RACF erişimi gerekli**
MQSO_CREATE ve MQSO_ALTER	Çeviri
MQSO_RESUME	READ

Çizelge 38. Yönetilmeyen bir hedef kuyruğu kullanarak abone olmak için ek yetki gerekli	
MQSUB seçeneği	**MQADMIN ya da MXADMIN sınıfında `hlq.CONTEXT.queuename` profili için RACF erişimi gerekli**
MQSO_CREATE, MQSO_ALTER ve MQSO_RESUME	GÜNCELLE
	MQQUEUE ya da MXQUEUE sınıfındaki `hlq.queuename` profili için RACF erişimi gerekli
MQSO_CREATE ve MQSO_ALTER	GÜNCELLE
	MQADMIN ya da MXADMIN sınıfında `hlq.ALTERNATE.USER.alternateuserid` profili için RACF erişimi gerekli
MQSO_ALTERNATE_USER_AUTHORITY	GÜNCELLE

Aboneliklere ilişkin yönetilen kuyruklara ilişkin dikkat edilecek noktalar

Konuya abone olmanıza izin verilip verilmediğini görmek için bir güvenlik denetimi gerçekleştirilir. Ancak, yönetilen kuyruk yaratıldığında ya da iletileri bu hedef kuyruğa koyma erişiminiz olup olmadığını belirlemek için güvenlik denetimi gerçekleştirilmez.

Yönetilen bir kuyruğu silmeyi kapatamazsınız.

Kullanılan model kuyrukları şunlardır: `SYSTEM.DURABLE.MODEL.QUEUE` ve `SYSTEM.NDURABLE.MODEL.QUEUE`.

Bu model kuyruklarından oluşturulan yönetilen kuyruklar, son niteleyicinin öngörülemediği `SYSTEM.MANAGED.DURABLE.A346EF00367849A0` ve `SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0` biçimindedir.

Bu kuyruklara herhangi bir kullanıcı erişimi vermeyin. Kuyruklar, yetki verilmediği için `SYSTEM.MANAGED.DURABLE.*` ve `SYSTEM.MANAGED.NDURABLE.*` biçiminde soysal tanıtımlar kullanılarak korunabilir.

İletiler, MQSUB isteğinde döndürülen tanıtıcı kullanılarak bu kuyruklardan alınabilir.

Belirtilen MQCO_REMOVE_SUB seçeneğiyle bir abonelik için belirtik olarak bir MQCLOSE çağrısı yaparsanız ve bu tanıtıcı altında kapatmakta olduğunuz aboneliği yaratmadıysanız, işlemi gerçekleştirmek için doğru yetkiye sahip olduğunuzdan emin olmak için kapanış sırasında bir güvenlik denetimi gerçekleştirilir.

Çizelge 39. Bir abone olma işleminin kapatılması için konu güvenliğine ilişkin profiller için gereken erişim düzeyi	
MQCLOSE seçeneği	**MXTOPIC sınıfındaki `hlq.SUBSCRIBE.topicname` profili için RACF erişimi gerekli**
MQCO_REMOVE_SUB	Çeviri

Yayınla

Bir konuda yayınlama yapmak için konuya ve diğer ad kuyruklarını kullanıyorsanız, diğer ad kuyruğuna da erişmeniz gerekir.

Çizelge 40. Konu güvenliğinin yayınlanması için gereken erişim düzeyi	
MQOPEN ya da MQPUT1 seçeneği	**MXTOPIC sınıfındaki `hlq.PUBLISH.topicname` profili için RACF erişimi gerekli**
MQOO_OUTPUT ya da MQPUT1	GÜNCELLE

Çizelge 41. Bir konuya çözülen bir diğer ad kuyruğunu açmak için gereken erişim düzeyi	
MQOPEN ya da MQPUT1 seçeneği	**Diğer ad kuyruğu için MQQUEUE ya da MXQUEUE sınıfındaki `hlq.queuename` profili için RACF erişimi gerekli**
MQOO_OUTPUT ya da MQPUT1	GÜNCELLE

Bir konu adına çözülen bir diğer ad kuyruğu yayınlanmak üzere açıldığında konu güvenliğinin nasıl çalıştığına ilişkin ayrıntılar için bkz. "Yayınlama işlemine ilişkin konulara çözümleyen diğer ad kuyruklarına ilişkin dikkat edilecek noktalar" sayfa 202.

PUT ya da GET kısıtlamaları için hedef kuyruklar için kullanılan diğer ad kuyruklarını göz önünde bulundurduğunuzda, bkz. "Diğer ad kuyruklarına ilişkin dikkat" sayfa 192.

Bir uygulamanın bir konu güvenliği profili için sahip olduğu RACF erişim düzeyi değiştirilirse, değişiklikler yalnızca o konu için elde edilen yeni nesne tanıtıcıları (yeni bir MQSUB ya da MQOPEN) için geçerli olur. Değişiklik sırasında var olan bu tanıtıcıları, konuya var olan erişimlerini korur. Ayrıca, var olan aboneler önceden yaptıkları aboneliklere erişimlerini korur.

Yayınlama işlemine ilişkin konulara çözümleyen diğer ad kuyruklarına ilişkin dikkat edilecek noktalar

Bir konuya çözülen diğer ad kuyruğu için bir MQOPEN ya da MQPUT1 çağrısı yayınladığınızda, IBM MQ iki kaynak denetimi yapar:

- MQOPEN ya da MQPUT1 çağrısındaki nesne tanımlayıcısında (MQOD) belirtilen diğer ad kuyruğu adına ilişkin ilk ad.
- Diğer ad kuyruğunun çözüldüğü konuya ilişkin ikinci

Bu davranışın, diğer ad kuyrukları diğer kuyruklara çözüldüğünde aldığınız davranıştan farklı olduğunu unutmayın. Yayınlama işleminin devam etmesi için her iki tanıtıma da doğru erişmeniz gerekir.

Sistem konusu güvenliği

Kanal başlatıcı adres alanından aşağıdaki sistem konularına erişilir.

Bu çalıştırmanın altında çalıştırıldığı kullanıcı kimliklerine, Çizelge 42 sayfa 202içinde gösterildiği gibi bu kuyruklar için RACF erişimi verilmelidir.

Çizelge 42. SYSTEM konularına erişim gerekli		
SYSTEM konusu	**Profil**	**Dağıtılmış kuyruğa alma için kanal başlatıcı**
SYSTEM.BROKER.ADMIN.STREAM	hlq.PUBLISH.topicname	GÜNCELLE
SYSTEM.BROKER.ADMIN.STREAM	hlq.SUBSCRIBE.topicname	Çeviri

z/OS *Süreçlere ilişkin tanıtımlar*

Süreç güvenliği etkinse, tanıtımları uygun sınıflarda tanımlamanız ve bu tanıtımlara gerekli grupların ya da kullanıcı kimlikleri erişiminin etkinleştirilmesine izin vermelisiniz.

Süreç güvenliği etkinse, şunları yapmak gerekir:

- Büyük harf tanıtımlar kullanılıyorsa, tanıtımları **MQPROC** ya da **GMQPROC** sınıflarında tanımlayın.
- Karma vaka profilleri kullanılıyorsa, tanıtımları **MXPROC** ya da **GMXPROC** sınıflarında tanımlayın.
- Bu profillere gerekli gruplar veya kullanıcı kimlikleri erişimine izin verin; böylece, bu grupların süreçleri kullanan IBM MQ API isteklerini yayınlayabilirler.

Süreçlere ilişkin tanıtımlar aşağıdaki formu alır:

```
hlq.processname
```

burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) ve `processname` , açılmakta olan işlemin adıdır.

Kuyruk yöneticisi adının önekli olduğu bir tanıtım, o kuyruk yöneticisinindeki tek bir süreç tanımlamasına erişimi denetler. Kuyruk paylaşım grubu adının önekli olduğu bir tanıtım, kuyruk paylaşım grubundaki tüm kuyruk yöneticilerindeki o adı taşıyan bir ya da daha çok süreç tanımlamasına erişimi denetler. Bu erişim, o kuyruk yöneticisininde o süreç tanımlaması için bir kuyruk yöneticisi düzeyi tanıtımı tanımlayarak, tek bir kuyruk yöneticisininde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adı önekli bir profil için denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar.

Aşağıdaki çizelge, bir süreci açmak için gereken erişimi göstermektedir.

Çizelge 43. Süreç güvenliği için erişim düzeyleri

MQOPEN seçeneği	**hlq.processnameiçin gerekenRACF erişim düzeyi**
MQOO_SORGULAMA	READ

For example, on queue manager MQS9, the RACF group INQVPRC must be able to inquire (`MQINQ`) on all processes starting with the letter V. Bunun için RACF tanımlamaları aşağıdaki gibi olur:

```
RDEFINE MQPROC MQS9.V* UACC(NONE)
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

Diğer kullanıcı güvenliği de, bir süreç tanımlaması nesnesi açıldığında belirtilen açma seçeneklerine bağlı olarak etkin olabilir.

z/OS *Ad listelerine ilişkin profiller*

Ad listesi güvenliği etkinse, tanıtımları uygun sınıflarda tanımlayabilir ve bu tanıtımlara gereken grupları ya da kullanıcı kimlikleri için erişim vermenizi sağlar.

Ad listesi güvenliği etkinse, şunları yapmak gerekir:

- Büyük harf tanıtımlar kullanılıyorsa, tanıtımları **MQNLIST** ya da **GMQNLIST** sınıflarında tanımlayın.
- Karma vaka profilleri kullanılıyorsa, tanıtımları **MXNLIST** ya da **GMXNLIST** sınıflarında tanımlayın.
- Bu tanıtımlara gerekli grupların ya da kullanıcı kimliklerinin erişmelerine izin verin.

Ad listelerine ilişkin tanıtımlar aşağıdaki formu alır:

```
hlq.namelistname
```

burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) ve `namelistname` , açılmakta olan ad listesinin adıdır.

Kuyruk yöneticisi adının önekli olduğu bir tanıtım, o kuyruk yöneticisindeki tek bir ad listesine erişimi denetler. Kuyruk paylaşım grubu adının önekli olduğu bir tanıtım, kuyruk paylaşım grubundaki tüm kuyruk yöneticilerindeki o adı taşıyan bir ya da daha çok ad listesine erişim erişimi denetler. Bu erişim, o kuyruk yöneticisindeki ad listesi için bir kuyruk yöneticisi düzeyi tanıtımı tanımlayarak, tek bir kuyruk yöneticisininde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adı önekli bir profil için denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar.

Aşağıdaki çizelge, bir ad listesi açmak için gereken erişimi göstermektedir.

Çizelge 44. Ad listesi güvenliği için erişim düzeyleri

MQOPEN seçeneği	**hlq.namelistnameiçin gerekenRACF erişim düzeyi**
MQOO_SORGULAMA	READ

For example, on queue manager (or queue sharing group) PQM3, the RACF group DEPT571 must be able to inquire (`MQINQ`) on these namelists:

- "DEPT571"ile başlayan tüm ad listeleri.
- PRINTER/DESTINATIONS/DEPT571
- AGENCY/REQUEST/QUEULER
- WAREHOUSE.BROADCAST

Bunu yapmak için gereken RACF tanımlamaları şunlardır:

```
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)
```

Bir ad listesi nesnesi açıldığında belirlenen seçeneklere bağlı olarak, diğer kullanıcı güvenliği etkin olabilir.

Sistem ad listesi güvenliği

Sistem adı listelerinin çoğu IBM MQ' un yan kısımlarıyla erişilir:

- CSQUTIL yardımcı programı
- İşlemler ve denetim panoları
- Kanal başlatıcı adres alanı (Kuyruğa Yollanmış Yayınlama/Abone Olma Daemon dahil)

The user IDs under which these run must be given RACF access to these namelists, as shown in Çizelge 45 sayfa 205.

Çizelge 45. IBM MQtarafından SYSTEM ad listelerine erişim gerekli			
SYSTEM adılistesi	**CSQUTIL**	**İşlemler ve denetim panoları**	**Dağıtılmış kuyruklama için kanal başlatıcısı**
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ

z/OS *Diğer kullanıcı güvenliği için profiller*

Diğer kullanıcı güvenliği etkinse, tanıtımları uygun sınıflarda tanımlamanız ve bu tanıtımlara gerekli grupların ya da kullanıcı kimlikleri erişiminin etkinleştirilmesine izin vermelisiniz.

*AlternateUserId*ile ilgili daha fazla bilgi için bkz. AlternateUserID (MQCHAR12).

Diğer kullanıcı güvenliği etkinse, şunları yapmak gerekir:

- Büyük harf tanıtımlar kullanıyorsanız, MQADMIN ya da GMQADMIN sınıflarında tanıtımları tanımlayın.
- Karma vaka profilleri kullanıyorsanız, MXADMIN ya da GMXADMIN sınıflarında tanıtımları tanımlayın.

Nesne açıldığında ALTERNATE_USER_AUTHORITY seçeneklerini kullanabilmesi için, bu tanıtımlara gereken grupların ya da kullanıcı kimliklerinin bu tanıtımlara erişmesine izin verir.

Diğer kullanıcı güvenliğine ilişkin tanıtımlar altsistem düzeyinde ya da kuyruk paylaşım grubu düzeyinde belirtilebilir ve aşağıdaki formu alabilir:

```
hlq.ALTERNATE.USER.alternateuserid
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) ve `alternateuserid` , nesne tanımlayıcısındaki *AlternateUserId* alanının değeridir.

Kuyruk yöneticisi adı önekli bir tanıtıma, o kuyruk yöneticisininde başka bir kullanıcı kimliği kullanılır. Kuyruk paylaşım grubu adının önekli olduğu bir tanıtım, kuyruk paylaşım grubu içindeki tüm kuyruk yöneticilerindeki diğer bir kullanıcı kimliğini kullanır. Bu alternatif kullanıcı kimliği, doğru erişimi olan bir kullanıcı tarafından kuyruk paylaşım grubu içindeki herhangi bir kuyruk yöneticisesinde kullanılabilir. Bu erişim, o kuyruk yöneticisindeki diğer kullanıcı kimliği için bir kuyruk yöneticisi düzeyi tanıtımı tanımlayarak, tek bir kuyruk yöneticilikinde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adı önekli bir profil için denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar.

Aşağıdaki tabloda, alternatif bir kullanıcı seçeneği belirtilirken erişim gösterilmektedir.

Çizelge 46. Diğer kullanıcı güvenliği için erişim düzeyleri	
MQOPEN, MQSUB ya da MQPUT1 seçeneği	**RACF erişim düzeyi gerekiyor**
MQOO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	GÜNCELLE

Diğer kullanıcı güvenlik denetimlerinin yanı sıra, kuyruk, süreç, ad listesi ve bağlam güvenliği için diğer güvenlik denetimleri de yapılabilir. Diğer kullanıcı kimliği (sağlandıysa) yalnızca, kuyruk, süreç tanımlaması ya da ad listesi kaynaklarına ilişkin güvenlik denetimleri için kullanılır. Diğer kullanıcı ve bağlam güvenliği denetimleri için, denetin kullanılmasını isteyen kullanıcı kimliği kullanılır. Kullanıcı kimliklerinin nasıl işlendiği ile ilgili ayrıntılar için bkz. “z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri” sayfa 227. Açık seçenekleri ve kuyruk, bağlam ve diğer kullanıcı güvenliği tüm etkin olduğunda gereken güvenlik denetimlerini gösteren bir özet tablosu için bkz. Çizelge 36 sayfa 197.

Diğer bir kullanıcı tanıtımı, istekte bulunan kullanıcı kimliğine, diğer kullanıcı kimlikle ilişkilendirilmiş olan kullanıcı kimliğiyle ilişkili kaynaklara erişim yetkisi verir. Örneğin, kuyruk yöneticisi QMPY ' de

kullanıcı kimliği PAYSERV altında çalışan bordro sunucusu, tüm PS ile başlayan personel kullanıcı kimliklerinden gelen istekleri işler. Bordro sunucusu tarafından gerçekleştirilen işin, istekte bulunan kullanıcının kullanıcı kimliği altında gerçekleştirilmesine neden olmak için, diğer kullanıcı yetkisi kullanılır. Bordro sunucusu, istekte bulunan programların MQPMO_DEFAULT_CONTEXT koyma iletisi seçeneğini kullanarak ileti üretmesi nedeniyle, hangi kullanıcı kimliğinin diğer kullanıcı kimliği olarak belirtileceğini bilir. Diğer kullanıcı kimliklerinin edinilmesiyle ilgili daha fazla bilgi için bkz. “z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri” sayfa 227 .

Aşağıdaki örnek RACF tanımları, sunucu programının, şu karakterler ile başlayan diğer kullanıcı kimliklerini belirtmesine olanak sağlar:

```
RDEFINE MQADMIN QMPY.ALTERNATE.USER.PS* UACC(NONE)
PERMIT QMPY.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSERV) ACCESS(UPDATE)
```

Not:

1. Nesne tanımlayıcısındaki ve abonelik tanımlayıcısındaki *AlternateUserId* alanları 12 bayt uzunluğundur. All 12 bytes are used in the profile checks, but only the first 8 bytes are used as the user ID by IBM MQ. Bu kullanıcı kimliği kesilmesi istenmiyorsa, isteği yapan uygulama programları, herhangi bir alternatif kullanıcı kimliğini 8 byte üzerinde daha uygun bir şeye çevirmelidir.
2. MQOO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY ya da MQPMO_ALTERNATE_USER_AUTHORITY değerini ve nesne tanımlayıcısında bir *AlternateUserId* alanı belirtmezseniz, bir kullanıcı kimliği olarak boşluk kullanılır. Diğer kullanıcı güvenliği amacıyla, *AlternateUserId* niteleyicisi için kullanılan kullanıcı kimliğinin -BLANK-. Örneğin, `RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-`. Örneğin, kullanıcı kimliği için kullanılması amaçlanır.

   Kullanıcının bu profile erişmesine izin veriliyorsa, tüm ek denetimler bir kullanıcı kimliği boşlukla yapılır. Boş kullanıcı kimliklerine ilişkin ayrıntılar için bkz. “Boş kullanıcı kimlikleri ve UACC düzeyleri” sayfa 235.

Genel alternatif kullanıcı profillerini kullanmanıza olanak sağlayan kullanıcı kimlikleri için bir adlandırma kuralınız varsa, diğer kullanıcı kimliklerinin denetlenmesi kolaylaşır. Bunu yapmazlarsa, RACF RACVARS özelliğini kullanabilirsiniz. RACVARS kullanımına ilişkin ayrıntılar için *z/OS SecureWay Security Server RACF Security Administrator's Guide*adlı yayına bakın.

Bir ileti, diğer kullanıcı yetkisi ile açılan bir kuyruğa konduğunda ve ileti bağlamı kuyruk yöneticisi tarafından oluşturulduğunu, MQMD_USER_IDENTIFIER alanı, diğer kullanıcı kimliğine ayarlanır.

z/OS *Bağlam güvenliğine ilişkin profiller*

IBM MQ , belirli bir iletiye özgü bağlam bilgilerine erişimi denetlemek için profilleri kullanır. Bağlam, ileti tanımlayıcısı (MQMD) içinde yer alır.

Bağlam güvenliği için profilleri kullanma

Bağlam güvenliği etkinse şunları yapmanız gerekir:

- Büyük harfli profiller kullanılıyorsa, **MQADMIN** sınıfında bir profil tanımlayın.
- Karışık büyük/küçük harf profilleri kullanılıyorsa, **MXADMIN** sınıfında profili tanımlayın.

Profil `hlq.CONTEXT.queuename` ya da `hlq.CONTEXT.topicname`olarak adlandırılır; burada:

hlq
`qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir.

queueName
Bağlam tanıtımını tanımlamak istediğiniz kuyruğun tam adı ya da soysal tanıtım olabilir.

konu adı
Bağlam tanıtımını tanımlamak istediğiniz konunun tam adı ya da soysal bir tanıtım olabilir.

Kuyruk yöneticisi adının öneki ve kuyruk ya da konu adı olarak ** belirtilmiş bir tanıtım, o kuyruk yöneticisine ait tüm kuyruklarda ve konularda bağlam güvenliğinin denetlenmesine olanak sağlar. Bu, söz konusu kuyruktaki ya da konudaki bağlam için belirli bir profil tanımlanarak, tek bir kuyrukta ya da konuda geçersiz kılınabilir.

Kuyruk paylaşım grubu adı öneki ve kuyruk ya da konu adı olarak ** belirtilmiş bir tanıtım, kuyruk paylaşım grubu içindeki kuyruk yöneticilerine ait tüm kuyruklar ve konular için bağlam denetimi sağlar. Kuyruk yöneticisi adı öneki eklenmiş bir tanıtım belirtilerek, o kuyruk yöneticisine ilişkin bağlam için kuyruk yöneticisi düzeyinde bir tanıtım tanımlanarak, bu tanıtım tek bir kuyruk yöneticisinde geçersiz kılınabilir. Kuyruk ya da konu adıyla bir tanıtım soneki belirlenerek, tek bir kuyrukta ya da konuda geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adının öneki olan bir tanıtımı denetler. Bir tanıtım bulamazsa, kuyruk paylaşım grubu adının öneki olan bir tanıtımı arar.

Bu tanıtım için gereken gruplara ya da kullanıcı kimliklerine erişim vermeniz gerekir. Aşağıdaki çizelge, kuyruk açıldığında bağlam seçeneklerinin belirtimine bağlı olarak, gereken erişim düzeyini gösterir.

Çizelge 47. Bağlam güvenliği için erişim düzeyleri

MQOPEN ya da MQPUT1 seçeneği	**RACF hlq.CONTEXT.queuename ya da hlq.CONTEXT.topicname için gereken erişim düzeyi**
MQPMO_NO_CONTEXT	Bağlam güvenliği denetimi yok
MQPMO_DEFAULT_CONTEXT	Bağlam güvenliği denetimi yok
MQOO_SAVE_ALL_CONTEXT	Bağlam güvenliği denetimi yok
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	READ
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	READ
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	GÜNCELLE
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT ya da MQPUT1(KULLANıM (XMITQ))	CONTROL
MQSUB seçeneği	
MQSO_SET_IDENTITY_CONTEXT **(Not 2)**	GÜNCELLE

Not:

1. Dağıtılmış kuyruğa alma için kullanılan kullanıcı kimlikleri, iletileri hedef kuyruğa koymak için `hlq.CONTEXT.queuename` ' e CONTROL erişimi gerektirir. Kullanılan kullanıcı kimliklerine ilişkin bilgi için bkz. “Kanal başlatıcısı tarafından kullanılan kullanıcı kimlikleri” sayfa 230 .
2. MQSUB isteğinde MQSO_CREATE ya da MQSO_ALTER seçenekleri belirtilirse, MQSD yapısında kimlik bağlamı alanlarından herhangi birini ayarlamak istiyorsanız, MQSO_SET_IDENTITY_CONTEXT seçeneğini belirtmeniz gerekir. Ayrıca, hedef kuyruğa ilişkin bağlam tanıtımı için gereken yetkiyi de vermeniz gerekir.

Komutları sistem komutu giriş kuyruğuna koyarsanız, doğru kullanıcı kimliğini komutla ilişkilendirmek için varsayılan bağlam koyma iletisi seçeneğini kullanın.

Örneğin, IBM MQtarafından sağlanan yardımcı program CSQUTIL, kuyruklardaki iletileri boşaltmak ve yeniden yüklemek için kullanılabilir. Boşaltılan iletiler bir kuyruğa geri yüklendiğinde, CSQUTIL yardımcı programı iletileri özgün durumlarına döndürmek için MQOO_SET_ALL_CONTEXT seçeneğini kullanır. Bu açık seçeneğin gerektirdiği kuyruk güvenliğine ek olarak, bağlam yetkisi de gereklidir.

Örneğin, MQS1kuyruk yöneticisindeki BACKGRP grubu için bu yetki gerekliyse, bu yetki aşağıdaki şekilde tanımlanır:

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

Belirlenen seçeneklere ve gerçekleştirilen güvenlik tiplerine bağlı olarak, kuyruk açıldığında diğer güvenlik denetimi tipleri de oluşabilir. Bunlar, kuyruk güvenliğini (bkz. “Kuyruk güvenliğine ilişkin profiller” sayfa 190) ve diğer kullanıcı güvenliğini içerir (bkz. “Diğer kullanıcı güvenliği için profiller” sayfa 205). Kuyruk, bağlam ve diğer kullanıcı güvenliğinin tümü etkin olduğunda gerekli olan açma seçeneklerini ve güvenlik denetimlerini gösteren bir özet tablo için bkz. Çizelge 36 sayfa 197.

Sistem kuyruğu bağlam güvenliği

Sistem kuyruklarının çoğuna IBM MQ' un yardımcı kısımları (örneğin, kanal başlatıcı adres alanı V 9.1.0) ve IBM MQ Console ve REST APItarafından kullanılan mqweb sunucusu) erişilir.

Bunların altında çalıştırıldığı kullanıcı kimliklerine, Çizelge 48 sayfa 208içinde gösterildiği gibi, bu kuyruklar için RACF erişimi verilmelidir.

Çizelge 48. Bağlam işlemleri için SYSTEM kuyruklarına erişim gerekli

SYSTEM kuyruğu	**Dağıtılmış kuyruğa alma için kanal başlatıcı**	**mqweb sunucusu**
SYSTEM.ADMIN.COMMAND.QUEUE	-	CONTROL
SYSTEM.BROKER.CONTROL.QUEUE	CONTROL	-
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	CONTROL	-
SYSTEM.CHANNEL.SYNCQ	CONTROL	-
SYSTEM.CLUSTER.COMMAND.QUEUE	CONTROL	-
SYSTEM.CLUSTER.TRANSMIT.QUEUE	CONTROL	-

z/OS *Komut güvenliği için tanıtımlar*

Komutlara ilişkin güvenlik denetimini etkinleştirmek için, MQCMDS sınıfına tanıtım ekleyin. Tanıtım adları MQSC komutlarına dayalıdır, ancak hem MQSC hem de PCF komutlarını denetler. Tanıtımlar, bir kuyruk yöneticisine ya da kuyruk paylaşım grubuna uygulanabilir.

Komutlara ilişkin güvenlik denetimi istiyorsanız (bu nedenle, hlq.NO.CMD.CHECKS), MQCMDS sınıfına tanıtım eklemelisiniz.

Aynı güvenlik profilleri, hem MQSC hem de PCF komutlarını denetler. Komut güvenliği denetimi için RACF tanıtımlarının adları, MQSC komut adlarının temelinde yer alır. Bu tanıtımlar aşağıdaki formu alır:

```
hlq.verb.pkw
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir; `verb` , komut adının, örneğin ALTER ve `pkw` nesne tipidir; örneğin, yerel bir kuyruk için QLOCAL biçimidir.

Bu nedenle, CSQ1 altsistemindeki ALTER QLOCAL komutuna ilişkin tanıtım adı:

```
CSQ1.ALTER.QLOCAL
```

Komut kümelerini korumak için soysal profilleri kullanabilirsiniz; böylece, daha az sayıda tanıtıma sahip olacak ve bu nedenle daha az sayıda erişim listesine sahip olabilirsiniz. Daha belirli bir tanıtıma karşı korunmayan tüm komutlar için geçerli olan soysal bir tanıtım yaratmayı düşünün. Bu profili UACC (NONE) ile tanımlayın ve yalnızca denetimcileri içeren RACF gruplarına ALTER erişimi verin. Daha sonra, tüm DISPLAY komutları için geçerli bir soysal profil yaratabilir ve bu tanıtıma yaygın erişim verebilirsiniz. Bu uç noktalar arasında, belirli komut kümelerine erişmesi gereken kullanıcı gruplarını belirleyebilirsiniz. Bu durumda, bu kümeler için profil oluşturabilir ve bu kullanıcı sınıflarını temsil eden RACF gruplarına erişim izni verebilirsiniz. Kullanıcılara, gerekmeyen komutlara erişim izni vermekten kaçının: En az ayrıcalık ilkesini uygulayın, böylece kullanıcıların yalnızca işleri için gereken komutlara erişimleri olur.

Kuyruk yöneticisi adının başına önek olarak eklenen bir tanıtım, o kuyruk yöneticisininde komutun kullanımını denetler. Kuyruk paylaşım grubu adının önekli olduğu bir tanıtım, kuyruk paylaşım grubundaki tüm kuyruk yöneticilerindeki komutların kullanımını denetler. Bu erişim, o kuyruk yöneticisininde o komut için bir kuyruk yöneticisi düzeyi tanıtımı tanımlayarak, tek bir kuyruk yöneticisininde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ , önekli bir profil için kuyruk yöneticisi adı önekli olarak denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar.

Bir kullanıcının, kuyruk yöneticisi düzeyinde komut tanıtımlarını ayarlayarak, belirli bir kuyruk yöneticisinde komutlar yayınlanarak kısıtlanabileceği bir değer olabilir. Diğer bir seçenek olarak, her komut komutu için bir kuyruk paylaşım grubu için tek bir profil tanımlayabilir ve tek tek kuyruk yöneticileri yerine tüm güvenlik denetimleri o profile göre gerçekleşebilir.

Hem altsistem güvenliği, hem de kuyruk paylaşım grubu güvenliği etkinse ve yerel bir tanıtım bulunamazsa, kullanıcının bir kuyruk paylaşım grubu profiline erişimi olup olmadığını görmek için bir komut güvenliği denetimi gerçekleştirilir.

Bir komutu bir kuyruk paylaşım grubundaki diğer kuyruk yöneticilerine yönlendirmek için CMDSCOPE özniteliğini kullanırsanız, komutun çalıştırıldığı her kuyruk yöneticisinde güvenlik denetlenir, ancak komutun girildiği kuyruk yöneticisinde olması gerekmez.

Çizelge 49 sayfa 209 shows, for each IBM MQ MQSC command, the profiles required for command security checking to be carried out, and the corresponding access level for each profile in the MQCMDS class.

Çizelge 50 sayfa 214 shows, for each IBM MQ PCF command, the profiles required for command security checking to be carried out, and the corresponding access level for each profile in the MQCMDS class.

Çizelge 49. MQSC komutları, profiller ve erişim düzeyleri

Komut	**MQCMDS için komut tanıtımı**	**MQCMDS için erişim düzeyi**	**MQADMIN ya da MXADMIN komut kaynağı tanıtımı**	**MQADMIN ya da MXADMIN erişim düzeyi**
ALTER AUTHINFO	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ARABELLEĞI DEĞIŞTIR	hlq.ALTER.BUFFPOOL	ALTER	Denetim yok	-
ALTER CFSTRUCT	hlq.ALTER.CFSTRUCT	ALTER	Denetim yok	-
KANALı ALTER	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
ALTER NAMELIST	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
ALTER PROCESS	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
ALTER PSID	hlq.ALTER.PSID	ALTER	Denetim yok	-
QALIAS ALTER	hlq.ALTER.QALIAS	ALTER	hlq.QUEUE.queue	ALTER

Çizelge 49. MQSC komutları, profiller ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
ALTER QLOCAL	hlq.ALTER.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ALTER QMGR	hlq.ALTER.QMGR	ALTER	Denetim yok	-
ALTER QMODEL	hlq.ALTER.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
ALTER QREMOTE	hlq.ALTER.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
ALTER SECURITY	hlq.ALTER.SECURITY	ALTER	Denetim yok	-
ALTER SMDS	hlq.ALTER.SMDS	ALTER	Denetim yok	-
ALTER STGCLASS	hlq.ALTER.STGCLASS	ALTER	Denetim yok	-
ALTER SUB	hlq.ALTER.SUB	ALTER	Denetim yok	-
KONUYU DEĞIŞTIR	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ALTER TRACE	hlq.ALTER.TRACE	ALTER	Denetim yok	-
GüNLüğü	hlq.ARCHIVE.LOG	CONTROL	Denetim yok	-
BACKUP CFSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	Denetim yok	-
QLOCAL ' I TEMIZLE	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
CLEAR TOPICSTR “3” sayfa 214	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
DEFINE YAZAR	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ARABELLEK HAVUZU TANIMLA	hlq.DEFINE.BUFFPOOL	ALTER	Denetim yok	-
CFSTRUCT DEFINE	hlq.DEFINE.CFSTRUCT	ALTER	Denetim yok	-
KANAL TANIMLA	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
OTURUM KAPAT	hlq.DEFINE.LOG	ALTER	Denetim yok	-
DEFINE MAXSSGS	hlq.DEFINE.MAXSMSGS	ALTER	Denetim yok	-
AD LISTESINI TANı	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
SüREç TANIMLA	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DEğERLERI	hlq.DEFINE.PSID	ALTER	Denetim yok	-
QALIAS ' YI	hlq.DEFINE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
QLOCAL ' I TANIMLA	hlq.DEFINE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
QMODEL ' I TANIMLA	hlq.DEFINE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
QREMOTE TANIMLA	hlq.DEFINE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
STGCLASS TANIMLA	hlq.DEFINE.STGCLASS	ALTER	Denetim yok	-
ALT	hlq.DEFINE.SUB	ALTER	Denetim yok	-
KONUYU TANIMLA	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER

Çizelge 49. MQSC komutları, profiller ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
YAZAR BILGILERINI SIL	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ARABELLEK HAVUZUNU SIL	hlq.DELETE.BUFFPOOL	ALTER	Denetim yok	-
CFSTRUCT SIL	hlq.DELETE.CFSTRUCT	ALTER	Denetim yok	-
KANAL SILME	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
ADı SIL	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Süreci Sil	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
PSID SIL	hlq.DELETE.PSID	ALTER	Denetim yok	-
QALIAS SIL	hlq.DELETE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
QLOCAL SIL	hlq.DELETE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
QMODEMI SIL	hlq.DELETE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
QREMOTE SIL	hlq.DELETE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
STGCLASı SIL	hlq.DELETE.STGCLASS	ALTER	Denetim yok	-
SUB SIL	hlq.DELETE.SUB	ALTER	Denetim yok	-
KONUYU SIL	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ARşIV “1” sayfa 214	hlq.DISPLAY.ARCHIVE	READ	Denetim yok	-
AUTHENTICAFO GÖRÜNTÜLE	hlq.DISPLAY.AUTHINFO	READ	Denetim yok	-
CFSTATUS GÖRÜNTÜLE	hlq.DISPLAY.CFSTATUS	READ	Denetim yok	-
CFSTRUCT GöRüNTüLE	hlq.DISPLAY.CFSTRUCT	READ	Denetim yok	-
KANAL GÖRÜNTÜLE	hlq.DISPLAY.CHANNEL	READ	Denetim yok	-
ÇINCE GöRüNTüLE	hlq.DISPLAY.CHINIT	READ	Denetim yok	-
CHLAUTH GÖRÜNTÜLE	hlq.DISPLAY.CHLAUTH	READ	Denetim yok	-
DURUMU GöRüNTüLE	hlq.DISPLAY.CHSTATUS	READ	Denetim yok	-
CLUSQMGR GöRüNTüLE	hlq.DISPLAY.CLUSQMGR	READ	Denetim yok	-
CMDSERV GöRüNTüLE	hlq.DISPLAY.CMDSERV	READ	Denetim yok	-
DISPLAY CONN “1” sayfa 214	hlq.DISPLAY.CONN	READ	Denetim yok	-
GRUBU GÖRÜNTÜLE	hlq.DISPLAY.GROUP	READ	Denetim yok	-

Çizelge 49. MQSC komutları, profiller ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
DISPLAY LOG “1” sayfa 214	hlq.DISPLAY.LOG	READ	Denetim yok	-
MAXSMSGS GÖRÜNTÜLE	hlq.DISPLAY.MAXSMSGS	READ	Denetim yok	-
GöRüNTüLEME	hlq.DISPLAY.NAMELIST	READ	Denetim yok	-
İşLEM SüRü	hlq.DISPLAY.PROCESS	READ	Denetim yok	-
PUBSUB GÖRÜNTÜLE	hlq.DISPLAY.PUBSUB	READ	Denetim yok	-
QALIAS (QALI	hlq.DISPLAY.QALIAS	READ	Denetim yok	-
QKüME GöRüN	hlq.DISPLAY.QCLUSTER	READ	Denetim yok	-
QLOCAL ' I GÖRÜNTÜLE	hlq.DISPLAY.QLOCAL	READ	Denetim yok	-
QMGR GöRüNTüLE	hlq.DISPLAY.QMGR	READ	Denetim yok	-
QMODEL ' I GÖRÜNTÜLE	hlq.DISPLAY.QMODEL	READ	Denetim yok	-
QREMOTE DISPLAY	hlq.DISPLAY.QREMOTE	READ	Denetim yok	-
QSTATUS GÖRÜNTÜLE	hlq.DISPLAY.QSTATUS	READ	Denetim yok	-
GöRüNTüLE	hlq.DISPLAY.QUEUE	READ	Denetim yok	-
SBSTATUS GÖRÜNTÜLE	hlq.DISPLAY.SBSTATUS	READ	Denetim yok	-
SMDS GöRüNTü	hlq.DISPLAY.SMDS	READ	Denetim yok	-
SMDSCONN GöRüNTüLE	hlq.DISPLAY.SMDSCONN	READ	Denetim yok	-
GöRüNTüLE	hlq.DISPLAY.SUB	READ	Denetim yok	-
GüVENLIK	hlq.DISPLAY.SECURITY	READ	Denetim yok	-
STGCLASS GöRüNTüLE	hlq.DISPLAY.STGCLASS	READ	Denetim yok	-
GÖRÜNTÜ SISTEMI “1” sayfa 214	hlq.DISPLAY.SYSTEM	READ	Denetim yok	-
GöRüNTüLE	hlq.DISPLAY.THREAD	READ	Denetim yok	-
TANıTıM	hlq.DISPLAY.TPSTATUS	READ	Denetim yok	-
KONUYU GÖRÜNTÜLE	hlq.DISPLAY.TOPIC	READ	Denetim yok	-
TANıTıM	hlq.DISPLAY.TPSTATUS	READ	Denetim yok	-
İZLEME IZLEME	hlq.DISPLAY.TRACE	READ	Denetim yok	-

Çizelge 49. MQSC komutları, profiller ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
DISPLAY USAGE “1” sayfa 214	hlq.DISPLAY.USAGE	READ	Denetim yok	-
QLOCAL ' I TAŞI	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
PING KANALI	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
BSSS ' LERI KURTAR	hlq.RECOVER.BSDS	CONTROL	Denetim yok	-
CFSTRUCT ' U KURTAR	hlq.RECOVER.CFSTRUCT	CONTROL	Denetim yok	-
KüME YENILE	hlq.REFRESH.CLUSTER	ALTER	Denetim yok	-
QMGR ' YI YENILE	hlq.REFRESH.QMGR	ALTER	Denetim yok	-
Güvenliği yenileme	hlq.REFRESH.SECURITY	ALTER	Denetim yok	-
CFSTRUCT İLE RESET	hlq.RESET.CFSTRUCT	CONTROL	Denetim yok	-
KANALı	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
KüMEYI Sı	hlq.RESET.CLUSTER	CONTROL	Denetim yok	-
QMGR RESET	hlq.RESET.QMGR	CONTROL	Denetim yok	-
QSTATS ' ı Sı	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
SMDS ' YI YENIDEN	hlq.RESET.SMDS	CONTROL	Denetim yok	-
TPIPE ' YI	hlq.RESET.TPIPE	CONTROL	Denetim yok	-
KANALıN	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
BELIRSIZ KALıCı	hlq.RESOLVE.INDOUBT	CONTROL	Denetim yok	-
QMGR ' YI Sü	hlq.RESUME.QMGR	CONTROL	Denetim yok	-
GüVENLIğI	hlq.RVERIFY.SECURITY	ALTER	Denetim yok	-
ARşIV	hlq.SET.ARCHIVE	CONTROL	Denetim yok	-
CHLAUTH KüMESI	hlq.SET.CHLAUTH	CONTROL	Denetim yok	-
OTURUM AçMA	hlq.SET.LOG	CONTROL	Denetim yok	-
SISTEM AYARLA	hlq.SET.SYSTEM	CONTROL	Denetim yok	-
KANAL BAşLAT	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
START CHINIT “4” sayfa 214	hlq.START.CHINIT	CONTROL	Denetim yok	-
CMDSERV BAşLAT	hlq.START.CMDSERV	CONTROL	Denetim yok	-
DINLEYICI BAşLAT	hlq.START.LISTENER	CONTROL	Denetim yok	-
QMGR ' YI	YOK“2” sayfa 214	-	-	-
SMDSCONN BAşLı	hlq.START.SMDSCONN	CONTROL	Denetim yok	-

Çizelge 49. MQSC komutları, profiller ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
İZLEMEYI	hlq.START.TRACE	CONTROL	Denetim yok	-
KANAL DURDUR	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
CHINIT DURDURUN	hlq.STOP.CHINIT	CONTROL	Denetim yok	-
CMDSERV ' I DURDUR	hlq.STOP.CMDSERV	CONTROL	Denetim yok	-
DINLEYICIYI DURDUR	hlq.STOP.LISTENER	CONTROL	Denetim yok	-
DURDUR QMGR	hlq.STOP.QMGR	CONTROL	Denetim yok	-
SMDSCONN ' ı DURDUR	hlq.STOP.SMDSCONN	CONTROL	Denetim yok	-
İZLEME DURDUR	hlq.STOP.TRACE	CONTROL	Denetim yok	-
QMGR ' YI AS	hlq.SUSPEND.QMGR	CONTROL	Denetim yok	-

Notlar:

1. Bu komutlar, kuyruk yöneticisi tarafından dahili olarak yayınlanabilir; bu durumlarda hiçbir yetki denetlenmez.
2. IBM MQ , QMGR komutunu START komutunu veren kullanıcının yetkisini denetmez. Ancak, START QMGR komutunun sonucu olarak verilen START xxxxMSTR komutuna erişimi denetlemek için RACFya da alternatif güvenlik olanaklarınızı kullanabilirsiniz. Bu işlem, RACF işletmen komutlarındaki (OPERCMDS) MVS.START.STC.xxxxMSTR tanıtımında erişimi denetleyerek yapılır. Bu yordama ilişkin ayrıntılar için *z/OS SecureWay Security Server RACF Security Administrator's Guide*adlı yayına bakın. Bu tekniği kullanırsanız ve yetkisiz bir kullanıcı kuyruk yöneticisini başlatma girişiminde bulunursa, bu durum 00F30216neden koduyla sona erer.
3. **hlq.TOPIC.topic** kaynağı, TOPICSTR nesnesinden türetilen Konu nesnesine gönderme yapar. Daha fazla ayrıntı için bkz. “Güvenliği yayınla/abone ol” sayfa 447
4. IBM MQ for z/OS V6öncesindeki yayın düzeylerinde, güvenlik denetimi MVS.START.STC.CSQ1CHIN. IBM MQ for z/OS V6 ve sonraki düzeylerde, kaynak adının sonuna ek bir JOBNAME niteleyicisi eklenmiş olur. Bu, kanal başlatıcısı başlatılırken sorunlara neden olabilir.

   Sorunu çözmek için MVS.START.STC' yi değiştirin. *Ssid* , MVS.START.STCadlı kaynak için bir profille CHIN. *ssid* CHIN **.*** ya da MVS.START.STC. *ssid* CHIN. *ssid* CHIN (burada *ssid* , kuyruk yöneticisinin altsistem tanıtıcısıdır). Bu, RACF UPDATE yetkisini gerektirir. Daha fazla ayrıntı için bkz. *İşlem planlama, MVS Komutları, RACF Erişim Yetkilileri ve Kaynak Adları*için z/OS ürün belgeleri .

   ssid MSTR için START işlevi, JOBNAME= değiştirgesini içermiyor. For consistency, you might want to update the profile for MVS.START.STC.ssidMSTR to MVS.START.STC.ssidMSTR.*.

Çizelge 50. PCF komutları, tanıtımlar ve erişim düzeyleri

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
Yedek CF Yapısı	hlq.BACKUP.CFSTRUCT	CONTROL	Denetim yok	-

Çizelge 50. PCF komutları, tanıtımlar ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
Kimlik Doğrulama Bilgileri Nesnesini Değiştir	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF Yapısını Değiştir	hlq.ALTER.CFSTRUCT	ALTER	Denetim yok	-
Kanalı Değiştir	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Ad listesini değiştir	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Süreci Değiştir	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Kuyruğu Değiştir	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Kuyruk Yöneticisini Değiştir	hlq.ALTER.QMGR	ALTER	Denetim yok	-
Güvenliği Değiştir	hlq.ALTER.SECURITY	ALTER	Denetim yok	-
SMDS ' yi Değiştir	hlq.ALTER.SMDS	ALTER	Denetim yok	-
Depolama Sınıfını Değiştir	hlq.ALTER.STGCLASS	ALTER	Denetim yok	-
Aboneliği Değiştir	hlq.ALTER.SUB	ALTER	Denetim yok	-
Konuyu Değiştir	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Kuyruğu Temizle	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Konu Dizgisini Temizle “1” sayfa 218	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
Kimlik Doğrulama Bilgileri Nesnesini Kopyala	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF Yapısını Kopyala	hlq.DEFINE.CFSTRUCT	ALTER	Denetim yok	-
Kanalı Kopyala	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Ad listesini kopyala	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
İşlemi Kopyala	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Kuyruğu Kopyala	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Aboneliği Kopyala	hlq.DEFINE.SUB	ALTER	Denetim yok	-
Depolama Sınıfını Kopyala	hlq.DEFINE.STGCLASS	ALTER	Denetim yok	-
Konuyu Kopyala	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Kimlik Doğrulama Bilgileri Nesnesi Yarat	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF Yapısı Yarat	hlq.DEFINE.CFSTRUCT	ALTER	Denetim yok	-
Kanal Yarat	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Ad Listesi Yarat	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Süreç Yarat	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Kuyruk Yarat	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER

Çizelge 50. PCF komutları, tanıtımlar ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
Depolama Sınıfı Yarat	hlq.DEFINE.STGCLASS	ALTER	Denetim yok	-
Abonelik Yarat	hlq.DEFINE.SUB	ALTER	Denetim yok	-
Konu Oluştur	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Kimlik Doğrulama Bilgileri Nesnesini Sil	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
CF Yapısını Sil	hlq.DELETE.CFSTRUCT	ALTER	Denetim yok	-
Kanalı Sil	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Ad listesini sil	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Süreci Sil	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Kuyruğu sil	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Depolama Sınıfını Sil	hlq.DELETE.STGCLASS	ALTER	Denetim yok	-
Aboneliği Sil	hlq.DELETE.SUB	ALTER	Denetim yok	-
Konuyu Sil	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Sorgu Arşivi	hlq.DISPLAY.ARCHIVE	READ	Denetim yok	-
Kimlik Doğrulama Bilgileri Nesnesi	hlq.DISPLAY.AUTHINFO	READ	Denetim yok	-
Kimlik Doğrulama Bilgileri Nesne Adları	hlq.DISPLAY.AUTHINFO	READ	Denetim yok	-
CF Yapısını Sorgula	hlq.DISPLAY.CFSTRUCT	READ	Denetim yok	-
CF Yapısı Adlarını Sorgula	hlq.DISPLAY.CFSTRUCT	READ	Denetim yok	-
CF Yapısı Durumunu Sorgula	hlq.DISPLAY.CFSTATUS	READ	Denetim yok	-
Kanal Sorgula	hlq.DISPLAY.CHANNEL	READ	Denetim yok	-
Kanal Doğrulama Kayıtları Sorgula	hlq.DISPLAY.CHLAUTH	READ	Denetim yok	-
Kanal Başlatıcı Sorgula	hlq.DISPLAY.CHINIT	READ	Denetim yok	-
Kanal Adlarını Sorgula	hlq.DISPLAY.CHANNEL	READ	Denetim yok	-
Kanal Durumunu Sorgula	hlq.DISPLAY.CHSTATUS	READ	Denetim yok	-
Sorgu Kümesi Kuyruk Yöneticisi	hlq.DISPLAY.CLUSQMGR	READ	Denetim yok	-
Bağlantı Sorgula	hlq.DISPLAY.CONNPCF	READ	Denetim yok	-
Sorgu Grubu	hlq.DISPLAY.GROUP	READ	Denetim yok	-
Günlüğü Sorgula	hlq.DISPLAY.LOG	READ	Denetim yok	-
Sorgu Adı Listesi	hlq.DISPLAY.NAMELIST	READ	Denetim yok	-
Sorgu Adı Listesi Adları	hlq.DISPLAY.NAMELIST	READ	Denetim yok	-
Süreç Sorgula	hlq.DISPLAY.PROCESS	READ	Denetim yok	-

Çizelge 50. PCF komutları, tanıtımlar ve erişim düzeyleri (devamı var)

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
Süreç Adlarını Sorgula	hlq.DISPLAY.PROCESS	READ	Denetim yok	-
Pub/Sub Durumu Sorgula	hlq.DISPLAY.PUBSUB	READ	Denetim yok	-
Sorgu Kuyruğu	hlq.DISPLAY.QUEUE	READ	Denetim yok	-
Sorgu Kuyruğu Yöneticisi	hlq.DISPLAY.QMGR	READ	Denetim yok	-
Sorgu Kuyruğu Adları	hlq.DISPLAY.QUEUE	READ	Denetim yok	-
Sorgu Kuyruğu Durumu	hlq.DISPLAY.QSTATUS	READ	Denetim yok	-
Güvenlik Takibi	hlq.DISPLAY.SECURITY	READ	Denetim yok	-
SMDS ' ye sor	hlq.DISPLAY.SMDS	READ	Denetim yok	-
SMDSCONN sorgulamak	hlq.DISPLAY.SMDSCONN	READ	Denetim yok	-
Depolama Sınıfı Sorgulama	hlq.DISPLAY.STGCLASS	READ	Denetim yok	-
Depolama Sınıfı Adlarını Sorgula	hlq.DISPLAY.STGCLASS	READ	Denetim yok	-
Sorgu Aboneliği	hlq.INQUIRE.SUB	READ	Denetim yok	-
Abonelik Durumunu Sorgula	hlq.INQUIRE.SBSTATUS	READ	Denetim yok	-
Sistem Sorgula	hlq.DISPLAY.SYSTEM	READ	Denetim yok	-
Konu Sorgula	hlq.DISPLAY.TOPIC	READ	Denetim yok	-
Konu Adlarını Sorgula	hlq.DISPLAY.TOPIC	READ	Denetim yok	-
Konu Durumunu Sorgula	hlq.DISPLAY.TPSTATUS	READ	Denetim yok	-
Bilgi Sorgula	hlq.DISPLAY.USAGE	READ	Denetim yok	-
Kuyruğu Taşı	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
Ping Kanalı	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
CF Yapısını Kurtar	hlq.RECOVER.CFSTRUCT	CONTROL	Denetim yok	-
Kümeyi Yenile	hlq.REFRESH.CLUSTER	ALTER	Denetim yok	-
Kuyruk Yöneticisini Yenile	hlq.REFRESH.QMGR	ALTER	Denetim yok	-
Güvenliği Yenile	hlq.REFRESH.SECURITY	ALTER	Denetim yok	-
CF Yapısını Sıfırla	hlq.RESET.CFSTRUCT	CONTROL	Denetim yok	-
Kanalı Sıfırla	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kümeyi Sıfırla	hlq.RESET.CLUSTER	CONTROL	Denetim yok	-
Kuyruk Yöneticisini Sıfırla	hlq.RESET.QMGR	CONTROL	Denetim yok	-
Kuyruk İstatistiklerini Sıfırla	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL

Çizelge 50. PCF komutları, tanıtımlar ve erişim düzeyleri (devamı var)				
Komut	**MQCMDS için komut tanıtımı**	**MQCMDS için erişim düzeyi**	**MQADMIN ya da MXADMIN komut kaynağı tanıtımı**	**MQADMIN ya da MXADMIN erişim düzeyi**
SDS ' yi Sıfırla	hlq.RESET.SMDS	CONTROL	Denetim yok	-
Kanalı Çözümle	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kuyruk Yöneticisini Sürdür	hlq.RESUME.QMGR	CONTROL	Denetim yok	-
Sürdürme Kuyruğu Yöneticisi Kümesi	hlq.RESUME.QMGR	CONTROL	Denetim yok	-
Güvenliği Yeniden Doğrula	hlq.RVERIFY.SECURITY	ALTER	Denetim yok	-
Arşivi Ayarla	hlq.SET.ARCHIVE	CONTROL	Denetim yok	-
Kanal Doğrulama Kaydını Ayarla	hlq.SET.CHLAUTH	CONTROL	Denetim yok	-
Günlüğü Ayarla	hlq.SET.LOG	CONTROL	Denetim yok	-
Sistem Ayarla	hlq.SET.SYSTEM	CONTROL	Denetim yok	-
Başlangıç Kanalı	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kanal Başlatıcısını Başlat	hlq.START.CHINIT	CONTROL	Denetim yok	-
Kanal Dinleyicisi Başlat	hlq.START.LISTENER	CONTROL	Denetim yok	-
SMDS Bağlantısını Başlat	hlq.START.SMDSCONN	CONTROL	Denetim yok	-
Kanalı Durdur	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kanal Başlatıcıyı Durdur	hlq.STOP.CHINIT	CONTROL	Denetim yok	-
Kanal Dinleyiciyi Durdur	hlq.STOP.LISTENER	CONTROL	Denetim yok	-
SMDS Bağlantısını Durdur	hlq.STOP.SMDSCONN	CONTROL	Denetim yok	-
Kuyruk Yöneticisini Askıya Al	hlq.SUSPEND.QMGR	CONTROL	Denetim yok	-
Kuyruk Yöneticisi Kümesini Askıya Al	hlq.SUSPEND.QMGR	CONTROL	Denetim yok	-

Notlar:

1. **hlq.TOPIC.topic** kaynağı, TOPICSTR nesnesinden türetilen Konu nesnesine gönderme yapar. Daha fazla ayrıntı için bkz. “Güvenliği yayınla/abone ol” sayfa 447

V 9.1.0 IBM MQ Consolekullanırken, gereken IBM MQ PCF tanıtımlarının ayrıntıları için “IBM MQ Console -gerekli komut güvenliği profilleri” sayfa 218 başlıklı konuya bakın.

z/OS V 9.1.0 *IBM MQ Console -gerekli komut güvenliği profilleri*

IBM MQ Console 'da bir kullanıcı tarafından `MQWebAdmin`ya da `MQWebAdminRO`' da gerçekleştirilen işlemler, mqweb sunucusunun güvenlik bağlamı altında yer alır ve görev kullanıcı kimliğini başlattı. IBM MQ Console' u kullanmak istiyorsanız, mqweb sunucusu başlatıldı görevi kullanıcı kimliği, bazı PCF komutlarını vermek için yetkilendirmeye gerek duyar.

Çizelge 51 sayfa 219 , her bir IBM MQ PCF komutu için, gerekli olan komut güvenliği profillerini ve IBM MQ Consoleile gereken MQCMDS sınıfındaki her bir profile ilişkin erişim düzeyini gösterir.

Çizelge 51. IBM MQ Console PCF komutları, profiller ve erişim düzeyleri

Komut	MQCMDS için komut tanıtımı	MQCMDS için erişim düzeyi	MQADMIN ya da MXADMIN komut kaynağı tanıtımı	MQADMIN ya da MXADMIN erişim düzeyi
Kimlik Doğrulama Bilgileri Nesnesini Değiştir	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Kanalı Değiştir	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Kuyruğu Değiştir	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Kuyruk Yöneticisini Değiştir	hlq.ALTER.QMGR	ALTER	Denetim yok	-
Konuyu Değiştir	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Kuyruğu Temizle	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Kimlik Doğrulama Bilgileri Nesnesi Yarat	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Kanal Yarat	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Kuyruk Yarat	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Abonelik Yarat	hlq.DEFINE.SUB	ALTER	Denetim yok	-
Konu Oluştur	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Kimlik Doğrulama Bilgileri Nesnesini Sil	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Kanalı Sil	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Kuyruğu sil	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Aboneliği Sil	hlq.DELETE.SUB	ALTER	Denetim yok	-
Konuyu Sil	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Kimlik Doğrulama Bilgileri Nesnesi	hlq.DISPLAY.AUTHINFO	READ	Denetim yok	-
Kimlik Doğrulama Bilgileri Nesne Adları	hlq.DISPLAY.AUTHINFO	READ	Denetim yok	-
Kanal Sorgula	hlq.DISPLAY.CHANNEL	READ	Denetim yok	-
Kanal Doğrulama Kayıtları Sorgula	hlq.DISPLAY.CHLAUTH	READ	Denetim yok	-
Kanal Başlatıcı Sorgula	hlq.DISPLAY.CHINIT	READ	Denetim yok	-
Kanal Adlarını Sorgula	hlq.DISPLAY.CHANNEL	READ	Denetim yok	-
Kanal Durumunu Sorgula	hlq.DISPLAY.CHSTATUS	READ	Denetim yok	-
Sorgu Kuyruğu	hlq.DISPLAY.QUEUE	READ	Denetim yok	-
Sorgu Kuyruğu Yöneticisi	hlq.DISPLAY.QMGR	READ	Denetim yok	-
Sorgu Kuyruğu Adları	hlq.DISPLAY.QUEUE	READ	Denetim yok	-
Sorgu Kuyruğu Durumu	hlq.DISPLAY.QSTATUS	READ	Denetim yok	-
Sorgu Aboneliği	hlq.INQUIRE.SUB	READ	Denetim yok	-
Abonelik Durumunu Sorgula	hlq.INQUIRE.SBSTATUS	READ	Denetim yok	-

Çizelge 51. IBM MQ Console PCF komutları, profiller ve erişim düzeyleri (devamı var)				
Komut	**MQCMDS için komut tanıtımı**	**MQCMDS için erişim düzeyi**	**MQADMIN ya da MXADMIN komut kaynağı tanıtımı**	**MQADMIN ya da MXADMIN erişim düzeyi**
Konu Sorgula	hlq.DISPLAY.TOPIC	READ	Denetim yok	-
Konu Adlarını Sorgula	hlq.DISPLAY.TOPIC	READ	Denetim yok	-
Konu Durumunu Sorgula	hlq.DISPLAY.TPSTATUS	READ	Denetim yok	-
Ping Kanalı	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kümeyi Yenile	hlq.REFRESH.CLUSTER	ALTER	Denetim yok	-
Güvenliği Yenile	hlq.REFRESH.SECURITY	ALTER	Denetim yok	-
Kanalı Sıfırla	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kanalı Çözümle	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kanal Doğrulama Kaydını Ayarla	hlq.SET.CHLAUTH	CONTROL	Denetim yok	-
Başlangıç Kanalı	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Kanalı Durdur	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

z/OS *Komut kaynağı güvenliği için tanıtımlar*

Komut kaynağı güvenliği anahtar profilini tanımlamadıysanız, komutlarla ilişkili kaynaklar için güvenlik denetimi yapmak istiyorsanız, her kaynak için uygun sınıfa kaynak tanıtımları eklemelisiniz. Aynı güvenlik profilleri, hem MQSC hem de PCF komutlarını denetler.

Komut kaynağı güvenliği anahtar profilini (`hlq.NO.CMD.RESC.CHECKS`) tanımlamadıysanız, komutlarla ilişkili kaynaklar için güvenlik denetimi yapmak istiyorsanız, şunları yapmak gerekir:

- Her kaynak için büyük harfli tanıtımlar kullanılıyorsa, **MQADMIN** sınıfına bir kaynak tanıtımı ekleyin.
- Her kaynak için karma vaka profilleri kullanılıyorsa, **MXADMIN** sınıfına bir kaynak profili ekleyin.

Aynı güvenlik profilleri, hem MQSC hem de PCF komutlarını denetler.

Komut kaynağı güvenliği denetimi için profiller formu alır:

```
hlq.type.resourcename
```

Burada `hlq` , `qmgr-name` (kuyruk yöneticisi adı) ya da `qsg-name` (kuyruk paylaşım grubu adı) olabilir.

Kuyruk yöneticisi adının önekli olduğu bir tanıtım, o kuyruk yöneticisiyle ilgili komutlarla ilişkili kaynaklara erişimi denetler. Kuyruk paylaşım grubu adının önekli olduğu bir tanıtım, kuyruk paylaşım grubu içindeki tüm kuyruk yöneticilerindeki komutlarla ilişkili kaynaklara erişimi denetler. Bu erişim, o kuyruk yöneticisininde o komut kaynağı için bir kuyruk yöneticisi düzeyi tanıtımı tanımlayarak, bir kuyruk yöneticisininde geçersiz kılınabilir.

Kuyruk yöneticiniz bir kuyruk paylaşım grubunun üyesiyse ve hem kuyruk yöneticisi, hem de kuyruk paylaşım grubu düzeyinde güvenlik kullanıyorsanız, IBM MQ önce kuyruk yöneticisi adı önekli bir profil için denetler. Bir değer bulamazsa, kuyruk paylaşım grubu adının başına önek olarak eklenmiş bir tanıtımı arar.

For example, the RACF profile name for command resource security checking against the model queue CREDIT.WORTHY in subsystem CSQ1 is:

```
CSQ1.QUEUE.CREDIT.WORTHY
```

Tüm komut kaynağı tiplerine ilişkin tanıtımlar MQADMIN sınıfında tutulduğu için, aynı adı sahip farklı tipteki kaynakları ayırt etmek için tanıtımda tanıtım adının "type" kısmına gerek vardır. Tanıtım adının "tip" kısmı KANAL, KUYRUK, KONU, süreç ya da NAMELIST olabilir. Örneğin, bir kullanıcının hlq.QUEUE.PAYROLL.ONE, ancak hlq.PROCESS.PAYROLL.ONE

Kaynak tipi bir kuyruksa ve tanıtım, kuyruk paylaşım grubu düzeyinde bir tanıtımsa, kuyruk paylaşım grubundaki bir ya da daha çok yerel kuyruğa erişimi ya da kuyruk paylaşım grubundaki herhangi bir kuyruk yöneticisinden tek bir paylaşılan kuyruğa erişimi denetler.

z/OS MQSC komutları, profiller ve erişim düzeyleri shows, for each IBM MQ MQSC command, the profiles required for command security checking to be carried out, and the corresponding access level for each profile in the MQCMDS class.

z/OS PCF komutları, tanıtımlar ve erişim düzeyleri shows, for each IBM MQ PCF command, the profiles required for command security checking to be carried out, and the corresponding access level for each profile in the MQCMDS class.

z/OS *Diğer ad kuyrukları ve uzak kuyruklar için komut kaynağı güvenliği denetimi*
Diğer ad kuyruğu ve uzak kuyruklar, başka bir kuyruk için yön sağlar. Bu kuyruklar için güvenlik denetimini dikkate aldığınızda ek noktalar uygulanır.

Diğer Adlar

Bir diğer ad kuyruğu tanımladığınızda, komut kaynağı güvenliği denetimleri yalnızca diğer ad kuyruğunun adına göre gerçekleştirilir; diğer ad, diğer adın çözdüğü hedef kuyruğun adına göre değil.

Diğer ad kuyrukları, hem yerel, hem de uzak kuyruklara çözülabilir. Kullanıcıların belirli yerel ya da uzak kuyruklara erişmelerine izin vermek istemiyorsanız, aşağıdakilerden her ikisini de yapmanız gerekir:

1. Kullanıcıların bu yerel ve uzak kuyruklara erişmelerine izin verilmez.
2. Kullanıcıların bu kuyruklar için diğer adları tanımlayabilmesinden kısıtlayın. Yani, bu, QALIAS ve ALTER QALIAS komutlarının tanımlanmasını engelleyin.

Uzak kuyruklar

Bir uzak kuyruk tanımladığınızda, komut kaynağı güvenliği denetimleri yalnızca uzak kuyruk adına göre gerçekleştirilir. Uzak kuyruk nesnesi tanımlamasındaki RNAME ya da XMITQ özniteliklerinde belirlenen kuyrukların adlarına karşı denetim gerçekleştirilmez.

z/OS RESVELL güvenlik profili

API-kaynak güvenliği için denetlenen kullanıcı kimliklerinin sayısını denetlemek için MQADMIN ya da MXADMIN sınıfında özel bir profil tanımlayabilirsiniz. Bu tanıtıma RESLEVEL tanıtımı adı verilir. Bu profil API 'yi nasıl etkiler-kaynak güvenliği, IBM MQ' e nasıl erişmenize bağlıdır.

When an application tries to connect to IBM MQ, IBM MQ checks the access that the user ID associated with the connection has to a profile in the MQADMIN or MXADMIN class called:

```
hlq.RESLEVEL
```

Burada `hlq` , `ssid` (altsistem tanıtıcısı) ya da `qsg` (kuyruk paylaşım grubu tanıtıcısı) olabilir.

Her bir bağlantı tipiyle ilişkilendirilen kullanıcı kimlikleri şunlardır:

- Toplu iş bağlantılarına ilişkin bağlama görevinin kullanıcı kimliği
- CICS bağlantıları için CICS adres alanı kullanıcı kimliği
- IMS bağlantıları için IMS bölgesi adres alanı kullanıcı kimliği
- Kanal başlatıcı bağlantıları için kanal başlatıcı adres alanı kullanıcı kimliği

Uyarı: RESLELEL çok güçlü bir seçenektir; belirli bir bağlantı için tüm kaynak güvenliği denetimlerinin atlanmasına neden olabilir.

Tanımlanmış bir RESLEVEL tanıtımınız yoksa, MQADMIN sınıfındaki başka bir tanıtıma hlq.RESLEVELeşleşmediği için dikkat etmeniz gerekir. Örneğin, MQADMIN ' de hlq. * * olarak adlandırılan bir tanıtımınız varsa ve no hlq.RESLEVEL profili, hlq. * * ' nin sonuçlarından dikkat edin. RESLEVELL denetimi için kullanıldığı için tanıtım.

Bir hlq.RESLEVEL tanıtımı tanımlayın ve RESLEVEL tanıtımı olmasın yerine UACC ' yi NONE (Yok) değerine ayarlayın. Erişim listesinde mümkün olduğunca az sayıda kullanıcı ya da grup bulundur. RESLELEL erişimi denetlenmesine ilişkin ayrıntılar için bkz. “z/OSile ilgili denetim konuları” sayfa 246.

If you are using queue manager level security only, IBM MQ performs RESLEVEL checks against the `qmgr-name.RESLEVEL` profile. If you are using queue sharing group level security only, IBM MQ performs RESLEVEL checks against the `qsg-name.RESLEVEL` profile. Hem kuyruk yöneticisi hem de kuyruk paylaşım grubu düzeyinde güvenlik birleşimi kullanıyorsanız, IBM MQ önce kuyruk yöneticisi düzeyinde RESLEFIL tanıtımının var olup olmadığını denetler. Bir değer bulamazsa, kuyruk paylaşım grubu düzeyinde RESLEFIL tanıtımını denetler.

RESLEL tanıtımı bulamazsa, IBM MQ , bir CICS ya da IMS bağlantısı için hem iş hem de görev (ya da diğer kullanıcı) tanıtıcısının denetlenmesine olanak sağlar. Bir toplu iş bağlantısı için IBM MQ , iş (ya da diğer) kullanıcı kimliğinin denetlenmesini etkinleştirir. Kanal başlatıcısı için IBM MQ , kanal kullanıcı kimliğinin ve MCA (ya da diğer) kullanıcı kimliğinin denetlenmesini etkinleştirir.

RESLEVL tanıtımı varsa, denetleme düzeyi, tanıtıma ilişkin ortama ve erişim düzeyine bağlıdır.

Remember that if your queue manager is a member of a queue sharing group and you do not define this profile at queue manager level, there might be one defined at queue sharing group level that will affect the level of checking.To activate the checking of two user IDs, you define a RESLEVEL profile (prefixed with either the queue manager name of the queue sharing group name) with a UACC(NONE) and ensure that the relevant users do not have access granted against this profile.

Kanal başlatıcısının kullanıcı kimliğinin RESLEFIL ' e erişimini dikkate aldığınızda, kanal başlatıcısı tarafından kurulan bağlantının, kanalların kullandığı bağlantı olduğunu unutmayın. Kanal başlatıcısının kullanıcı kimliği için tüm kaynak güvenliği denetimlerinin atlanmasına neden olan bir ayar, tüm kanallara ilişkin güvenlik denetimlerini etkin bir şekilde atlar. Kanal başlatıcısının RESLELEL için kullanıcı kimliği NONE dışında bir değer varsa, erişim için yalnızca bir kullanıcı kimliği (bir okuma ya da UPDATE için erişim düzeyi için) ya da kullanıcı kimliği (CONTROL ya da ALTER erişim düzeyi için) denetlenmez. Kanal başlatıcının kullanıcı kimliğine RESVELL değeri için NONE dışında bir erişim düzeyi verirseniz, kanal için yapılan güvenlik denetimlerinde bu ayarın etkisini anladığınızdan emin olun.

RESFIELL tanıtımının kullanılması, olağan güvenlik denetleme kayıtlarının alınmamasını sağlar. Örneğin, bir kullanıcıya UAUDIT öğesini koyarsanız, MQADMIN ' deki hlq.RESLEVEL tanıtıma erişimi denetlenmez.

hlq.RESLEVEL tanıtımında RACF WARNING seçeneğini kullanırsanız, RESLEVL sınıfındaki tanıtımlar için RACF uyarı iletileri üretilmez.

COD gibi rapor iletileri için güvenlik denetimi, kaynak uygulama ile ilişkili RESLEVEL tanıtımıyla denetlenir. Örneğin, bir toplu işin kullanıcı kimliği RESFILEL tanıtıma CONTROL ya da ALTER yetkisine sahipse, rapor iletilerinin güvenlik denetimi de içinde olmak üzere, toplu iş tarafından gerçekleştirilen tüm kaynak denetimi atlanır.

RESLEVL tanıtımını değiştirirseniz, değişiklik gerçekleşmeden önce kullanıcıların bağlantıyı kesmesi ve yeniden bağlanması gerekir. (Bu, dağıtılmış kuyruğa alma adres alanı kullanıcı kimliğinin RESLEVEL tanıtımı değiştirildiğinde, kanal başlatıcının durdurulmasına ve yeniden başlatılmasına da dahildir.)

RESLEVEL denetimini kapatmak için REAUDIT sistem parametresini kullanın.

z/OS *RESVEL ve toplu iş bağlantıları*

Varsayılan olarak, bir IBM MQ kaynağına toplu iş ve toplu iş tipi bağlantılarıyla erişiliyorsa, kullanıcının bu kaynağa erişim yetkisi olması gerekir. Uygun bir RESLEFIL tanımlaması belirleyerek güvenlik denetimini atlayabilirsiniz.

Kullanıcının denetlenmiş olup olmadığı, bağlanma sırasında kullanılan kullanıcı kimliğine, bağlantı denetimi için kullanılan kullanıcı kimliğine dayalı olarak mı, yoksa değil mi?

Örneğin, RESLEVL ayarlayabilirsiniz; böylece, güvendiğiniz bir kullanıcı belirli kaynaklara toplu iş bağlantısıyla eriştiğinde, hiçbir API-kaynak güvenlik denetimi gerçekleştirilmez; ancak güvenmediğiniz bir kullanıcı aynı kaynaklara erişmeyi denediğinde, güvenlik denetimleri olağan şekilde yürütülür. Yalnızca kullanıcıya ve o kullanıcı tarafından çalıştırılan programlara yeterince güvendiğinizde API kaynak güvenliği denetimlerini atlamak için RESLEFIL denetimini ayarlamalısınız.

Aşağıdaki tabloda toplu bağlantılar için yapılan çekler gösterilmektedir.

Çizelge 52. Toplu bağlantılar için farklı RACF erişim düzeylerinde yapılan denetimler

RACF erişim düzeyi	**Denetleme düzeyi**
YOK	Kaynak denetimleri gerçekleştirildi
READ	Kaynak denetimleri gerçekleştirildi
GÜNCELLE	Kaynak denetimleri gerçekleştirildi
CONTROL	Kontrol yok.
ALTER	Kontrol yok.

z/OS *RESLELEL ve sistem iÝlevleri*

İşlem ve denetim panolarına ve CSQUTIL ' e RESLEVELL uygulaması.

İşlem ve denetim panoları ve CSQUTIL yardımcı programı, kuyruk yöneticisinin komut sunucusuna yönelik istekleri oluşturan toplu iş tipi uygulamalardır ve bu nedenle “RESVEL ve toplu iş bağlantıları” sayfa 222içinde açıklanan hususlara tabi olur. RESLELEL kullanarak, kullandıkları SYSTEM.COMMAND.INPUT ve SYSTEM.COMMAND.REPLY.MODEL kuyruklarına ilişkin güvenlik denetimini atlamak için, ancak SYSTEM.CSQXCMDdinamik kuyrukları için kullanamazsınız. *, SYSTEM.CSQOREXX.*, ve SYSTEM.CSQUTIL. *.

Komut sunucusu, kuyruk yöneticisinin ayrılmaz bir parçasıdır ve kendisiyle ilişkilendirilmiş bir bağlantı ya da RESLEVEL denetimi yapmamaktadır. Bu nedenle, güvenlik sağlamak için, komut sunucusu, istekte bulunan uygulamanın kullanıcı kimliğinin, yanıtlar için kullanılan kuyruğu açma yetkisinin olduğunu doğrulamalıdır. İşlemler ve denetim panoları için bu SYSTEM.CSQOREXX. *. CSQUTIL için, SYSTEM.CSQUTIL. *. Kullanıcıların, bu kuyrukları (“Sistem kuyruğu güvenliği” sayfa 196içinde açıklandığı gibi), verilen tüm RESDüL yetkilendirmesine ek olarak kullanabilmeleri için yetki edinmeleri gerekir.

Komut sunucusunu kullanan diğer uygulamalar için, adı yanıtlarının gönderileceği kuyruk olarak adlanandır. Bu tür diğer uygulamalar, komut sunucusunu, komut sunucusuna göre daha güvenilir bir kullanıcı kimliği geçirerek (ileti bağlamında) yetkisiz kuyruklara ileti yerleştirmeye yardımcı olabilir. Bunu önlemek için, SYSTEM.COMMAND.INPUT.

z/OS *RESLELEL ve CICS bağlantıları*

Varsayılan olarak, bir CICS bağlantısında API kaynağı güvenlik denetimi yapıldığında, iki kullanıcı kimliği denetlenir. RESLEVEL tanıtımı ayarlanarak hangi kullanıcı kimliklerinin denetlendiğini değiştirebilirsiniz.

İlk olarak denetlenen ilk kullanıcı kimliği, CICS adres alanının adını içerir. Bu, CICS işinin iş kartındaki kullanıcı kimliğidir ya da z/OS STARTED sınıfı ya da başlatılmış yordamlar tablosu tarafından CICS başlatma görevine atanmış olan kullanıcı kimliği. (CICS DFLTEUSER değil.)

Denetlenen ikinci kullanıcı kimliği, CICS işlemiyle ilişkili olan kullanıcı kimliğidir.

Bu kullanıcı kimliklerinden birinin kaynağa erişimi yoksa, istek MQRC_NOT_AUTULIZED tamamlanma koduyla başarısız olur. Hem CICS adresi alanı kullanıcı kimliği, hem de CICS işlemini çalıştıran kişinin kullanıcı kimliği, kaynağa doğru düzeyde erişimleri olmalıdır.

RESVEL ' in yapılan çekleri nasıl etkileyebileceği

RESELELL tanıtımınızı nasıl ayarlamanıza bağlı olarak, bir kaynağa erişim istendiğinde hangi kullanıcı kimliklerinin denetlenmiş olduğunu değiştirebilirsiniz. Ek bilgi için Çizelge 53 sayfa 224 başlıklı konuya bakın.

Denetlenen kullanıcı kimlikleri, bağlantı sırasında kullanılan kullanıcı kimliğine (yani, CICS adres alanı kullanıcı kimliği) bağlı olarak değişir. Bu denetim öğesi, bir sistemden gelen IBM MQ istekleri (örneğin, bir test sistemi, TESTCICS,) ancak bunları başka bir sisteme (örneğin, bir üretim sistemi, PRODCICS) uygulamak için API kaynak güvenlik denetimini atmanızı sağlar.

Not: If you set up your CICS address space user ID with the "güvenilen" attribute in the STARTED class or the RACF started procedures table ICHRIN03, this overrides any user ID checks for the CICS address space established by the RESLEVEL profile for your queue manager (that is, the queue manager does not perform the security checks for the CICS address space). Daha fazla bilgi için *CICS Transaction Server for z/OS V3.2 RACF Security Guide*adlı yayına bakın.

Aşağıdaki tabloda, CICS bağlantıları için yapılan denetimler gösterilmektedir.

Çizelge 53. CICS bağlantıları için farklı RACF erişim düzeylerinde yapılan denetimler

RACF erişim düzeyi	**Denetleme düzeyi**
YOK	IBM MQ , CICS adres alanı kullanıcı kimliğini ve işlem kullanıcı kimliğini denetler.
READ	IBM MQ , yalnızca CICS adres alanı kullanıcı kimliğini denetler.
GÜNCELLE	Hareket, RESSEC (YES) ile CICS olarak tanımlandıysa, IBM MQ , CICS adres alanı kullanıcı kimliğini ve işlem kullanıcı kimliğini denetler.
GÜNCELLE	Hareket RESSEC (NO) ile CICS olarak tanımlandıysa, IBM MQ yalnızca CICS adres alanı kullanıcı kimliğini denetler.
CONTROL ya da ALTER	IBM MQ , hiçbir kullanıcı kimliğini denetmiyor.

z/OS *RESLELEL ve IMS bağlantıları*

Varsayılan olarak, bir IMS bağlantısı için API kaynağı güvenliği denetimi yapıldığında, iki kullanıcı kimliği denetlenir. RESLEVEL tanıtımı ayarlanarak hangi kullanıcı kimliklerinin denetlendiğini değiştirebilirsiniz.

Varsayılan olarak, bir IMS bağlantısı için API kaynağı güvenliği denetimi yapıldığında, kaynağa erişimin izin verilip verilmediğini görmek için iki kullanıcı kimliği denetlenir.

İlk olarak denetlenen ilk kullanıcı kimliği, IMS bölgesinin adres alanının yer aldığından emin olun. This is taken from either the USER field from the job card or the user ID assigned to the region from the z/OS STARTED class or the started procedures table (SPT).

İşaretlenen ikinci kullanıcı kimliği, bağımlı bölgede yapılan çalışmayla ilişkilendirilir. It is determined according to the type of the dependent region as shown in İkinci kullanıcı kimliğinin IMS(tm) bağlantısı için nasıl saptanması.

Birinci ya da ikinci IMS kullanıcı kimliğinin kaynağa erişimi yoksa, istek MQRC_NOT_YETKILI tamamlanma kodu ile başarısız olur.

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. Bu kullanıcı kimliği, tetikleme izleyicisinin PSBNAME 'sidir ve varsayılan olarak CSQQTRMN 'dir.

RESVEL ' in yapılan çekleri nasıl etkileyebileceği

RESELELL tanıtımınızı nasıl ayarlamanıza bağlı olarak, bir kaynağa erişim istendiğinde hangi kullanıcı kimliklerinin denetlenmiş olduğunu değiştirebilirsiniz. Olası denetimler şunlardır:

- IMS bölge adresi alanı kullanıcı kimliğini ve ikinci kullanıcı kimliğini ya da diğer kullanıcı kimliğini denetleyin.
- Yalnızca IMS bölge adres alanı kullanıcı kimliğini denetleyin.
- Hiçbir kullanıcı kimliğini kontrol etmemek.

Aşağıdaki tabloda, IMS bağlantıları için yapılan denetimler gösterilmektedir.

Çizelge 54. IMS bağlantıları için farklı RACF erişim düzeylerinde yapılan denetimler

RACF erişim düzeyi	**Denetleme düzeyi**
YOK	IMS adres alanı kullanıcı kimliğini ve IMS ikinci kullanıcı kimliğini ya da diğer kullanıcı kimliğini denetleyin.
READ	IMS adres alanı kullanıcı kimliğini denetleyin.
GÜNCELLE	IMS adres alanı kullanıcı kimliğini denetleyin.
CONTROL	Kontrol yok.
ALTER	Kontrol yok.

z/OS *RESLELEL ve kanal başlatıcı bağlantısı*

Varsayılan olarak, kanal başlatıcısı tarafından bir API kaynağı güvenlik denetimi yapıldığında, iki kullanıcı kimliği denetlenir. RESLEVEL tanıtımı ayarlanarak hangi kullanıcı kimliklerinin denetlendiğini değiştirebilirsiniz.

Varsayılan olarak, kanal başlatıcısı tarafından bir API kaynağı güvenlik denetimi yapıldığında, kaynağa erişilmesine izin verilip verilmediğini görmek için iki kullanıcı kimliği denetlenir.

Denetlenen kullanıcı kimlikleri, ağ tarafından alınan MCAUSER kanal özniteliğinden, kanal başlatıcı adres alanının ya da ileti tanımlayıcısının diğer kullanıcı kimliğininse belirtilebilir. Hangi kullanıcı kimliklerinin denetlendiği, kullandığınız iletişim protokolünün ve PUUTAT kanal özniteliğinin ayarına bağlıdır. Ek bilgi için “Kanal başlatıcısı tarafından kullanılan kullanıcı kimlikleri” sayfa 230 başlıklı konuya bakın.

Bu kullanıcı kimliklerinden birinin kaynağa erişimi yoksa, istek MQRC_NOT_AUTULIZED tamamlanma koduyla başarısız olur.

RESVEL ' in yapılan çekleri nasıl etkileyebileceği

RESELELL tanıtımınızı nasıl ayarlamanıza bağlı olarak, bir kaynağa erişim istendiğinde hangi kullanıcı kimliklerinin denetleneceğini ve kaç tane denetlendiğini değiştirebilirsiniz.

Aşağıdaki çizelge, kanal başlatıcısının bağlantısı için yapılan denetimleri ve bu bağlantıyı kullandığından bu yana tüm kanallar için yapılan denetimleri göstermektedir.

Çizelge 55. Kanal başlatıcı bağlantıları için farklı RACF erişim düzeylerinde yapılan denetimler

RACF erişim düzeyi	**Denetleme düzeyi**
YOK	İki kullanıcı kimliğini denetleyin.
READ	Bir kullanıcı kimliğini denetleyin.
GÜNCELLE	Bir kullanıcı kimliğini denetleyin.
CONTROL	Kontrol yok.
ALTER	Kontrol yok.
Not: Denetlenmiş kullanıcı kimliklerinin bir tanımı için bkz. “Kanal başlatıcısı tarafından kullanılan kullanıcı kimlikleri” sayfa 230	

z/OS *RESLELEL ve grup içi kuyruğa alma*

Varsayılan olarak, grup içi kuyruğa alma aracısı tarafından bir API kaynağı güvenlik denetimi yapıldığında, kaynağa erişilmesine izin verilip verilmediğini görmek için iki kullanıcı kimliği denetlenir. RESLEVEL tanıtımı ayarlanarak hangi kullanıcı kimliklerinin denetlendiğini değiştirebilirsiniz.

The user IDs checked can be the user ID determined by the IGQUSER attribute of the receiving queue manager, the user ID of the queue manager within the queue sharing group that put the message on to the SYSTEM.QSG.TRANSMIT.QUEUE, or the alternate user ID specified in the *UserIdentifier* field of the message descriptor of the message. Ek bilgi için “Grup içi kuyruğa alma aracısı tarafından kullanılan kullanıcı kimlikleri” sayfa 234 başlıklı konuya bakın.

Grup içi kuyruğa alma aracısı bir iç kuyruk yöneticisi görevi olduğu için, belirtik bir bağlantı isteği yayınlamaz ve kuyruk yöneticisinin kullanıcı kimliği altında çalışır. Grup içi kuyruğa alma aracısı, kuyruk yöneticisi kullanıma hazırlanmaya başlar. Grup içi kuyruğa alma aracısının kullanıma hazırlanması sırasında, IBM MQ , kuyruk yöneticisiyle ilişkilendirilmiş kullanıcı kimliğinin, MQADMIN sınıfındaki bir tanıtıma sahip olduğu erişimi denetler:

```
hlq.RESLEVEL
```

Bu denetim, her zaman hlq.NO.SUBSYS.SECURITY anahtarı ayarlanmadığı sürece gerçekleştirilir.

RESLEL tanıtımı yoksa, IBM MQ iki kullanıcı kimliği olup olmadığını denetlemesini etkinleştirir. RESPELL tanıtımı varsa, denetleme düzeyi, tanıtıma ilişkin kuyruk yöneticisinin kullanıcı kimliğine verilen erişim düzeyine bağlıdır. Grup içi kuyruğa alma aracısı için farklı RACF(r) erişim düzeylerinde yapılan denetimler , grup içi kuyruğa alma aracısı için yapılan çekleri gösterir.

Çizelge 56. Grup içi kuyruğa alma aracısı için farklı RACF erişim düzeylerinde yapılan denetimler

RACF erişim düzeyi	**Denetleme düzeyi**
YOK	İki kullanıcı kimliğini denetleyin.
READ	Bir kullanıcı kimliğini denetleyin.
GÜNCELLE	Bir kullanıcı kimliğini denetleyin.
CONTROL	Kontrol yok.
ALTER	Kontrol yok.
Not: Denetlenmiş kullanıcı kimliklerinin bir tanımı için bkz. “Grup içi kuyruğa alma aracısı tarafından kullanılan kullanıcı kimlikleri” sayfa 234	

Kuyruk yöneticisinin kullanıcı kimliği için RESLEVEL tanıtıma izin verilen izinler değiştirilirse, yeni izinleri almak için grup içi kuyruğa alma aracısı durdurulmalı ve yeniden başlatılmalıdır. Grup içi kuyruğa alma aracısını bağımsız olarak durdurmanın ve yeniden başlatmanın bir yolu olmadığından, bunu gerçekleştirmek için kuyruk yöneticisi durdurulmalı ve yeniden başlatılmalıdır.

z/OS *RESLELEL ve kullanıcı kimlikleri denetlendi*

RESLEVL tanıtımı ayarlayıp buna erişim verilme örneği.

Toplu iş bağlantılarına ilişkin profil adını denetleyerek kullanıcı kimliği denetimi - LU 6.2 ve TCP/IP sunucusu bağlantı kanallarının tanıtım adına göre kullanıcı kimlikleri denetlenir , RESVLEL ' in farklı MQI istekleri için hangi kullanıcı kimliklerinin denetlendiğini gösterir.

Örneğin, aşağıdaki gereksinimlerle QM66 adlı bir kuyruk yöneticiniz var:

- Kullanıcı WS21B , kaynak güvenliğinden muaf tutulacak.
- CICS , adres alanı kullanıcı kimliği CICSSWXN altında çalışan WXNCICS görevini, yalnızca RESSEC (YES) ile tanımlanan işlemler için tam kaynak denetleyişi gerçekleştirmek üzere başlatıldı.

Uygun RESLEVEL tanıtımını tanımlamak için aşağıdaki RACF komutunu verin:

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

Daha sonra, aşağıdaki komutları kullanarak kullanıcılara bu tanıtıma erişim yetkisi verin:

```
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(WS21B) ACCESS(CONTROL)
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(CICSWXN) ACCESS(UPDATE)
```

If you make these changes while the user IDs are connected to queue manager QM66, the users must disconnect and connect again before the change takes place.

Bir kullanıcı bağlandığında ancak, altsistem güvenliği etkin değilse, altsistem güvenliği etkin duruma gelir ve kullanıcı için tam kaynak güvenliği denetimi uygulanır. Doğru RESLEFIL işlemini almak için kullanıcının yeniden bağlanması gerekir.

z/OS z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri

IBM MQ , kullanıcılar, uçbirimler, uygulamalar ve diğer kaynaklarla ilişkili kullanıcı kimliklerine dayalı güvenlik denetimlerini başlatır. Bu konular derlemi, her güvenlik denetimi tipi için hangi kullanıcı kimliklerinin kullanıldığını listeler.

z/OS *Bağlantı güvenliği için kullanıcı kimlikleri*

Bağlantı güvenliği için kullanılan kullanıcı kimliği, bağlantı tipine bağlıdır.

Bağlantı tipi	**Kullanıcı kimliği içeriği**
Toplu iş bağlantısı	Bağlanılan görevin kullanıcı kimliği. Örneğin: • TSO kullanıcı kimliği • USER JCL parametresi tarafından bir toplu iş için atanan kullanıcı kimliği • STARTED sınıfı ya da başlatılmış yordamlar tablosu tarafından başlatılan bir göreve atanan kullanıcı kimliği
CICS bağlantı	CICS adres alanı kullanıcı kimliği.
IMS bağlantı	IMS bölge adresi alanı kullanıcı kimliği.
Kanal başlatıcı bağlantısı	Kanal başlatıcı adres alanı kullanıcı kimliği.

z/OS *Komut ve komut kaynağı güvenliği için kullanıcı kimlikleri*

Komut güvenliği ya da komut kaynağı güvenliği için kullanılan kullanıcı kimliği, komutun yayınlandığı yere bağlıdır.

Bu kaynak ...	**Kullanıcı kimliği içeriği**
CSQINP1, CSQINP2ya da CSQINPT	Denetim yapılmadı.
Sistem komutu giriş kuyruğu	Komutu içeren iletinin ileti tanımlayıcısının *UserIdentifier* ' inde bulunan kullanıcı kimliği. İleti bir *UserIdentifier*içermiyorsa, güvenlik yöneticisine bir kullanıcı kimliği boşluk karakteri geçirilir.
Konsol	Kullanıcı kimliği konsolda oturum açmış. Konsol oturum açmazsa, CSQ6SYSP' deki CMDUSER sistem değiştirgesinin varsayılan kullanıcı kimliği belirlenir. Bir konsoldan komut vermek için, konsolda z/OS SYS AUTHORITY özniteliği bulunmalıdır.

Bu kaynak ...	Kullanıcı kimliği içeriği
SDSF/TSO konsolu	TSO ya da iş kullanıcı kimliği.
İşlemler ve denetim panoları	TSO kullanıcı kimliği. İşlemleri ve denetim panolarını kullanabildiyseniz, seçtiğiniz işlemlere karşılık gelen komutları vermek için uygun yetkiye sahip olmanız gerekir. Ayrıca, tüm hlq.DISPLAYokuma erişimine sahip olmanız gerekir. Panolar, sundukları bilgileri toplamak için çeşitli DISPLAY komutlarını kullanacağından, MQCMDS sınıfındaki*nesne* tanıtımlarını kullanın.
MGCRE	MGCRE, UTOKEN ile kullanılırsa, UTOKEN kullanıcı kimliği kullanılır. MGCRE, UTOKEN olmadan yayınlanırsa, TSO ya da iş kullanıcısı kimliği kullanılır.
CSQ0UTIL	İş kullanıcı kimliği.
CSQUTIL	İş kullanıcı kimliği.
CSQINPX	Kanal başlatıcı adres alanına ilişkin kullanıcı kimliği.

z/OS *Kaynak güvenliği için kullanıcı kimlikleri (MQOPEN, MQSUB ve MQPUT1)*

Bu bilgiler, her bağlantı tipine ilişkin normal ve diğer kullanıcı kimliklerine ilişkin kullanıcı kimliklerinin içeriğini gösterir. Denetim sayısı, RESLEFIL tanıtımlarıyla tanımlanır. The user ID checked is that used for **MQOPEN**, **MQSUB**, or **MQPUT1** calls.

Not: Tüm kullanıcı kimliği alanları, tam olarak alındıkları şekilde denetlenir. Dönüştürmeler gerçekleşmez ve örneğin, "Bob", "BOB"ve "bob" içeren üç kullanıcı kimliği alanı eşdeğer değildir.

z/OS *Toplu iş bağlantıları için denetlenen kullanıcı kimlikleri*

Bir toplu iş bağlantısı için denetlenen kullanıcı kimliği, görevin nasıl çalıştırıldığı ve diğer bir kullanıcı kimliğinin belirlenmesine bağlı olarak değişir.

Çizelge 57. Toplu iş bağlantılarına ilişkin profil adını denetleyerek kullanıcı kimliği denetimi

Açık olarak başka bir kullanıcı kimliği belirlendi mi?	hlq.ALTERNATE.USER.userid tanıtımı	hlq.CONTEXT.queuename tanıtımı	hlq.resourcename profili
Hayır	-	İŞ	İŞ
Evet	İŞ	İŞ	Alt

Anahtar:

Alt
Diğer kullanıcı kimliği.

İŞ

- Bir TSO ya da USS oturum açma (USS) oturum açma kullanıcı kimliği.
- Toplu iş için atanan kullanıcı kimliği.
- STARTED sınıfı ya da başlatılmış yordamlar tablosu tarafından başlatılan bir göreve atanan kullanıcı kimliği.
- Yürütülen Db2 saklanmış yordamıyla ilişkili kullanıcı kimliği

A Batch job is performing an MQPUT1 to a queue called Q1 with RESLEVEL set to READ and alternate user ID checking turned off.

Toplu bağlantılar için farklı RACF(r) erişim düzeylerinde yapılan denetimler ve Toplu iş bağlantılarına ilişkin profil adını denetleyerek kullanıcı kimliği denetimi , iş kullanıcı kimliğinin hlq.Q1tanıtıma göre denetlendiğini gösterir.

z/OS *User IDs checked for CICS connections*

CICS bağlantıları için denetlenen kullanıcı kimlikleri, bir ya da iki denetin gerçekleştirilip gerçekleştirilmeyeceğine ve diğer bir kullanıcı kimliğinin belirtilip belirtilmediğine bağlıdır.

Çizelge 58. CICS-type kullanıcı kimlikleri için profil adını denetleyerek kullanıcı kimliği denetimi

Açık olarak başka bir kullanıcı kimliği belirlendi mi?	hlq.ALTERNATE.USER.userid tanıtımı	hlq.CONTEXT.queuename tanıtımı	hlq.resourcename profili
Hayır, 1 denetim	-	ADS	ADS
Hayır, 2 denetim	-	ADS + TXN	ADS + TXN
Evet, 1 denetimi	ADS	ADS	ADS
Evet, 2 çek	ADS + TXN	ADS + TXN	ADS + ALT

Anahtar:

Alt
Diğer kullanıcı kimliği

ADS
CICS toplu işi ile ilişkili kullanıcı kimliği ya da CICS başlatılmış bir görev olarak çalışıyorsa, STARTED sınıfı ya da başlatma yordamları tablosu aracılığıyla.

TXN
CICS işlemiyle ilişkili kullanıcı kimliği. Bu olağan durumda, işlemi başlatan uçbirim kullanıcısının kullanıcı kimliğidir. It can be the CICS DFLTUSER, a PRESET security terminal, or a manually signed-on user.

Aşağıdaki koşullar için denetlenen kullanıcı kimliklerini saptayın:

- Bir CICS adres alanı kullanıcı kimliği için, RESLEVEL tanıtıma RACF erişim düzeyi NONE olarak ayarlanır.
- MQOO_OUTPUT ve MQOO_PASST_IDENTITY_CONTEXT içeren bir kuyruk için MQOPEN çağrısı yapılıyor.

Önce, RESLEFIL tanıtımına CICS adres alanı kullanıcı kimliği erişimi temelinde kaç CICS kullanıcı kimliği denetlendiğini görün. “RESLELEL ve CICS bağlantıları” sayfa 223konusunda Çizelge 53 sayfa 224 ' dan, RESLEFEL tanıtımı NONE olarak ayarlandıysa iki kullanıcı kimliği denetlenir. Daha sonra, Çizelge 58 sayfa 229 ' tan bu denetimler gerçekleştirilmektedir:

- hlq.ALTERNATE.USER.userid tanıtımı denetlenmez.
- hlq.CONTEXT.queuename tanıtımı, hem CICS adres alanı kullanıcı kimliği, hem de CICS işlem kullanıcı kimliği ile denetlenir.
- hlq.resourcename tanıtımı, hem CICS adres alanı kullanıcı kimliği, hem de CICS işlem kullanıcı kimliği ile denetlenir.

Bu, bu MQOPEN çağrısı için dört güvenlik denetinin yapıldığını belirtir.

z/OS *User IDs checked for IMS connections*

IMS bağlantıları için denetlenen kullanıcı kimlikleri, bir ya da iki denetin gerçekleştirilip gerçekleştirilmeyeceğine ve diğer bir kullanıcı kimliğinin belirtilip belirtilmediğine bağlıdır. İkinci bir kullanıcı kimliği denetlenirse, bu kimlik, bağımlı bölgenin tipine ve kullanıcı kimliklerinin kullanılabilir olduğu tipe bağlıdır.

Çizelge 59. IMS-type kullanıcı kimlikleri için profil adını denetleyerek kullanıcı kimliği denetimi			
Açık olarak başka bir kullanıcı kimliği belirlendi mi?	**hlq.ALTERNATE.USER.userid tanıtımı**	**hlq.CONTEXT.queuename tanıtımı**	**hlq.resourcename profili**
Hayır, 1 denetim	-	YENİ	YENİ
Hayır, 2 denetim	-	REG + SEC	REG + SEC
Evet, 1 denetimi	YENİ	YENİ	YENİ
Evet, 2 çek	REG + SEC	REG + SEC	REG + ALT

Anahtar:

Alt
Diğer kullanıcı kimliği.

YENİ
Kullanıcı kimliği olağan durumda STARTED sınıfı ya da başlatılan yordamlar çizelgesi ya da IMS çalışıyorsa, USER JCL parametresiyle ayarlanır.

sn
İkinci kullanıcı kimliği, bağımlı bir bölgede yapılmakta olan çalışmayla ilişkilendirilir. Bu, Çizelge 60 sayfa 230değerine göre belirlenir.

Çizelge 60. How the second user ID is determined for the IMS connection	
Bağımlı bölge tipleri	**İkinci kullanıcı kimliğini belirlemeye ilişkin sıradüzeni**
• BMP iletisi yönlendirilen ve başarılı GET UNIQUE yayınlandı. • IFP ve GET UNIQUE yayınlandı. • MPP.	Kullanıcı oturum açmışsa, IMS işlemiyle ilişkili kullanıcı kimliği. Varsa, LTERM adı. PSBNAME.
• BMP iletisi yönlendirilen ve başarılı GET UNIQUE yayınlanmadı. • BMP iletilmedi. • IFP ve GET UNIQUE komutu verilmemiş.	IMS bağımlı bölge adresi boşluğuyla ilişkilendirilmiş olan kullanıcı kimliği, boşluk ya da tüm sıfırlar değilse, bu alan adresi alanı ile ilişkilendirilir. PSBNAME.

z/OS *Kanal başlatıcısı tarafından kullanılan kullanıcı kimlikleri*

Bu konular grubunda, giriş kanalları ve sunucu bağlantısı kanalları üzerinden gönderilen istemci MQI istekleri için kullanılan ve denetlenen kullanıcı kimlikleri açıklanır. TCP/IP ve LU6.2için bilgi sağlanır.

Kullanılacak güvenlik denetimi tipini saptamak için, alma kanalı tanımlamasının PUTAUT parametresini kullanabilirsiniz. IBM MQ ağınız boyunca tutarlı bir güvenlik denetimi yapmak için, ONLYMCA ve ALTMCA seçeneklerini kullanabilirsiniz.

MCA tarafından kullanılan kullanıcı kimliğini belirlemek için DISPLAY CHSTATUS komutunu kullanabilirsiniz.

z/OS *TCP/IP ' yi kullanarak kanal alma*

Denetlenmiş kullanıcı kimlikleri, kanalın PUTAUT seçeneğine ve bir ya da iki denetinin gerçekleştirilip gerçekleştirilmeyeceğini bağlıdır.

Çizelge 61. TCP/IP kanallarına ilişkin tanıtım adı için kimlik denetlenmiş kullanıcı kimlikleri			
Alıcıda ya da istekte bulunan kanalda PUUTAT seçeneği belirtildi	**hlq.ALTERNATE.USER.userid tanıtımı**	**hlq.CONTEXT.queuename tanıtımı**	**hlq.resourcename profili**
DEF, 1 denetimi	-	CHL	CHL
DEF, 2 denetimleri	-	CHL + MCA	CHL + MCA
CTX, 1 denetimi	CHL	CHL	CHL
CTX, 2 denetimleri	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 denetimi	-	MCA	MCA
ONLYMCA, 2 çek	-	MCA	MCA
ALTMCA, 1 denetimi	MCA	MCA	MCA
ALTMCA, 2 denetleme	MCA	MCA	MCA + ALT

Anahtar:

MCA (MCA kullanıcı kimliği)
Alıcıda MCAUSER kanal özniteliği için belirlenen kullanıcı kimliği; boşsa, alıcı ya da istek isteyen tarafın kanal başlatıcı adres alanı kullanıcı kimliği kullanılır.

CHL (Kanal kullanıcı kimliği)
TCP/IP ' de güvenlik, kanala ilişkin iletişim sistemi tarafından desteklenmiyor. Aktarım Katmanı Güvenliği (TLS) kullanılıyorsa ve ortaktan bir sayısal sertifika akıtıldıysa, bu sertifikaya (kuruluysa) ilişkin kullanıcı kimliği ya da RACF Sertifika Adı Süzgeci (CNF) kullanılarak bulunan eşleşen bir süzgeçle ilişkilendirilmiş kullanıcı kimliği kullanılır. İlişkili bir kullanıcı kimliği bulunamazsa ya da TLS kullanılmıyorsa, alıcı ya da istek sonunun kanal başlatıcı adres alanının kullanıcı kimliği, PUTAUT değiştirgesiyle DEF ya da CTX değerine ayarlanmış kanallarda kanal kullanıcı kimliği olarak kullanılır.

Not: RACF Certificate Name Filtering (CNF) kullanımı, aynı RACF kullanıcı kimliğini birden çok uzak kullanıcıya atamanıza olanak sağlar; örneğin, aynı kuruluş birimindeki tüm kullanıcılar, doğal olarak aynı güvenlik yetkisine sahip olur. Bu, sunucunun dünyadaki olası her uzak kullanıcının sertifikasının bir kopyasına sahip olması gerekmediği ve sertifika yönetimini ve dağıtımını büyük ölçüde basitleştirdiği anlamına gelir.

PUTAUT parametresi kanal için ONLYMCA ya da ALTMCA olarak ayarlandıysa, kanal kullanıcı kimliği yoksayılır ve alıcının MCA kullanıcı kimliği ya da istekçisi kullanılır. Bu, TLS kullanan TCP/IP kanalları için de geçerlidir.

ALT (Diğer kullanıcı kimliği)
Kullanıcı kimliği, iletinin ileti tanımlayıcısı içindeki bağlam bilgisinden (*UserIdentifier* alanı) gelen kullanıcı kimliği. Hedef hedef kuyruğu için bir **MQOPEN** ya da **MQPUT1** çağrısı yayınlanmadan önce, bu kullanıcı kimliği nesne tanımlayıcısındaki *AlternateUserID* alanına taşınır.

z/OS *LU 6.2kullanan kanalların alınması*
Denetlenmiş kullanıcı kimlikleri, kanalın PUTAUT seçeneğine ve bir ya da iki denetinin gerçekleştirilip gerçekleştirilmeyeceğini bağlıdır.

Çizelge 62. Kullanıcı kimlikleri LU 6.2 kanallarına ilişkin profil adını denetlendi			
Alıcıda ya da istekte bulunan kanalda PUUTAT seçeneği belirtildi	**hlq.ALTERNATE.USER.userid tanıtımı**	**hlq.CONTEXT.queuename tanıtımı**	**hlq.resourcename profili**
DEF, 1 denetimi	-	CHL	CHL
DEF, 2 denetimleri	-	CHL + MCA	CHL + MCA
CTX, 1 denetimi	CHL	CHL	CHL
CTX, 2 denetimleri	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 denetimi	-	MCA	MCA
ONLYMCA, 2 çek	-	MCA	MCA
ALTMCA, 1 denetimi	MCA	MCA	MCA
ALTMCA, 2 denetleme	MCA	MCA	MCA + ALT

Anahtar:

MCA (MCA kullanıcı kimliği)
Alıcıda MCAUSER kanal özniteliği için belirlenen kullanıcı kimliği; boşsa, alıcı ya da istek isteyen tarafın kanal başlatıcı adres alanı kullanıcı kimliği kullanılır.

CHL (Kanal kullanıcı kimliği)

İstekçi-sunucu kanalları
Kanal istekçiden başlatıldıysa, ağ kullanıcı kimliği (kanal kullanıcı kimliği) alma olanağı yoktur.

PUTAUT parametresi, istekte bulunan kanalda DEF ya da CTX olarak ayarlandıysa, ağdan kullanıcı kimliği alınmadığından, kanal kullanıcı kimliği, istekte bulunan kişinin kanal başlatıcı adres alanına sahip olur.

PUTAUT parametresi ONLYMCA ya da ALTMCA olarak ayarlandıysa, kanal kullanıcı kimliği yoksayılır ve istekte bulunanın MCA kullanıcı kimliği kullanılır.

Diğer kanal tipleri
PUTAUT parametresi, alıcı ya da istekte bulunan kanalda DEF ya da CTX olarak ayarlandıysa, kanal kullanıcı kimliği, kanal başlatıldığında iletişim sisteminden alınan kullanıcı kimliğidir.

- Gönderme kanalı z/OSüzeriyse, alınan kanal kullanıcı kimliği, gönderen kanal başlatıcı adres alanı kullanıcı kimliğidir.
- Gönderme kanalı farklı bir altyapıdaysa (örneğin, AIX), alınan kanal kullanıcı kimliği tipik olarak, kanal tanımlamasının USERID parametresi tarafından sağlanır.

Alınan kullanıcı kimliği boşsa ya da herhangi bir kullanıcı kimliği alınmazsa, bir kanal kullanıcı kimliği boşluk kullanılır.

ALT (Diğer kullanıcı kimliği)
Kullanıcı kimliği, iletinin ileti tanımlayıcısı içindeki bağlam bilgisinden (*UserIdentifier* alanı) gelen kullanıcı kimliği. Bu kullanıcı kimliği, hedef hedef kuyruğu için bir MQOPEN ya da MQPUT1 çağrısı yayınlanmadan önce nesne tanımlayıcısındaki *AlternateUserID* alanına taşınır.

z/OS *İstemci MQI istekleri*

Çeşitli kullanıcı kimlikleri, hangi kullanıcı kimliklerinin ve ortam değişkenlerinin ayarlandığını bağlı olarak kullanılabilir. Bu kullanıcı kimlikleri, kullanılan PUTAUT seçeneğine ve diğer bir kullanıcı kimliğinin belirtilmesine bağlı olarak, çeşitli tanıtımlara göre denetlenir.

Bu bölümde, TCP/IP ve LU 6.2için sunucu bağlantısı kanalları üzerinden verilen istemci MQI istekleri için denetlenen kullanıcı kimlikleri açıklanmaktadır. MCA kullanıcı kimliği ve kanal kullanıcı kimliği, önceki bölümlerde açıklanan TCP/IP ve LU 6.2 kanallarına uygun olarak bulunur.

Sunucu bağlantısı kanallarında, MCAUSER özniteliği boş bırakılırsa, istemciden alınan kullanıcı kimliği kullanılır.

Ek bilgi için "İstemciler için erişim denetimi" sayfa 93 başlıklı konuya bakın.

İstemci **MQOPEN**, **MQSUB**ve **MQPUT1** istekleri için, denetlenen profili belirlemek için aşağıdaki kuralları kullanın:

- İstek alternatif kullanıcı yetkisi belirtiyorsa, *hlq*.ALTERNATE.USERile ilgili bir onay işareti yapılır. *userid* tanıtımı.
- İstek bağlam yetkisini belirtiyorsa, *hlq*ile ilgili bir onay imi yapılır.BAğLAM. *queuename* profili.
- Tüm **MQOPEN**, **MQSUB**ve **MQPUT1** istekleri için, *hlq.resourcename* profili için bir onay işareti yapılır.

Hangi tanıtımların denetlendiğini saptadığınızda, bu tanıtımlara karşı hangi kullanıcı kimliklerinin denetleneceğini belirlemek için aşağıdaki çizelgeyi kullanın.

Çizelge 63. Kullanıcı kimlikleri LU 6.2 ve TCP/IP sunucusu bağlantı kanallarına ilişkin profil adını denetlendi

Sunucu-bağlantı kanalında PUTAUT seçeneği belirtildi	Açık olarak başka bir kullanıcı kimliği belirlendi mi?	hlq.ALTERNATE.USER.userid tanıtımı	hlq.CONTEXT.queuename tanıtımı	hlq.resourcename profili
DEF, 1 denetimi	Hayır	-	CHL	CHL
DEF, 1 denetimi	Evet	CHL	CHL	CHL
DEF, 2 denetimleri	Hayır	-	CHL + MCA	CHL + MCA
DEF, 2 denetimleri	Evet	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 denetimi	Hayır	-	MCA	MCA
ONLYMCA, 1 denetimi	Evet	MCA	MCA	MCA
ONLYMCA, 2 çek	Hayır	-	MCA	MCA
ONLYMCA, 2 çek	Evet	MCA	MCA	MCA + ALT

Anahtar:

MCA (MCA kullanıcı kimliği)
Sunucu bağlantısında MCAUSER kanal özniteliği için belirtilen kullanıcı kimliği; boş bırakılırsa, kanal başlatıcı adres alanı kullanıcı kimliği kullanılır.

CHL (Kanal kullanıcı kimliği)
TCP/IP ' de güvenlik, kanala ilişkin iletişim sistemi tarafından desteklenmiyor. Aktarım Katmanı Güvenliği (TLS) kullanılıyorsa ve ortaktan bir sayısal sertifika akıtıldıysa, bu sertifikaya (kuruluysa) ilişkin kullanıcı kimliği ya da RACF Sertifika Adı Süzgeci (CNF) kullanılarak bulunan eşleşen bir süzgeçle ilişkilendirilmiş kullanıcı kimliği kullanılır. İlişkili bir kullanıcı kimliği bulunamazsa ya da TLS

kullanılmıyorsa, kanal başlatıcı adres alanının kullanıcı kimliği, PUTAUT değiştirgesiyle DEF ya da CTX değerine ayarlanmış kanallarda kanal kullanıcı kimliği olarak kullanılır.

Not: RACF Certificate Name Filtering (CNF) kullanımı, aynı RACF kullanıcı kimliğini birden çok uzak kullanıcıya atamanıza olanak sağlar; örneğin, aynı kuruluş birimindeki tüm kullanıcılar, doğal olarak aynı güvenlik yetkisine sahip olur. Bu, sunucunun dünyadaki olası her uzak kullanıcının sertifikasının bir kopyasına sahip olması gerekmediği ve sertifika yönetimini ve dağıtımını büyük ölçüde basitleştirdiği anlamına gelir.

PUTAUT parametresi kanal için ONLYMCA ya da ALTMCA olarak ayarlandıysa, kanal kullanıcı kimliği yoksayılır ve sunucu bağlantısı kanalının MCA kullanıcı kimliği kullanılır. Bu, TLS kullanan TCP/IP kanalları için de geçerlidir.

ALT (Diğer kullanıcı kimliği)
Kullanıcı kimliği, iletinin ileti tanımlayıcısı içindeki bağlam bilgisinden (*UserIdentifier* alanı) gelen kullanıcı kimliği. Bu kullanıcı kimliği, nesne ya da abonelik tanımlayıcısındaki *AlternateUserID* alanına, istemci uygulaması adına bir **MQOPEN**, **MQSUB** ya da **MQPUT1** çağrısı yayınlanmadan önce taşınmış olur.

z/OS *Kanal başlatıcı örneği*

Kullanıcı kimliklerinin RACF profillerine nasıl denetleneceğini gösteren bir örnek.

A user performs an **MQPUT1** operation to a queue on queue manager QM01 that resolves to a queue called QB on queue manager QM02. İleti, QM01.TO.QM02. RESLEEL değeri NONE (Yok) değerine ayarlıdır ve açık, diğer kullanıcı kimliği ve bağlam denetimiyle gerçekleştirilir. Alıcı kanalı tanımlamasında PUTAUT (CTX) bulunur ve MCA kullanıcı kimliği ayarlanır. İletiyi kuyruğa almak için, alıcı kanalda hangi kullanıcı kimliklerinin kullanıldığını QB kuyruğuna yerleştirecek?

Yanıt: Çizelge 55 sayfa 225 , RESLELEL değeri NONE olarak ayarlandığından, iki kullanıcı kimliklerinin denetlendiğini gösterir.

Çizelge 61 sayfa 231 shows that, with PUTAUT set to CTX and 2 checks, the following user IDs are checked:

- Kanal başlatıcı kullanıcı kimliği ve MCAUSER kullanıcı kimliği hlq.ALTERNATE.USER.userid tanıtımı.
- Kanal başlatıcı kullanıcı kimliği ve MCAUSER kullanıcı kimliği hlq.CONTEXT.queuename tanıtıcıyla karşılaştırılır.
- Kanal başlatıcı kullanıcı kimliği ve ileti tanımlayıcısında belirtilen diğer kullanıcı kimliği (MQMD), hlq.Q2 tanıtımında denetlenir.

z/OS *Grup içi kuyruğa alma aracısı tarafından kullanılan kullanıcı kimlikleri*

Grup içi kuyruğa alma aracısının hedef kuyrukları açtığı sırada denetlenen kullanıcı kimlikleri, IGQAUT ve IGQUSER kuyruk yöneticisi özniteliklerinin değerlerine göre belirlenir.

Olası kullanıcı kimlikleri şunlardır:

Grup içi kuyruğa alma kullanıcı kimliği (IGQ)
Alma kuyruk yöneticisinin IGQUSER özniteiyle belirlenen kullanıcı kimliği. Bu değer boşluklara ayarlanmışsa, alıcı kuyruk yöneticisinin kullanıcı kimliği kullanılır. Ancak, alma kuyruk yöneticisinin tanımlı olan tüm kuyruklara erişim yetkisi olduğu için, alma kuyruğu yöneticisinin kullanıcı kimliği için güvenlik denetimleri gerçekleştirilmez. Bu durumda:

- Yalnızca bir kullanıcı kimliği denetlenecekse ve kullanıcı kimliği alan kuyruk yöneticisiniyse, hiçbir güvenlik denetimi gerçekleşmez. IGQAUT, ONLYIGQ ya da ALTIGQ değerine ayarlandığında bu durum oluşabilir.
- İki kullanıcı kimliği denetlenecekse ve kullanıcı kimliklerinden biri alan kuyruk yöneticisininse, güvenlik denetimleri yalnızca diğer kullanıcı kimliği için geçerli olur. Bu durum, IGQAUT, DEF, CTX ya da ALTIGQ olarak ayarlandığında ortaya çıkabilir.
- İki kullanıcı kimliği denetlenecekse ve her iki kullanıcı kimliği alan kuyruk yöneticisinden her iki kullanıcı kimliği de varsa, hiçbir güvenlik denetimi gerçekleşmez. IGQAUT, ONLYIGQ değerine ayarlandığında ortaya çıkabilir.

Kuyruk Yöneticisi Kullanıcı Kimliği Gönderiliyor (SND)
İletiyi, SYSTEM.QSG.TRANSMIT.QUEUE.

Diğer kullanıcı kimliği (ALT)
İletinin ileti tanımlayıcısında *UserIdentifier* alanında belirtilen kullanıcı kimliği.

Çizelge 64. Grup içi kuyruğa alma için profil adına karşı kullanıcı kimlikleri denetlendi

Alma kuyruk yöneticilesinde IGQAUT seçeneği belirtildi	hlq.ALTERNATE.USER.userid tanıtımı	hlq.CONTEXT.queuename tanıtımı	hlq.resourcename profili
DEF, 1 denetimi	-	SND	SND
DEF, 2 denetimleri	-	SND + IGQ	SND + IGQ
CTX, 1 denetimi	SND	SND	SND
CTX, 2 denetimleri	SND + IGQ	SND + IGQ	SND + ALT
ONLYIGQ, 1 denetimi	-	IGQ	IGQ
ONLYIGQ, 2 denetimleri	-	IGQ	IGQ
ALTIGQ, 1 denetimi	-	IGQ	IGQ
ALTIGQ, 2 denetimleri	IGQ	IGQ	IGQ + ALT

Anahtar:

Alt
Diğer kullanıcı kimliği.

IGQ
IGQ kullanıcı kimliği.

SND
Kuyruk yöneticisi kullanıcı kimliği gönderiliyor.

z/OS *Boş kullanıcı kimlikleri ve UACC düzeyleri*

If a blank user ID occurs, a RACF undefined user is signed on. Tanımlanmamış kullanıcıya geniş kapsamlı erişim yetkisi verme.

Bir kullanıcı bağlamı ya da diğer kullanıcı güvenliğini kullanarak iletileri kurcalarken ya da IBM MQ boş bir kullanıcı kimliği geçirdiğinde boş kullanıcı kimlikleri olabilir. Örneğin, sistem komut giriş kuyruğuna bağlam olmadan bir ileti yazıldığında, boş bir kullanıcı kimliği kullanılır.

Not: Kullanıcı kimliği: " * " (bu, yedi boşlukların izlediği bir yıldız işareti), tanımsız bir kullanıcı kimliği olarak işlem görür.

IBM MQ passes the blank user ID to RACF and a RACF undefined user is signed on. Tüm güvenlik denetimleri, ilgili tanıtıma ilişkin evrensel erişimi (UACC) kullanır. Erişim düzeylerinizi nasıl ayarlamanıza bağlı olarak, UACC tanımlanmamış kullanıcıya geniş kapsamlı bir erişim verebilir.

Örneğin, TSO ' dan bu RACF komutunu yayınlayın:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

you define a profile that enables both z/OS-defined user IDs (that have not been put in the access list) and the RACF undefined user ID to put messages on, and get messages from, that queue.

Boş kullanıcı kimliklerine karşı korumak için erişim düzeylerinizi dikkatli bir şekilde planlamanız ve bağlam ve diğer kullanıcı güvenliğini kullanabilecek kişi sayısını sınırlamanız gerekir. RACF tanımlanmamış kullanıcı kimliğini kullanarak, erişmemeleri gereken kaynaklara erişmelerini önlemeniz gerekir. Ancak, aynı zamanda, tanımlı kullanıcı kimlikleri bulunan kişilere erişime izin vermelisiniz. To do this, you can specify a user ID of asterisk (*) in a RACF command PERMIT, giving access to resources for all defined user IDs. Bu nedenle, tanımlanmamış tüm kullanıcı kimlikleri (örneğin, " * ") erişimi reddedilir. Örneğin, bu RACF komutları, RACF tanımsız kullanıcı kimliğinin, iletileri yerleştirmek ya da almak için kuyruğa erişim kazanmasını önlemesini sağlar:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY UACC(NONE)
PERMIT Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY CLASS(MQQUEUE) ACCESS(UPDATE) ID(*)
```

z/OS z/OS kullanıcı kimlikleri ve çok faktörlü kimlik doğrulaması (MFA)

IBM Multi-Factor Authentication for z/OS , z/OS güvenlik denetimcilerinin, tanımlanan kullanıcıların z/OS sisteminde oturum açmak için birden çok kimlik doğrulama etmenini (örneğin, bir parola ve bir şifreleme simgesi) kullanmalarını gerektirerek SAF kimlik doğrulamasını geliştirmelerini sağlar. IBM MFA, RSA SecureIdgibi zamana dayalı tek seferlik parola oluşturma teknolojileri için de destek sağlar.

Çoğu zaman IBM MQ , kullanıcıların CICS ya da IBM MQ işini kullanan toplu iş sistemlerinde nasıl "oturum açtığından" habersiz olur; oturum açan kullanıcı kimliği kimlik bilgileri z/OS görev ya da adres alanıyla ilişkilendirilir ve IBM MQ kaynak yetkilendirmesini denetlemek için bunu kullanır. MFA için etkinleştirilen kullanıcı kimlikleri, CICS ve IMS köprüleriyle kullanılan geçiş kartları aracılığıyla IBM MQ kaynaklarına ve kimlik doğrulamasına yetki vermek için kullanılabilir.

Önemli: Ancak, *MQCSP_AUTH_USER_ID_AND_PWD* seçeneğiyle bir MQCONNX API çağrısında bir kullanıcı kimliği ve parola kimlik bilgilerini ileten IBM MQ Explorergibi uygulamalar kullanılırken dikkat edilmesi gereken özel noktalar vardır. IBM MQ ' in bu API isteğinde ek kimlik bilgisi iletmek için bir olanağı yok.

Sınırlamalar ve olası geçici çözümler aşağıdaki metinde açıklanmıştır.

IBM MQ Explorer

IBM MQ Explorer , MFA 'nın etkinleştirildiği bir kullanıcı kimliğiyle z/OS sisteminde oturum açmak için kullanılamaz; IBM MQ Explorer ' den z/OS' e ikinci bir kimlik doğrulama katsayısı geçirme olanağı yoktur.

Buna ek olarak, IBM MQ Explorer tarafından bir kullanıcı kimliği ve parola kimlik bilgilerini yeniden kullanmak için kullanılan ve bir kerelik kullanım parolaları etkin olduğunda özel dikkat edilmesi gereken iki farklı mekanizma vardır:

1. IBM MQ Explorer , parolaları daha sonra oturum açmak üzere yerel makinede gizlenmiş biçimde saklama yeteneğine sahiptir. Bu yetenek, z/OS kuyruk yöneticisiyle her bağlantı kurulduğunda Explorer (Gezgin) tarafından parola istenerek devre dışı bırakılmalıdır.

   Bunu yapmak için aşağıdaki yordamı kullanın:

   a. **Kuyruk Yöneticileri**seçeneğini belirleyin.
   b. Görüntülenen listeden, istediğiniz kuyruk yöneticisini seçin ve o kuyruk yöneticisini sağ tıklatın.
   c. Görüntülenen menü listesinden **Bağlantı Ayrıntıları** seçeneğini belirleyin.
   d. Sonraki menü listesinden **Özellikler** seçeneğini belirleyin ve **Kullanıcı kimliği** sekmesini seçin.

      Parola istemi radyo düğmesini seçtiğinizden emin olun.
2. Kuyruklardaki iletilere göz atma, abonelikleri sınama gibi IBM MQ Explorericindeki çeşitli işlemler, oturum açmada ilk kullanılan kimlik bilgilerini kullanarak IBM MQ kimlik doğrulamasını başlatan yeni bir iş parçacığı başlatır. Parola kimlik bilgileri yeniden kullanılamadığı için bu işlemleri kullanamazsınız.

Bu sorunlar için MFA yapılandırma düzeyinde iki olası geçici çözüm vardır:

- IBM MQ görevlerini MFA işlemesinden tamamen dışlamak için MFA ' nın uygulama tanıtıcısı hariç tutmasını kullanın.

Bunu yapmak için aşağıdaki komutları verin:

1. ```
   RDEFINE MFADEF MFABYPASS.USERID.chinuser
   ```

   Burada *chinuser* , kanal başlatıcı adres alanı düzeyi kullanıcı kimliğidir (STC sınıfı aracılığıyla kanal başlatıcısıyla ilişkilendirilir).

2. ```
   PERMIT MFABYPASS.USERID.chinuser CLASS MFADEF ACCESS(READ) ID(explorer user)
   ```

Bu yaklaşımla ilgili daha fazla bilgi için bkz. Uygulamalar için IBM MFA.

- IBM MFA 1.2ile tanıtılan MFA ' da bant dışı desteği kullanın. Bu yaklaşımla, IBM MFA web sunucusunda önceden kimlik doğrulamasını gerçekleştirdiniz ve kullanıcı kimliğiniz ve parolanızın yanı sıra, ilke aracılığıyla belirlendiği şekilde ek kimlik doğrulamasını da belirlersiniz. IBM MFA sunucusu, IBM MQ Explorer kimlik doğrulama iletişim penceresinde belirttiğiniz bir önbellek simgesi kimlik bilgisi oluşturur. Güvenlik yöneticisi, bu kimlik bilgilerinin makul bir süre boyunca yeniden yürütülmesine izin verebilir, bu nedenle normal IBM MQ Explorer kullanımı etkinleştirilir.

Bu yaklaşımla ilgili daha fazla bilgi için bkz. Introduction to IBM MFA.

z/OS IBM MQ for z/OS güvenlik yönetimi

IBM MQ , her bir kullanıcıyla ve her bir kullanıcı tarafından yapılan erişim istekleriyle ilgili bilgileri tutmak için bir depolama tablosu kullanır. Bu tabloyu verimli bir şekilde yönetmek ve IBM MQ ' dan dış güvenlik yöneticisine (ESM) yapılan istek sayısını azaltmak için, bir dizi denetim kullanılabilir.

Bu denetimler, hem işlemler, hem de denetim panoları ve IBM MQ komutları aracılığıyla kullanılabilir.

z/OS *Kullanıcı kimliği yeniden doğrulaması*

If the RACF definition of a user who is using IBM MQ resources has been changed, for example by connecting the user to a new group, you can tell the queue manager to sign this user on again the next time it tries to access an IBM MQ resource. You can do this by using the IBM MQ command RVERIFY SECURITY.

- User HX0804 is getting and putting messages to the PAYROLL queues on queue manager PRD1. Ancak, HX0804 artık aynı kuyruk yöneticisininde (PRD1) bazı EMEKLILIK kuyruklarına erişim gerektirir.
- The data security administrator connects user HX0804 to the RACF group that allows access to the PENSION queues.
- So that HX0804 can access the PENSION queues immediately (that is, without shutting down queue manager PRD1 or waiting for HX0804 to time out) you must use the IBM MQ command:

```
RVERIFY SECURITY(HX0804)
```

Not: Kuyruk yöneticisi çalışırken kullanıcı kimliği zamanaşımını uzun süre (gün ya da çift hafta) kapadıysanız, bu süre içinde iptal edilmiş ya da silinmiş olan kullanıcılar için RVERDONE Security komutunu çalıştırmasını unutmamalısınız.

z/OS *Kullanıcı kimliği zamanaşımları*

IBM MQ ' un bir etkinlik dışı durum döneminden sonra kuyruk yöneticilerinden bir kullanıcıyı imzalayabilmesi için bu işlemi gerçekleştirmesini sağlar.

Bir kullanıcı bir IBM MQ kaynağına eriştiğinde, kuyruk yöneticisi bu kullanıcıyı kuyruk yöneticisine imzalamayı dener (altsistem güvenliği etkinse). Bu, kullanıcının ESM ' ye doğrulanmış olduğu anlamına gelir. Bu kullanıcı, kuyruk yöneticisi kapatılıncaya kadar ya da kullanıcı kimliği *zamanaşımına uğradı* (kimlik doğrulama lapları) ya da yeniden doğrulanıncaya kadar (yeniden doğrulanıncaya kadar) IBM MQ ' ta oturum açmayı sürdürmektedir.

Bir kullanıcı zamanaşımına uğradığında, kullanıcı kimliği kuyruk yöneticisi içinde *oturum kapatılır* ve bu kullanıcı için saklanan güvenlikle ilgili tüm bilgiler atılır. Kullanıcı, kuyruk yöneticisi içindeki oturum açılıp kapatıldığında, uygulama programı ya da kullanıcı için belirgin bir değer değildir.

Kullanıcılar, önceden belirlenmiş bir süre için herhangi bir IBM MQ kaynağı kullanmadıklarında zamanaşımını almaya hak kazanır. Bu zaman dönemi MQSC ALTER SECURITY komutu tarafından ayarlanır.

ALTER SECURITY komutunda iki değer belirtilebilir:

TIMEOUT
Kullanılmayan bir kullanıcı kimliğinin ve ilişkili kaynaklarının, IBM MQ kuyruk yöneticisi içinde kalabileceği süre (dakika).

Aralık
Kullanıcı kimlikleri ve ilişkili kaynaklarıyla ilgili denetimler arasındaki süre (dakika), *Zaman aşımı* ' in süresinin dolup dolup olmadığını belirlemek için.

Örneğin, *TIMEOUT* değeri 30 ise ve *INTERVAL* değeri 10 ise, her 10 dakikada bir IBM MQ kullanıcı kimliğini ve ilişkili kaynakları denetler ve 30 dakika boyunca kullanılmamış olup olmadığını denetler. Zaman aşımına uğramış bir kullanıcı kimliği bulunursa, bu kullanıcı kimliği kuyruk yöneticisi içinde oturum kapatılır. Zaman aşımına uğramamış kullanıcı kimlikleriyle ilişkili zaman aşımına uğramış kaynak bilgileri bulunursa, bu kaynak bilgileri atılır. Kullanıcı kimliklerinin dışarı çıkmasını istemiyorsanız, *INTERVAL* değerini sıfır olarak ayarlayın. Ancak, *INTERVAL* değeri sıfırsa, kullanıcı kimlikleri ve ilişkili kaynakları tarafından doldurulan depolama alanı, bir **REFRESH SECURITY** ya da **RVERIFY SECURITY** komutu yayınlanıncaya kadar serbest bırakılmaz.

Bu değerin ayarlanması, bir çok sayıda kullanıcının olması durumunda önemli olabilir. Küçük aralık ve zamanaşımı değerleri ayarlıyorsanız, artık gerekli olmayan kaynaklar serbest bırakılır.

Not: Varsayılan değer olarak *INTERVAL* ya da *TIMEOUT* değerlerini kullanırsanız, her kuyruk yöneticisi başlatıldığında komutu yeniden girmeniz gerekir. Bu işlemi, kuyruk yöneticisi için ayarlanan CSQINP1 veri kümesine **ALTER SECURITY** komutunu koyarak otomatik olarak yapabilirsiniz.

z/OS *z/OSüzerinde kuyruk yöneticisi güvenliği yenileniyor*

IBM MQ for z/OS , performansı artırmak için RACF verilerini önbelleğe alır. Belirli güvenlik sınıflarını değiştirdiğinizde, bu önbelleğe alınmış bilgileri yenilemişmeniz gerekir. Performans nedenlerinden dolayı güvenliği sık sık yenileyin. Yalnızca TLS güvenlik bilgilerini yenilemeyi de seçebilirsiniz.

Bir kuyruk ilk kez açıldığında (ya da bir güvenlik yenilemesinden bu yana ilk defa) IBM MQ , kullanıcının erişim haklarını almak için bir RACF denetimi gerçekleştirir ve bu bilgileri önbelleğe alır. Önbelleğe alınan veriler, güvenlik denetiminin gerçekleştirildiği kullanıcı kimliklerini ve kaynakları içerir. If the queue is opened again by the same user, the presence of the cached data means that IBM MQ does not have to issue RACF checks, which improves performance. The action of a security refresh is to discard any cached security information and so force IBM MQ to make a new check against RACF. MQADMIN, MXADMIN, MQPROC, MXPROC, MQQUEUE, MXQUEUE, MQNLIST, MXNLIST ya da MXTOPIC sınıfındaki bir RACF kaynak tanıtımını eklediğinizde ya da sildiğinizde, kuyruk yöneticilerine bu sınıfı kullanan kuyruk yöneticilerine tuttukları güvenlik bilgilerini yenilemeye ilişkin bilgi vermelisiniz. Bunu yapmak için şu komutları verin:

- The RACF SETROPTS RACLIST(classname) REFRESH command to refresh at the RACF level.
- Kuyruk yöneticisi tarafından tutulan güvenlik bilgilerini yenilemek için IBM MQ REFRESH SECURITY komutu. Bu komutun, değişen tanıtımlara erişen her bir kuyruk yöneticisi tarafından verilmesi gerekir. Bir kuyruk paylaşım grubunuz varsa, komutu gruptaki tüm kuyruk yöneticilerine yönlendirmek için komut kapsamı özniteliğini kullanabilirsiniz.

  Not: Var olan bir gruba yeni bir kullanıcı bağladıysanız, IBM MQ RVERIFY SECURITY(kullanıcı kimliği) komutunu çalıştırmanız gerekir. REFRESH SECURITY (*) komutu, bir IBM MQ kaynağına erişmeye çalışırken kuyruk yöneticisinin bu kullanıcıyı yeniden imzalamamasına izin vermiyor.

If you are using generic profiles in any of the IBM MQ classes, you must also issue normal RACF refresh commands if you change, add, or delete any generic profiles. Örneğin, SETROPTS GENERIC (sınıf adı) YENILE.

Ancak, bir RACF kaynak profili eklenirse, değiştirildiğinde ya da silindiyse ve uygulanacağı kaynağa henüz erişilmediyse (bu nedenle hiçbir bilgi önbelleğe alınmamış), IBM MQ yeni RACF bilgilerini, REFRESH SECURITY komutu verilmeden kullanır.

RACF denetimi açılırsa (örneğin, RACF RALTER AUDIT (erişim-deneme (audit_access_level)) komutu kullanılarak), önbelleğe alma gerçekleşmez ve bu nedenle IBM MQ , her denetim için doğrudan RACF veri alanına gönderme yapar. Bu nedenle, değişikliklere erişmek için hemen ve REFRESH SECURITY gerekmediği için değişiklikler kaldırılır. RACF RIST komutunu kullanarak RACF denetiminin açık olup olmadığını doğrulayabilirsiniz. Örneğin, komutu yayınlayabilirdiniz

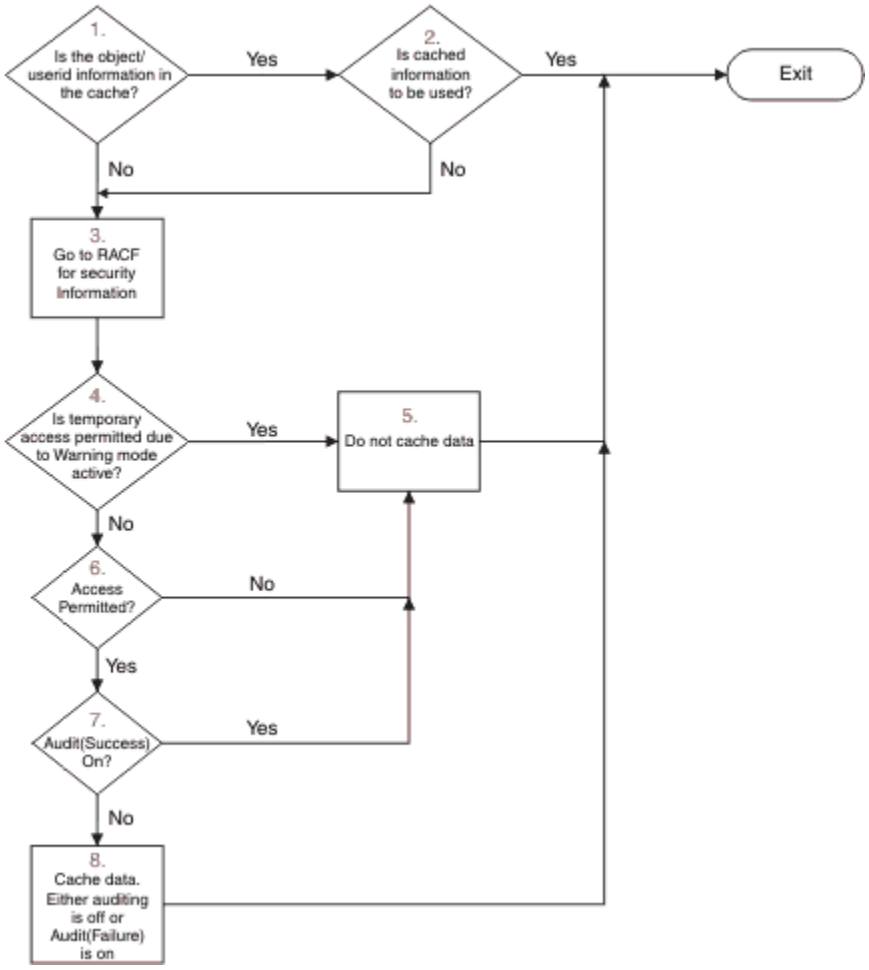
```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

ve sonuçları alma

```
CLASS      NAME
-----      ----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
    AUDITING
    --------
    FAILURES(READ)
```

Bu, denetlemenin açık olduğunu gösterir. Daha fazla bilgi için *z/OS Security Server RACF Auditor's Guide* ve *z/OS Security Server RACF Command Language Reference*adlı kılavuza bakın.

Şekil 17 sayfa 239 , güvenlik bilgilerinin önbelleğe alınacağı ve önbelleğe alınan bilgilerin kullanıldığı durumları özetler.



Şekil 17. IBM MQ güvenliği önbelleğe alma için mantık akışı

MQADMIN ya da MXADMIN sınıflarına anahtar tanıtımları ekleyerek ya da silerek güvenlik ayarlarınızı değiştirirseniz, bu değişiklikleri dinamik olarak almak için şu komutlardan birini kullanın:

GüVENLIK (*)
GüVENLIK YENILE (MQADMIN

GüVENI YENILE (MXADMIN

Başka bir deyişle, yeni güvenlik tiplerini etkinleştirebilir ya da kuyruk yöneticisini yeniden başlatmak zorunda kalmadan bunları devre dışı bırakabilirsiniz.

Başarım nedenleriyle, REFRESH SECURITY komutlarından etkilenen tek sınıflardır. Bir tanıtımı MQCONN ya da MQCMDS sınıflarında değiştirirseniz, REFRESH SECURITY seçeneğini kullanmanız gerekmez.

Not: RESLEVL güvenlik profilini değiştirirseniz, MQADMIN ya da MXADMIN sınıfı yenilenmez.

Performans nedenlerinden dolayı, REFRESH GüVENLIğINI, mümkün olduğunca yoğun bir şekilde, ideal olarak en yoğun zamanlarda kullanın. You can minimize the number of security refreshes by connecting users to RACF groups that are already in the access list for IBM MQ profiles, rather than putting individual users in the access lists. Bu şekilde, kaynak tanıtımından çok kullanıcıyı değiştirebilirsiniz. Güvenliği yenilemek yerine, uygun kullanıcıyı RIVERIVE GüVENLERINI DE ONAYLAYABILIRSINIZ.

REFRESH SECURITY gibi bir örnek olarak, kuyruk yöneticisi PRMQ ' da INSURANCE.LIFE ile başlayan kuyruklara erişimi korumak için yeni tanıtımları tanımladığınızı varsayalım. Bu RACF komutlarını kullanıyorsunuz:

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

RACF ' un tutması gereken güvenlik bilgilerini yenilemesini sağlamak için aşağıdaki komutu vermelisiniz; örneğin:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Bu tanıtımlar soysal olduğu için, MQQUEUE için soysal profilleri yenilemesini RACF ' e söylemeniz gerekir. Örneğin:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Bundan sonra, kuyruk yöneticisi PRMQ ' ya kuyruk tanıtımlarının değiştiğini söylemek için bu komutu kullanmanız gerekir:

```
REFRESH SECURITY(MQQUEUE)
```

SSL/TLS güvenliği yenileniyor

TLS Key Repository 'nin önbelleğe alınmış görünümünü yenilemek için, REFRESH SECURITY komutunu seçenek TYPE (SSL) ile verin. Bu, kanal başlatıcınızın yeniden başlatılmasına gerek kalmadan TLS ayarlarınızın bazılarını güncellemenizi sağlar.

z/OS *Güvenlik durumunun görüntülenmesi*

Güvenlik anahtarlarının durumunu ve diğer güvenlik denetimlerinin durumunu görüntülemek için, MQSC DISPLAY SECURITY komutunu verin.

Aşağıdaki şekil, DISPLAY SECURITY ALL komutunun tipik çıkışını göstermektedir.

```
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
```

Şekil 18. DISPLAY SECURITY komutundan gelen tipik çıkış

Bu örnek, komutta yanıt veren kuyruk yöneticisinin, kuyruk yöneticisi düzeyinde altsistem, komut, diğer kullanıcı, işlem, ad listesi ve kuyruk güvenliği olduğunu, ancak kuyruk paylaşım grubu düzeyinde etkin olmadığını gösterir. Bağlantı, komut kaynağı ve bağlam güvenliği etkin değil. Ayrıca, kullanıcı kimliği zamanaşımlarının etkin olduğunu ve kuyruk yöneticisinin bu kuyruk yöneticisinde 54 dakika boyunca kullanılmamış olan kullanıcı kimliklerini denetleyerek her 12 dakikada bir, bunları kaldırdığını da gösterir.

Not: Bu komut, geçerli güvenlik durumunu gösterir. It does not necessarily reflect the current status of the switch profiles defined to RACF, or the status of the RACF classes. Örneğin, bu kuyruk yöneticisinin son yeniden başlatılmasından ya da REFRESH SECURITY komutundan sonra, anahtar tanıtımları değiştirilmiş olabilir.

z/OS z/OSiçin güvenlik kuruluşu görevleri

After installing and customizing IBM MQ, authorize started task procedures to RACF, authorize access to various resources, and set up RACF definitions. İsteğe bağlı olarak, sisteminizi TLS için yapılandırın.

IBM MQ ilk kurulduğunda ve özelleştirildiğinde, bu güvenlikle ilgili görevleri gerçekleştirmeniz gerekir:

1. IBM MQ veri kümesini ve sistem güvenliğini aşağıdaki şekilde ayarlayın:
   - Kuyruk yöneticisi başlatıldı-görev yordamı xxxxMSTR ve dağıtımlı kuyruğa alma başlatma-görev yordamı xxxxCHIN , RACFaltında çalışır.
   - Kuyruk yöneticisi veri kümelerine erişim yetkisi verme.
   - Kuyruk yöneticisini ve yardımcı program programlarını kullanacak olan kullanıcı kimlikleri için kaynaklara erişim yetkisi verir.
   - Bağlaşım olanağı listesi yapılarını kullanacak kuyruk yöneticileri için erişim yetkisi verme.
   - Db2' u kullanacak kuyruk yöneticileri için erişim yetkisi verme.
2. IBM MQ güvenliği için RACF tanımlarını ayarlayın.
3. TLS (Transport Layer Security; İletim Katmanı Güvenliği) olanağını kullanmak istiyorsanız, sisteminizi sertifikaları ve anahtarları kullanmak üzere hazırlayın.

z/OS *IBM MQ for z/OS veri kümesi güvenliğinin ayarlanması*

Birçok IBM MQ kullanıcısı tipi vardır. Sistem veri kümelerine erişimlerini denetlemek için RACF seçeneğini kullanın.

IBM MQ veri kümelerinin olası kullanıcıları aşağıdaki varlıkları içerir:

- Kuyruk yöneticisinin kendisi.
- Kanal başlatıcı

- IBM MQ veri kümeleri oluşturmak, yardımcı programları çalıştırmak ve benzer görevleri yapmak zorunda olanIBM MQ yöneticileri.
- IBM MQtarafından sağlanan telif kitaplarını kullanması gereken uygulama programcıları, veri kümelerini, makroları ve benzeri kaynakları içerir.
- Aşağıdakilerden birini ya da daha fazlasını içeren uygulamalar:
  - Toplu işler
  - TSO kullanıcıları
  - CICS bölge
  - IMS bölge
- Veri kümeleri CSQOUTX ve CSQSNAP
- Dinamik kuyruklar SYSTEM.CSQXCMD.*

For all these potential users, protect the IBM MQ data sets with RACF.

Tüm 'CSQINP' veri kümelerine erişimi de denetlemeniz gerekir.

z/OS *RACF authorization of started-task procedures*

Bazı IBM MQ veri kümeleri, kuyruk yöneticisinin dışlayıcı kullanımı içindir. If you protect your IBM MQ data sets using RACF, you must also authorize the queue manager started-task procedure xxxxMSTR, and the distributed queuing started-task procedure xxxxCHIN, using RACF. Bunu yapmak için STARTED sınıfını kullanın. Diğer bir seçenek olarak, başlatılan yordamlar çizelgesini (ICHRIN03) kullanabilirsiniz, ancak değişikliklerden önce z/OS sisteminde bir IPL işlemi gerçekleştirmeniz gerekir.

Ek bilgi için *z/OS Security Server RACF System Programmer's Guide*adlı yayına bakın.

Tanımlanan RACF kullanıcı kimliği, başlatılan görev yordamında veri kümeleri için gerekli erişime sahip olmalıdır. For example, if you associate a queue manager started task procedure called CSQ1MSTR with the RACF user ID QMGRCSQ1, the user ID QMGRCSQ1 must have access to the z/OS resources accessed by the CSQ1 queue manager.

Ayrıca, kuyruk yöneticisinin kullanıcı kimliğindeki GROUP alanının içeriği, o kuyruk yöneticisine ilişkin STARTED profilindeki GROUP alanının içeriğiyle aynı olmalıdır. Her bir grup alanındaki içerik eşleşmiyorsa, uygun kullanıcı kimliği sisteme girilmesini önlemektedir. Bu durum, IBM MQ ' un bir güvenlik ihlali nedeniyle tanımlanmamış bir kullanıcı kimliğiyle çalışmasına ve sonuç olarak kapanmasına neden olur.

Kuyruk yöneticisiyle ve kanal başlatıcısı ile ilişkilendirilmiş RACF kullanıcı kimlikleri, görev yordamlarıyla güvenilir (TRUSTED) öznitelik kümesine sahip olmamalıdır.

z/OS *Veri kümelerine erişim yetkisi verme*

The IBM MQ data sets should be protected so that no unauthorized user can run a queue manager instance, or gain access to any queue manager data. Bunu yapmak için, olağan z/OS RACF veri kümesi korumasını kullanın.

Çizelge 65 sayfa 243 , kuyruk yöneticisinin başlattığı görev yordamlarıyla farklı veri kümelerine sahip olması gereken RACF erişimini özetler.

Çizelge 65. Bir kuyruk yöneticisiyle ilişkili veri kümelerineRACF erişimi	
RACF erişim	**Veri kümeleri**
READ	• `thlqual.SCSQAUTH` ve `thlqual.SCSQANLx` (burada x, ulusal diliniz için dil harfidir). • Kuyruk yöneticisinde başlatılan görev yordamında CSQINP1, CSQINP2 ve CSQXLIB tarafından başvurulan veri kümeleri. • Gruptaki diğer kuyruk yöneticilerine ait SMDS veri kümeleri. • Gruptaki diğer kuyruk yöneticileri için günlük, BSDS ve arşiv günlüğü veri kümelerinin günlüğe kaydedilmesini sağlar.
GÜNCELLE	• Tüm sayfa kümeleri ve günlük ve BSDS veri kümeleri. • Bir kuyruk yöneticisine ait SMDS veri kümeleri
ALTER	• Tüm arşiv günlüğü veri kümeleri.

Çizelge 66 sayfa 243 , dağıtılmış kuyruğa alma işlemine ilişkin başlatılan görev yordamlarının farklı veri kümelerine sahip olması gereken RACF erişimini özetler.

Çizelge 66. Dağıtılmış kuyruğa alma ile ilişkili veri kümelerineRACF erişimi	
RACF erişim	**Veri kümeleri**
READ	• thlqual.SCSQAUTH, thlqual.SCSQANLx (burada x, ulusal diliniz için dil harfidir) ve thlqual.SCSQMVR1. • LE kitaplığı veri kümeleri. • Kanal başlatıcı sırasında, CSQXLIB ve CSQINPX tarafından başvurulan veri kümeleri, görev yordamında başlatıldı.
GÜNCELLE	• Veri kümeleri CSQOUTX ve CSQSNAP

Daha fazla bilgi için *z/OS Security Server RACF Security Administrator's Guide*adlı yayına bakın.

z/OS V 9.1.4 *Veri kümeleri şifreleniyor*

The IBM MQ data sets can be encrypted with z/OS data set encryption, so that the data is protected, or for regulatory reasons.

z/OS veri kümesi şifrelemesiyle tüm sayfa kümelerini, etkin günlüğü, arşiv günlüğünü ve önyükleme (BSDS) veri kümelerini koruyabilirsiniz.

Uyarı: You cannot protect shared message data sets (SMDS) with z/OS data set encryption by IBM MQ for z/OS 9.1.3 or earlier.

confidentiality for data at rest on IBM MQ for z/OS with data set encryption.bölümüne bakın. daha fazla bilgi için.

z/OS *IBM MQ for z/OS kaynak güvenliğinin ayarlanması*

Birçok IBM MQ kullanıcısı tipi vardır. IBM MQ kaynaklarına erişimlerini denetlemek için RACF seçeneğini kullanın.

The possible users of IBM MQ resources, such as queues and channels include the following entities:

- Kuyruk yöneticisinin kendisi.
- Kanal başlatıcı
- IBM MQ veri kümeleri oluşturmak, yardımcı programları çalıştırmak ve benzer görevleri yapmak içinIBM MQ yöneticileri

- IBM MQtarafından sağlanan telif kitaplarını kullanması gereken uygulama programcıları, veri kümelerini, makroları ve benzeri kaynakları içerir.
- Aşağıdakilerden birini ya da daha fazlasını içeren uygulamalar:
  - Toplu işler
  - TSO kullanıcıları
  - CICS bölge
  - IMS bölge
- Veri kümeleri CSQOUTX ve CSQSNAP
- Dinamik kuyruklar SYSTEM.CSQXCMD.*

Tüm bu olası kullanıcılar için IBM MQ kaynaklarını RACFile koruyun. Özellikle, kanal başlatıcısının "Security considerations for the channel initiator on z/OS" sayfa 250içinde açıklandığı gibi çeşitli kaynaklara erişmesi gerektiğini ve bu nedenle çalıştırdığı kullanıcı kimliğinin bu kaynaklara erişmeye yetkili olması gerektiğini unutmayın.

Bir kuyruk paylaşım grubu kullanıyorsanız, kuyruk yöneticisi çeşitli komutları dahili olarak yayınlayabilir, bu nedenle kullandığı kullanıcı kimliğinin bu tür komutları yayınlaması için yetki verilmelidir. Komutlar şunlardır:

- QSGDISP (GROUP) içeren her nesne için DEFINE, ALTER ve DELETE işlemi
- CHLDISP (SHARED) ile kullanılan her kanal için START ve STOP KANAL

z/OS *Configuring your z/OS system to use TLS*

Use this topic as example of how to configure IBM MQ for z/OS with Transport Layer Security (TLS) using RACF commands.

Kanal güvenliği için TLS ' yi kullanmak istiyorsanız, sisteminizde gerçekleştirmeniz gereken bazı görevler vardır. (Sertifikalar ve anahtar havuzları (anahtar halkalar) için RACF komutlarının kullanılmasıyla ilgili ayrıntılar için bkz. z/OS üzerinde TLS ile çalışma.)

1. Create a key ring in RACF to hold all the keys and certificates for your system, using the RACF RACDCERT command. Örneğin:

   ```
   RACDCERT ID(CHINUSER) ADDRING(QM1RING)
   ```

   Tanıtıcı, kanal başlatıcı adres alanı kullanıcı kimliği ya da paylaşılan anahtar halkası olması durumunda anahtarlık (key ring) sahibi olmak istediğiniz kullanıcı kimliği olmalıdır.
2. RACF RACDCERT komutunu kullanarak, her kuyruk yöneticisi için bir sayısal sertifika yaratın.

   The label of the certificate must be either the value of the IBM MQ **CERTLABL** attribute, if it is set, or the default `ibmWebSphereMQ` with the name of the queue manager or queue sharing group appended. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın. Bu örnekte bu `ibmWebSphereMQQM1`olur.

   Örneğin:

   ```
   RACDCERT ID(USERID) GENCERT
   SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
   WITHLABEL('ibmWebSphereMQQM1')
   ```
3. Connect the certificate in RACF to the key ring, using the RACF RACDCERT command. Örneğin:

```
RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQQM1') RING(QM1RING))
CONNECT ID(CHINUSER)
```

Ayrıca, ilgili imzalayıcı sertifikalarını (bir sertifika yetkilisinden) anahtarlık ile bağlamaya da gerek vardır. Yani, bu kuyruk yöneticisinin TLS sertifikasına ilişkin tüm sertifika yetkilileri ve bu kuyruk yöneticisinin iletişim kurduğu tüm TLS sertifikalarına ilişkin tüm sertifika yetkilileridir. Örneğin:

```
RACDCERT ID(CHINUSER)
CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
```

4. Kuyruk yöneticilerinizin her birinde, kuyruk yöneticisinin işaret etmesi gereken anahtar havuzunu belirtmek için IBM MQ ALTER QMGR komutunu kullanın. Örneğin, anahtarlık kanal başlatıcı adres alanına aitse:

```
ALTER QMGR SSLKEYR(QM1RING)
```

ya da paylaşılan anahtar halkası kullanıyorsanız:

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

Burada *kullanıcı kimliği* , paylaşılan anahtar halkasının sahibi olan kullanıcı kimliğidir.

5. Sertifika İptal Listeleri (CRL ' ler), sertifika yetkililerinin artık güvenilir olmayan sertifikaları iptal edebilmesini sağlar. CRL ' ler LDAP sunucularında depolanır. LDAP sunucusunda bu listeye erişmek için, öncelikle IBM MQ DEFINE AUTHINFO komutunu kullanarak AUTHTYPE CRLLDAP için AUTHINFO nesnesi yaratmanız gerekir. Örneğin:

```
DEFINE AUTHINFO(LDAP1)
AUTHTYPE(CRLLDAP)
CONNAME(ldap.server(389))
LDAPUSER('')
LDAPPWD('')
```

Bu örnekte, sertifika iptal listesi LDAP sunucusunun genel bir alanında saklanır, böylece LDAPUSER ve LDAPPWD alanları gerekli değildir.

Daha sonra, AUTHINFO nesnesini bir ad listesine, IBM MQ DEFINE NAMELIST komutunu kullanarak bir ad listesine koyun. Örneğin:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

Son olarak, ad listesini IBM MQ ALTER QMGR komutunu kullanarak her kuyruk yöneticisiyle ilişkilendirin. Örneğin:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. TLS çağrılarını çalıştırmak için IBM MQ ALTER QMGR komutunu kullanarak kuyruk yöneticinizi ayarlayın. Bu, yalnızca SSL çağrılarını işleyen sunucu alt görevlerini tanımlar; bu da olağan dağıtıcıların herhangi bir SSL çağrısından etkilenmeden normal olarak işlemeye devam etmesini sağlar. Bu alt görevlerden en az iki tane olmalıdır. Örneğin:

```
ALTER QMGR SSLTASKS(8)
```

   Bu değişiklik, yalnızca kanal başlatıcı yeniden başlatıldığında yürürlüğe girer.
7. IBM MQ DEFINE CHANNEL ya da ALTER KANAL komutunu kullanarak, her kanal için kullanılacak şifreleme belirtimini belirtin. Örneğin:

```
ALTER CHANNEL(LDAPCHL)
CHLTYPE(SDR)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

   Kanalın her iki ucu da aynı şifre belirtimini belirtmelidir.

z/OS Kanal doğrulama kayıtlarının QSG ' de yönetilmesi

Kanal doğrulama kayıtları, oluşturuldukları kuyruk yöneticisi için geçerlidir, kuyruk paylaşım grubu (QSG) boyunca paylaşılmaz. Bu nedenle, kuyruk paylaşım grubundaki tüm kuyruk yöneticilerinin aynı kurallara sahip olması gerekiyorsa, bazı yönetmenin tüm kuralları tutarlı tutmak için yürütülmesi gerekir.

1. Always add the `CMDSCOPE(*)` option to all `SET CHLAUTH` commands. Bu komut, komutu, kuyruk paylaşım grubundaki çalışan tüm kuyruk yöneticilerine gönderir
2. Use the `DISPLAY CHLAUTH` command with the `CMDSCOPE(*)` option and then analyze the responses to see if the records are the same from all queue managers. Bir tutarsızlık bulunduğunda, `CMDSCOPE(*)` ya da `CMDSCOPE(`*qmgr-name*`)` ile aynı kural içeren bir `SET CHLAUTH` komutu yayınlanabilir.
3. Kuyruk yöneticisinin CSQINP2 birleşmesine bir üye ekleyin (ayrıntılar için Başlatma komutları konusuna bakın) bu, tam kural kümesine sahip olur. Bunlar, kuyruk yöneticisinin kullanıma hazırlama işleminin bir parçası olarak okunacaktır. `SET CHLAUTH` komutu `ACTION(ADD)` kullanıyorsa, kural yoksa, kural eklenecektir. Var olan bir kuralın yerine `ACTION(REPLACE)` kullanılması, varsa, varolan bir kuralın yerini alır. Daha sonra, aynı üye, kuyruk paylaşım grubundaki tüm kuyruk yöneticilerinin CSQINP2 birleştirmesine yerleştirilebilir.
4. Use the CSQUTIL utility (see IBM MQ komutlarına komut verilmesi (COMMAND) for details) to extract the rules from one queue manager using either the `MAKEDEF` or `MAKEREP` option. Daha sonra, CSQUTIL komutunu hedef kuyruk yöneticisine kullanarak çıktıyı yeniden yürütün.

İlgili kavramlar

Kanal doğrulama kayıtları

Kanal düzeyinde bağlanan sistemlere verilen erişim üzerinde daha kesin denetim sağlamak için kanal kimlik doğrulama kayıtlarını kullanabilirsiniz.

z/OS z/OSile ilgili denetim konuları

Olağan RACF denetim denetimleri, kuyruk yöneticisine ilişkin bir güvenlik denetimi yürütmekte kullanılabilir. IBM MQ , kendi güvenlik istatistiklerini toplamaz. Tek istatistik, denetleyerek oluşturulabilecek tek istatistiklerdir.

RACF denetimi aşağıdakine dayalı olabilir:

- Kullanıcı Kimlikleri
- Kaynak sınıfları
- Profiller

Daha fazla ayrıntı için *z/OS Security Server RACF Auditor's Guide*adlı yayına bakın.

Not: Denetleme performansı düşebilir; ne kadar çok denetim uygulansa, performans düşer. Bu, RACF WARNING seçeneğinin kullanılmasıyla da ilgili bir değerlendirmedir.

z/OS *Denetlemeyi DENETLEME*

RESLELEL denetleme kayıtlarının üretimini denetlemek için RESOAUDIT sistem parametresini kullanın. RACF GENEL denetleme kayıtları üretilir.

READUIT sistem değiştirgesini YES değerine ayarlayarak RESLEPEL denetleme kayıtları üretin. RESAUDIT parametresi NO olarak ayarlandıysa, denetleme kayıtları üretilmez. Bu parametrenin ayarlanmasıyla ilgili daha fazla ayrıntı için bkz. CSQ6SYSPkomutunu kullanma.

READUIT değeri YES olarak ayarlandıysa, bir adres alanı kullanıcı kimliğinin hlq.RESLEVEL tanıtımı için ne erişimi olduğunu görmek için RESLELEL denetimi yapıldığında, olağan RACF denetim kayıtları alınmaz. Bunun yerine IBM MQ , RACF ' un bir GENERAL denetim kaydı (olay numarası 27) yarattısını ister. Bu denetimler yalnızca bağlanma sırasında gerçekleştirilir, bu nedenle performans maliyeti en düşük düzeyde olur.

IBM MQ genel denetleme kayıtlarını RACF rapor yazarını (RACFRW) kullanarak bildirebilirsiniz. RESLELEL erişimini raporlamak için aşağıdaki RACFRW komutlarını kullanabilirsiniz:

```
RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END
```

A sample report from RACFRW, excluding the *Date*, *Time*, and *SYSID* fields, is shown in Şekil 19 sayfa 247.

```
       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
```

Şekil 19. RESLEEL genel denetleme kayıtlarını gösteren RACFRW ' den örnek çıkış

From checking the LOGSTR data in this sample output, you can see that TSO user WS21B has CONTROL access to QM66.RESLEVEL. Bu, kullanıcı WS21B tarafından QM66 kaynakları eriştiğinde tüm kaynak güvenliği denetimlerinin atlanması anlamına gelir.

RACFRW kullanılmasına ilişkin ek bilgi için *z/OS Security Server RACF Auditor's Guide*adlı yayına bakın.

z/OS Güvenliği özelleştirme

IBM MQ güvenliğinin çalışma şeklini değiştirmek istiyorsanız, bunu SAF çıkışı (ICHRFR00) aracılığıyla yapmanız ya da dış güvenlik yöneticinizin çıkışlarını yapmanız gerekir.

RACF çıkışlarıyla ilgili daha fazla bilgi için *z/OS Security Server RACROUTE Macro Reference* adlı elkitabına bakın.

Not: IBM MQ çağrıları ESM ' ye göre eniyiler; örneğin, belirli bir kullanıcı tarafından belirli bir kuyruğa ilişkin her açık için RACROUTE istekleri yapılamayabilir.

z/OS z/OSüzerindeki güvenlik ihlali iletileri

Bir güvenlik ihlali, bir uygulama programında ya da iş günlüğündeki bir iletiyle MQRC_NOT_YETKILI dönüş koduyla gösterilir.

Aşağıdaki nedenlerden dolayı, bir uygulama programına MQRC_NOT_AUTONIZED dönüş kodu döndürülebiliyor:

- Bir kullanıcının kuyruk yöneticisine bağlanmasına izin verilmiyor. Bu durumda, Toplu İş/TSO, CICSya da IMS iş günlüğüne bir ICH408I iletisi alabilirsiniz.
- Kuyruk yöneticisine kullanıcı oturum açma işlemi başarısız oldu; örneğin, iş kullanıcı kimliği geçerli ya da uygun değil ya da görev kullanıcı kimliği ya da diğer kullanıcı kimliği geçerli değil. Bu kullanıcı kimliklerinden biri ya da daha fazlası iptal edilmiş ya da silindiği için geçerli olmayabilir. Bu durumda, oturum açma başarısızlığı nedenini belirten bir ICHxxxx iletisi ve olasılıkla kuyruk yöneticisi iş günlüğünde bir IRRxxxx iletisi alabilirsiniz. Örneğin:

```
ICH408I USER(NOTDFND ) GROUP(        ) NAME(???                 )
  LOGON/JOB INITIATION - USER AT TERMINAL          NOT RACF-DEFINED
IRR012I  VERIFICATION FAILED. USER PROFILE NOT FOUND
```

- Başka bir kullanıcı istendi, ancak iş ya da görev kullanıcı kimliğinin diğer kullanıcı kimliğine erişimi yok. Bu hata nedeniyle, ilgili kuyruk yöneticisinin iş günlüğüne aykırılık iletisi alabilirsiniz.
- Bir bağlam seçeneği kullanıldı ya da çıkış için iletim kuyruğu açılarak örtük olarak kullanıldı, ancak iş kullanıcısı kimliği ya da geçerli olduğu durumlarda, görev ya da diğer kullanıcı kimliğinin bağlam seçeneğine erişimi yok. Bu durumda, ilgili kuyruk yöneticisinin iş günlüğüne aykırılık iletisi konması gerekir.
- Yetkisiz bir kullanıcı, güvenli bir kuyruk yöneticisi nesnesine (örneğin, bir kuyruk) erişme girişiminde bulundu. Bu durumda, aykırılık için bir ICH408I iletisi, ilgili kuyruk yöneticisinin iş günlüğüne konmaktadır. Bu aykırılık, işin ya da ilgili görevin, görevin ya da diğer kullanıcı kimliğinin nedeni olabilir.

Komut güvenliği ve komut kaynağı güvenliği için ihlal iletileri, kuyruk yöneticisinin iş günlüğünde de bulunabilir.

ICH408I ihlali iletisi, bir kullanıcı kimliği yerine kuyruk yöneticisi iş adını gösteriyorsa, olağan durumda bu, boş bir diğer kullanıcı kimliğinin belirlenmesinden kaynaklanır. Örneğin:

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          INSUFFICIENT ACCESS AUTHORITY
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

MQADMINMQADMIN tanıtımının erişim listesini denetleyerek boş diğer kullanıcı kimliklerini kullanma izni olan kişileri bulabilirsiniz. hlq.ALTERNATE.USER.-BLANK-.

Aşağıdaki gibi bir ICH408I ihlali iletisi de oluşturulabilir:

- Sistem komutu giriş kuyruğuna bağlam olmadan gönderilen bir komut. Sistem komutu giriş kuyruğuna yazan kullanıcı tarafından yazılan programlar her zaman bir bağlam seçeneği kullanmalıdır. Daha fazla bilgi için bkz “Bağlam güvenliğine ilişkin profiller” sayfa 206.
- IBM MQ kaynağına erişen iş, kendisiyle ilişkilendirilmiş bir kullanıcı kimliğine sahip değilse ya da bir IBM MQ bağdaştırıcısı kullanıcı kimliğini bağdaştırıcı ortamından çıkaramıyorsa.

Hem kuyruk paylaşım grubu, hem de kuyruk yöneticisi düzeyinde güvenlik kullanıyorsanız, ihlal iletileri de yayınlanabilir. Kuyruk yöneticisi düzeyinde herhangi bir tanıtımın bulunamadığını, ancak kuyruk paylaşım grubu düzeyi tanıtımı nedeniyle erişim verilmeye devam ettiğini bildiren iletiler alabilirsiniz.

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

z/OS Erişime izin verilirse ya da yanlış izin verilirse ne yapılır

*z/OS Security Server RACF Security Administrator's Guide*adlı yayında ayrıntılı olarak açıklanan adımlara ek olarak, bir kaynağa erişim yanlış olarak denetleniyorsa bu denetim listesini kullanın.

- Anahtar profilleri doğru ayarlanmış mı?
  - RACF etkin mi?
  - Are the IBM MQ RACF classes installed and active?

    Bunu denetlemek için RACF komutunu, SETROPTS LIST ' i kullanın.
  - Yürürlükteki anahtar durumunu kuyruk yöneticisinden görüntülemek için IBM MQ DISPLAY SECURITY komutunu kullanın.
  - MQADMIN sınıfındaki anahtar tanıtımlarını denetleyin.

    Use the RACF commands, SEARCH and RLIST, for this.
  - IBM MQ REFRESH SECURITY (MQADMIN) komutunu vererek RACF anahtar profillerini yeniden denetleyin.
- RACF kaynak profili değişti mi? Örneğin, tanıtıma ilişkin evrensel erişim değişti mi, yoksa tanıtımın erişim listesi değişti mi?
  - Profil genel mi?

    Eğer varsa, RACF komutunu verin, SETROPTS GENERIC (sınıf adı) YENILE.
  - Bu kuyruk yöneticisindeki güvenliği yenilediniz mi?

    Gerekiyorsa, RACF komutunu SETROPTS RACLIST (sınıf adı) komutunu verin. YENILE.

    Gerekiyorsa, IBM MQ REFRESH SECURITY (*) komutunu verin.
- Kullanıcının RACF tanımlaması değişti mi? Örneğin, kullanıcı yeni bir gruba bağlı mı, yoksa kullanıcı erişim yetkisi iptal mi edildi?
  - Have you reverified the user by issuing the IBM MQ RVERIFY SECURITY(userid) command?
- RESLELEL nedeniyle güvenlik denetimleri atlanıyor mu?
  - Bağlanılan kullanıcı kimliğinin RESLEVL tanıtıma erişimini denetleyin. RESLEGEL ' in ayarının ne olduğunu belirlemek için RACF denetleme kayıtlarını kullanın.
  - Kanallar için, kanal başlatıcısının kullanıcı kimliğinin RESLELEL için sahip olduğu erişim düzeyinin tüm kanallar tarafından devralındığını unutmayın; bu nedenle, ALTER gibi bir erişim düzeyi atlanacak tüm denetimlerin tüm kanallar için atlanacak güvenlik denetimlerine neden olmasına neden olur.
  - CICS' tan çalıştırılıyorsanız, hareketin RESSEC ayarını denetleyin.
  - Bir kullanıcı bağlıyken RESLEVEL değiştirildiyse, yeni RESLEVEL ayarının yürürlüğe girmesinden önce bağlantı kesmeleri ve yeniden bağlanmaları gerekir.
- Kuyruk paylaşım gruplarını kullanıyor musunuz?
  - Hem kuyruk paylaşım grubu, hem de kuyruk yöneticisi düzeyinde güvenlik kullanıyorsanız, doğru tanıtımların tümünü tanımladığınızı doğrulayın. Kuyruk yöneticisi tanıtımı tanımlı değilse, tanıtıma bulunamadığını bildiren bir ileti günlüğe gönderilir.
  - Tam güvenlik denetimine ilişkin geçerli olmayan bir anahtar ayarı bileşimi kullandınız mı?
  - Kuyruk yöneticinizin kuyruk paylaşım grubu ayarlarını geçersiz kılmak için güvenlik anahtarları tanımlamanız gerekiyor mu?

– Kuyruk yöneticisi düzeyinde bir profil, kuyruk paylaşım grubu düzeyi profiline göre öncelikli mi?

z/OS Security considerations for the channel initiator on z/OS

Dağıtılmış bir kuyruğa alma ortamında kaynak güvenliği kullanıyorsanız, Kanal başlatıcı adres alanının çeşitli IBM MQ kaynaklarına uygun erişimleri olması gerekir. Parola koruma algoritmasını tohumlamak için Integrated Cryptographic Support Facility (ICSF) olanağını kullanabilirsiniz.

Kaynak güvenliğinin kullanılması

Kaynak güvenliği kullanıyorsanız, dağıtımlı kuyruğa alma kullanıyorsanız aşağıdaki noktaları göz önünde bulundurun:

Sistem kuyrukları
The channel initiator address space needs RACF UPDATE access to the system queues listed at "Sistem kuyruğu güvenliği" sayfa 196, and to all the user destination queues and the dead-letter queue (but see "Ölü-mektup kuyruğu güvenliği" sayfa 194).

İletim kuyrukları
Kanal başlatıcı adres alanının tüm kullanıcı iletim kuyruklarına ilişkin ALTER erişimi gerekir.

Bağlam güvenliği
Kanal kullanıcı kimliği (ve belirtilmişse MCA kullanıcı kimliği), MQADMIN sınıfındaki hlq.CONTEXT.queuename tanıtımlarıyla RACF CONTROL erişimine sahip olmalıdır. RESLELEL tanıtımına bağlı olarak, kanal kullanıcı kimliğinin bu tanıtımlara CONTROL erişimi de gerekebilir.

Tüm kanalların MQADMIN hlq.CONTEXTiçin CONTROL erişimine sahip olması gerekir. -Ölü harf kuyruğu profili. Tüm kanallar (başlatmaya ya da yanıtlamaya ilişkin) raporlar oluşturabilir ve bunun sonucunda hlq.CONTEXT.reply-q profili için CONTROL (Kontrol) erişimine sahip olur.

SENDER, CLUSSDR Ve Sunucu Kanallarının, iletileri zarafetle sona erdirmek üzere iletim kuyruğuna yerleştirebilmeleri için, ileti iletim kuyruğuna konabileceği için, hlq.CONTEXT.xmit-queue-name tanıtımlarına CONTROL (denetim) erişimi gerekir.

Not: Kanal kullanıcı kimliği ya da kanal kullanıcı kimliğinin bağlı olduğu bir RACF grubu, hlq.RESLEVELiçin CONTROL ya da ALTER (ALTER) erişimine sahipse, kanal başlatıcısı ya da kanallarının herhangi bir kaynağı için kaynak denetimi yoktur.

Daha fazla bilgi için bkz. "Bağlam güvenliğine ilişkin profiller" sayfa 206 "RESLELEL ve kanal başlatıcı bağlantısı" sayfa 225 ve "z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri" sayfa 227 .

CSQINPX
If you are using the CSQINPX input data set, the channel initiator also needs READ access to CSQINPX, and UPDATE access to data set CSQOUTX and dynamic queues SYSTEM.CSQXCMD.*.

Bağlantı güvenliği
Kanal başlatıcı adres alanı bağlantı istekleri, uygun erişim güvenliğinin ayarlanması gereken bir bağlantı tipini (CHIN) kullanır; bkz. "Kanal başlatıcısı için bağlantı güvenliği profilleri" sayfa 189.

Veri kümeleri
Kanal başlatıcı adres alanının kuyruk yöneticisi veri kümeleri için uygun erişime ihtiyacı var, bkz. "Veri kümelerine erişim yetkisi verme" sayfa 242.

Komutlar
Dağıtılmış kuyruğa alma komutlarının (örneğin, DEFINE CHANNEL, START CHINIT, START LISTENER ve diğer kanal komutları) uygun komut güvenliği kümesine sahip olması gerekir, bkz. Çizelge 49 sayfa 209.

Bir kuyruk paylaşım grubu kullanıyorsanız, kanal başlatıcısı çeşitli komutları dahili olarak yayınlayabilir, bu nedenle kullandığı kullanıcı kimliğinin bu tür komutları yayınlaması için yetki verilmelidir. Bu komutlar, CHLDS (SHARED) ile kullanılan her kanal için START (START) ve STOP (KANAL) komutlarını içerir.

Kuyruk yöneticisinin PSMODE değeri geçersiz kılınmadıysa, kanal başlatıcının DISPLAY PUBALT komutuna okuma erişimi olmalıdır.

Kanal güvenliği

Kanallar, özellikle günlük nesneleri ve sunucu bağlantıları, ayarlanabilmek için uygun güvenlik gerekir; ek bilgi için bkz. “z/OSüzerinde güvenlik denetimi için kullanıcı kimlikleri” sayfa 227 .

Kanallarda güvenliği sağlamak için TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolünü de kullanabilirsiniz. TLS ' nin IBM MQile kullanılmasına ilişkin ek bilgi için “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22 konusuna bakın.

Sunucu bağlantısı güvenliğiyle ilgili bilgi için bkz. “İstemciler için erişim denetimi” sayfa 93 .

Kullanıcı Kimlikleri

“Kanal başlatıcısı tarafından kullanılan kullanıcı kimlikleri” sayfa 230 ve “Grup içi kuyruğa alma aracısı tarafından kullanılan kullanıcı kimlikleri” sayfa 234 ' ta açıklanan kullanıcı kimlikleri aşağıdaki erişime gereksinim duyarlar:

- RACF UPDATE erişimi, uygun hedef kuyruklara ve ölü-mektup kuyruğuna erişir
- RACF CONTROL access to the `hlq.CONTEXT.queuename` profile if context checking is performed at the receiver
- hlq.ALTERNATE.USER.userid tanıtımlarını.
- İstemciler için, kullanılacak kaynaklar için uygun RACF erişimi.

APPC güvenliği

LU 6.2 iletim protokolünü kullanıyorsanız, uygun APPC güvenliğini ayarlayın. (Örneğin, APPCLU RACF sınıfını kullanın.) APPC ' nin güvenliğini ayarlama hakkında bilgi için aşağıdaki elkitaplarına bakın:

- *z/OS V1R2.0 MVS Planlama: APPC Yönetimi*
- *Çoklu platform APPC Yapılandırma Kılavuzu*, bir IBM Redbooks yayını

Giden iletimler "SECURITY (SAME)" APPC seçeneğini kullanır. Sonuç olarak, kanal başlatıcı adres alanının kullanıcı kimliği ve varsayılan tanıtımı (RACF GROUP), kullanıcı kimliğinin doğrulanmış (ALREADYV) olduğunu gösteren bir göstergeyle, ağ üzerinden alıcıya akıp geçmiştir.

Giriş tarafı da z/OSise, kullanıcı kimliği ve tanıtımı APPC tarafından doğrulanır ve kullanıcı kimliği alıcı kanalına sunulur ve kanal kullanıcı kimliği olarak kullanılır.

Kuyruk yöneticisinin aynı ya da başka bir z/OS sisteminde başka bir kuyruk yöneticisiyle iletişim kurmak için APPC kullandığı bir ortamda aşağıdakilerden birini doğrulamanız gerekir:

- İletişen LU ' ya ilişkin VTAM tanımlaması SETACPT (ALREADYV) değerini belirtir.
- LU ' lar arasında CONVSEC (ALREADYV) değerini belirten bağlantı için bir RACF APPCLU profili vardır.

Güvenlik ayarlarının değiştirilmesi

Kanal kullanıcı kimliği ya da MCA kullanıcı kimliğinin bir hedef kuyruğa sahip olması gereken RACF erişim düzeyi değişirse, bu değişiklik yalnızca hedef kuyruk için yeni nesne tanıtıcıları (yani, yeni MQOPER ' ler) için yürürlüğe girer. MCA ' nın kuyrukları açma ve kapatma süreleri değişkendir; böyle bir erişim değişikliği yapıldığında bir kanal zaten çalışıyorsa, MCA, güncellenen güvenlik erişimi yerine, kullanıcı kimliklerinin var olan güvenlik erişimini kullanarak hedef kuyruğa ileti koymaya devam edebilir. Güncellenen erişim düzeyini uygulamak için kanalların durdurulması ve yeniden başlatılması bu senaryonun engellenmesini sağlar.

Otomatik yeniden başlatma

If you are using the z/OS Automatic Restart Manager (ARM) to restart the channel initiator, the user ID associated with the XCFAS address space must be authorized to issue the IBM MQ START CHINIT command.

Integrated Cryptographic Service Facility (ICSF) olanağının kullanılması

Kanal başlatıcı, TLS kullanılmıyorsa, istemci kanallarının üzerinden akan parolaların karartılması için parola koruma algoritmasını görürken rasgele bir sayı oluşturmak için ICSF ' yi kullanabilir. Rasgele sayı oluşturma işleminin adı *entropi*olarak adlandırılır.

If you have the z/OS feature installed but have not started ICSF, you see message CSQX213E and the channel initiator uses STCK for entropy.

CSQX213E iletisi, parola koruma algoritmasının olduğu kadar güvenli olmadığı konusunda sizi uyarır. Ancak, sürecinizi devam ettirebilirsiniz; çalıştırma zamanında başka bir etki yok.

z/OS özelliği kurulu değilse, kanal başlatıcısı STCK ' yi otomatik olarak kullanır.

Notlar:

1. Entropi için ICSF kullanılması, STCK ' ı kullanmaya göre daha rasgele sıralar oluşturur.
2. ICSF ' yi başlatayorsanız, kanal başlatıcıyı yeniden başlatmalısınız.
3. Belirli CipherSpecsiçin iCSF gereklidir. If you attempt to use one of these CipherSpecs and you do not have ICSF installed, you receive message CSQX629E.

z/OS z/OSüzerindeki kuyruk yöneticisi kümelerindeki güvenlik

Kümeler için güvenlik konuları, kümelenmemiş kuyruk yöneticileri ve kanallar için de aynıdır. Kanal başlatıcının bazı ek sistem kuyruklarına erişmesi ve bazı ek komutların uygun güvenlik kümesine gerek duyması gerekir.

MCA kullanıcı kimliğini, kanal kimlik doğrulama kayıtlarını, TLS ' yi ve küme kanallarını doğrulamak için güvenlik çıkışlarını kullanabilirsiniz (geleneksel kanallarda olduğu gibi). Kanal doğrulama kayıtları ya da küme alıcı kanalına ilişkin güvenlik çıkışı, uzak kuyruk yöneticisinin sunucu kuyruğu yöneticisinin küme kuyruklarına erişmesine izin verilip verilmemesine izin vermelidir. Var olan kuyruk erişim güvenliğinizi değiştirmeden IBM MQ küme desteğini kullanmaya başlayabilirsiniz. Ancak, kümedeki diğer kuyruk yöneticilerinin kümeye katılmaları durumunda SYSTEM.CLUSTER.COMMAND.QUEUE ' a yazmalarına izin vermelisiniz.

IBM MQ küme desteği, bir kümenin bir üyesini yalnızca istemci rolleriyle sınırlandırmak için bir mekanizma sağlamaz. Sonuç olarak, kümeye izin verdiğiniz kuyruk yöneticilerine güvendiğinizden emin olmanız gerekir. Kümedeki herhangi bir kuyruk yöneticisi belirli bir adı taşıyan bir kuyruk yarattıysa, uygulamanın bu kuyruğa ileti koyup koymadığına bakılmaksızın, bu kuyruğa ilişkin iletileri alabilir.

Bir kümenin üyeliğini kısıtlamak için, alıcı kanallarına bağlanan kuyruk yöneticilerini önlemek için bu işlemi yapmak üzere aynı işlemi gerçekleştirin. Bir kümeyle üyeliği, kanal doğrulama kayıtlarını kullanarak ya da alıcı kanalına bir güvenlik çıkış programı yazarak kısıtladınız. Yetkisiz kuyruk yöneticilerinin SYSTEM.CLUSTER.COMMAND.QUEUE' e yazmasını önlemek için bir çıkış programı da yazabilirsiniz.

Not: Uygulamaların SYSTEM.CLUSTER.TRANSMIT.QUEUE doğrudan. Ayrıca, bir uygulamanın başka bir iletim kuyruğunu doğrudan açmasına izin vermek de önerilmez.

Kaynak güvenliği kullanıyorsanız, “Security considerations for the channel initiator on z/OS” sayfa 250içinde yer alan dikkat edilecek noktalara ek olarak aşağıdaki noktaları göz önünde bulundurun:

Sistem kuyrukları
Kanal başlatıcısında aşağıdaki sistem kuyruklarına RACF ALTER erişimi gerekir:

- SYSTEM.CLUSTER.COMMAND KUYRUK
- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

ve SYSTEM.CLUSTER.REPOSITORY.QUEUE

Ayrıca, kümeleme için kullanılan ad listelerine okuma erişimine de gerek vardır.

Komutlar
Uygun komut güvenliğini ayarlayın (Çizelge 49 sayfa 209 içinde açıklandığı gibi) Küme desteği komutları için (REFRESH VE RESET CLUSTER, SUSPEND ve RESUME QMGR.

z/OS Security considerations for using IBM MQ with CICS

All the CICS versions supported by IBM MQ 9.0.0, and later, use the CICS supplied version of the adapter and bridge.

Güvenlikle ilgili önemli noktalar için aşağıdaki başlara bakın:

- CICS-IBM MQ bağdaştırıcısına ilişkin güvenlik.

- CICS-IBM MQ köprüsü için güvenlik.

z/OS Security considerations for using IBM MQ with IMS

Use this topic to plan your security requirements when you use IBM MQ with IMS.

OPERCMDS sınıfının kullanılması

OPERCMDS sınıfındaki kaynakları korumak için RACF kullanıyorsanız, IBM MQ kuyruk yöneticisi adres alanınızla ilişkili kullanıcı kimliğinin, MODIFY komutunu, bağlanabileceği herhangi bir IMS sistemi için verme yetkisi olduğundan emin olun.

IMS köprüsü için güvenlik konuları

IMS köprüsü için güvenlik gereksinimlerinize karar verirken göz önünde bulundurmanız gereken dört bir öğe vardır:

- IBM MQ 'u IMS' e bağlamak için hangi güvenlik yetkilendirmesi gerekir
- How much security checking is performed on applications using the bridge to access IMS
- Bu uygulamaların kullanılmasına izin verilen IMS kaynakları
- köprü tarafından konulan ve elde edilen mesajlar için hangi otorite kullanılacak?

IMS köprüsü için güvenlik gereksinimlerinizi tanımladığınızda şunları göz önünde bulundurmanız gerekir:

- Köprüyü geçen iletiler, güçlü güvenlik özellikleri sunmayan platformlardaki uygulamalardan kaynaklanabilir.
- Köprüden geçen iletiler, aynı kurum ya da kuruluş tarafından denetlenmeyen uygulamalardan kaynaklanabilir.

z/OS *IMS' a bağlanmaya ilişkin güvenlik konuları*

OTMA grubuna IBM MQ kuyruk yöneticisi adres alanı erişimi için kullanıcı kimliği atayın.

IMS köprüsü bir OTMA istemcidir. IMS bağlantısı, IBM MQ kuyruk yöneticisi adres alanı kullanıcı kimliği altında çalışır. Olağan durumda bu, başlatılan görev grubunun bir üyesi olarak tanımlanır. Bu kullanıcı kimliğine, OTMA grubuna erişim izni verilmelidir (/SECURE OTMA ayarı NONE değilse).

Bunu yapmak için, TESIS sınıfında aşağıdaki profili tanımlayın:

```
IMSXCF.xcfgname.mqxcfmname
```

Where `xcfgname` is the XCF group name and `mqxcfmname` is the XCF member name of IBM MQ.

Bu profil için IBM MQ kuyruk yöneticisi kullanıcı kimliği okuma erişimi vermelisiniz.

Not:

1. TESIS sınıfındaki yetkileri değiştirirseniz, değişiklikleri etkinleştirmek için RACF komutunun SETROPTS RACLIST (TESIS) REFRESH komutunu yayınlamanız gerekir.
2. MQADMIN sınıfında hlq.NO.SUBSYS.SECURITY tanıtımı varsa, hiçbir kullanıcı kimliği IMS ' e iletilmez ve /SECURE OTMA ayarı NONE değilse bağlantı başarısız olur.

z/OS *IMS köprüsü için uygulama erişim denetimi*

Her bir IMS sistemi için TESIS sınıfında bir RACF profili tanımlayın. IBM MQ kuyruk yöneticisi kullanıcı kimliğine uygun bir erişim düzeyi atayın.

IMS köprüsünün bağlandığı her bir IMS sistemi için, IMS sistemine aktarılan her ileti için ne kadar güvenlik denetimi gerçekleştirildiğini belirlemek üzere TESIS sınıfında aşağıdaki RACF tanıtımını tanımlayabilirsiniz.

```
IMSXCF.xcfgname.imsxcfmname
```

Burada `xcfgname` , XCF grup adı ve `imsxcfmname` , IMSiçin XCF üyesi adıdır. (Her bir IMS sistemi için ayrı bir profil tanımlamanız gerekir.)

Bu tanıtımda IBM MQ kuyruk yöneticisi kullanıcı kimliği için izin verdiğiniz erişim düzeyi, IMS köprüsü IMS'e bağlandığında IBM MQ ' a döndürülür ve sonraki işlemlerde gereken güvenlik düzeyini belirtir. Sonraki işlemler için IBM MQ , uygun hizmetleri RACF 'den ister ve kullanıcı kimliğinin yetkilendirilmiş olduğu durumlarda iletiyi IMS' e iletir.

OTMA, IMS /SIGN komutunu desteklemez; ancak, IBM MQ , gerekli denetim düzeyinin uygulanmasını etkinleştirmek için her ileti için erişim denetimini ayarlamanıza olanak tanır.

Aşağıdaki erişim düzeyi bilgileri döndürülebiliyor:

TANıTıM YA DA PROFIL BUL
Bu değerler, en yüksek düzeyde güvenlik gerektiğini belirtir; yani, her işlem için kimlik doğrulaması gereklidir. MQMD yapısının *UserIdentifier* alanında belirtilen kullanıcı kimliğinin ve MQIIH yapısının *Authenticator* alanındaki parolanın ya da PassTicket parolasının RACFolarak bilindiğini ve geçerli bir birleşim olduğunu doğrulamak için bir onay imi vardır. Bir UTOKEN, bir parola ya da PassTicketile oluşturulur ve IMS ' a iletilir; UTOKEN önbelleğe alınmıyor.

Not: MQADMIN sınıfında hlq.NO.SUBSYS.SECURITY tanıtımı varsa, bu güvenlik düzeyi tanıtımda tanımlı olan her şeyi geçersiz kılar.

READ
Bu değer, aşağıdaki koşullar altında aynı kimlik doğrulamasının NONE olarak gerçekleştirileceğini belirtir:

- Belirli bir kullanıcı kimliği ile ilk kez karşılaşıldığında
- Daha önce kullanıcı kimliği saptandığında, ancak önbelleğe alınan UTOKEN bir parolayla ya da PassTicketile yaratılmadığında

IBM MQ gerekirse bir UTOKEN ister ve bunu IMS' a iletir.

Not: Güvenliği yeniden doğrulama isteği yürürlüğe girdiyse, önbelleğe alınan tüm bilgiler kaybolur ve her kullanıcı kimliğinin ilk kez saptanması için bir UTOKEN değeri istenir.

GÜNCELLE
MQMD yapısının *UserIdentifier* alanında kullanıcı kimliğinin RACFtarafından bilindiği bir denetim yapılır.

Bir UTOKEN, IMS ' a oluşturulur ve iletilir; UTOKEN önbelleğe alındı.

DENETIMLI/ALTER
Bu değerler, bu IMS sistemi için herhangi bir kullanıcı kimliği için herhangi bir güvenlik UTOKENIN sağlanmadığına işaret eder. (Bu seçeneği yalnızca geliştirme ve test sistemleri için kullanmanız gerekir.)

Uyarı: MQMD yapısındaki *UserIdentifier* alanında bulunan kullanıcı kimliğinin **CONTROL/ ALTER**için hala iletilmeye devam ettiğini unutmayın.

Not:

1. Bu erişim, IBM MQ IMS' a bağlandığında tanımlanır ve bağlantı süresi boyunca sürer. Güvenlik düzeyini değiştirmek için, güvenlik profiline erişim değiştirilmeli ve sonra köprü durdurulur ve yeniden başlatılmalıdır (örneğin, OTMA ' yı durdurup yeniden başlatın).
2. TESIS sınıfındaki yetkileri değiştirirseniz, değişiklikleri etkinleştirmek için RACF komutunun SETROPTS RACLIST (TESIS) REFRESH komutunu yayınlamanız gerekir.

3. Bir parola ya da bir PassTicketkullanabilirsiniz, ancak IMS köprüsünün verileri şifrelemediğini unutmamalısınız. PassTickets' ın kullanılmasıyla ilgili bilgi için bkz. “IMS üstbilgisinde RACF PassTickets ' ı kullanma” sayfa 256.
4. Bu sonuçların bazıları, /SECURE OTMA komutu kullanılarak IMSiçindeki güvenlik ayarlarından etkilenebilir.
5. Önbelleğe alınan UTOKEN bilgileri, IBM MQ ALTER SECURITY komutunun INTERVAL ve TIMEOUT değiştirgeleriyle tanımlanan süre için tutulur.
6. RACF WARNING seçeneği, IMSXCF.xcfgname.imsxcfmname profili üzerinde bir etkisi yoktur. Bu kullanım, verilen erişim düzeyini etkilemez ve hiçbir RACF UYARI iletisi üretmez.

z/OS *IMSüzerinde güvenlik denetimi*

Köprüde geçen iletiler güvenlik bilgilerini içerir. Yapılan güvenlik denetimleri, IMS komutunun /SECURE OTMA komutunun ayarına bağlıdır.

Köprüden geçen her IBM MQ iletisi aşağıdaki güvenlik bilgilerini içerir:

- MQMD yapısındaki *UserIdentifier* alanında bulunan bir kullanıcı kimliği
- MQIIH yapısındaki *SecurityScope* alanında bulunan güvenlik kapsamı (MQIIH yapısı varsa)
- Bir UTOKEN (IBM MQ alt sistemi, ilgili `IMSXCF.xcfgname.imsxcfmname` tanıtımına CONTROL ya da ALTER erişimine sahip değilse)

Yapılan güvenlik denetimleri IMS komutunun /SECURE OTMA komutunun ayarına bağlı olarak değişir:

/GüVENLI OTMA
İşlem için herhangi bir güvenlik denetimi yapılmadı.

/GüVENLI OMA DENETIMI
MQMD yapısındaki *UserIdentifier* alanı, hareket ya da komut yetkisi denetimi için IMS ' e geçirilir.

IMS denetim bölgesinde bir ACEE (Accessor Environment Element) oluşturulur.

/SECURE OTMA FULL
MQMD yapısındaki *UserIdentifier* alanı, hareket ya da komut yetkisi denetimi için IMS ' e geçirilir.

IMS bağımlı bölgesinde ve IMS denetim bölgesinin yanı sıra, bir ACEE oluşturulur.

/SECURE OTMA PROFILI
MQMD yapısındaki *UserIdentifier* alanı, hareket ya da komut yetkisi denetimi için IMS ' e geçirilir.

MQIIH yapısındaki *SecurityScope* alanı, denetim bölgesinin yanı sıra IMS bağımlı bölgesinde bir ACEE oluşturulup oluşturulmayacağını belirlemek için kullanılır.

Not:

1. TIMS ya da CIMS sınıfında ya da GIMS ya da DIMSilişkili grup sınıflarındaki yetkileri değiştirirseniz, değişiklikleri etkinleştirmek için aşağıdaki IMS komutlarını yayınlamanız gerekir:
   - /DEğIşTIR RACF
   - /KALDıRMA
2. /SECURE OTMA TANıTıMı KULLANMAZSANıZ, MQIIH yapısının *SecurityScope* alanında belirtilen değer yoksayılır.

z/OS *Security checking done by the IMS bridge*

Gerçekleştirilmekte olan işleme bağlı olarak farklı yetkiler kullanılır.

Köprü bir ileti yerleştirdiğinde ya da aldığında, aşağıdaki yetkiler kullanılır:

Köprü kuyruğundan ileti alınıyor
Hiçbir güvenlik denetimi gerçekleştirilmedi.

Bir kural dışı durum ya da COA rapor iletisi koyma
MQMD yapısındaki *UserIdentifier* alanında kullanıcı kimliğinin yetkisini kullanır.

Yanıt iletisi koyma
Özgün iletinin MQMD yapısındaki *UserIdentifier* alanında kullanıcı kimliğinin yetkisini kullanır.

İleti kuyruğuna ileti konması
Hiçbir güvenlik denetimi gerçekleştirilmedi.

Not:

1. IBM MQ sınıfı tanıtımlarını değiştirirseniz, değişiklikleri etkinleştirmek için IBM MQ REFRESH SECURITY (*) komutunu yayınlamanız gerekir.
2. Bir kullanıcının yetkisini değiştirirseniz, değişikliği etkinleştirmek için MQSC RVERIFY SECURITY komutunu yayınlamanız gerekir.

z/OS *IMS üstbilgisinde RACF PassTickets ' ı kullanma*

IMS üstbilgisindeki bir parola yerine PassTicket (PassTicket) kullanabilirsiniz.

IMS üstbilgisindeki (MQIIH) bir parola yerine bir PassTicket kullanmak istiyorsanız, iletinin yöneltileceği IMS köprü kuyruğunun STGCLASS tanımlamasının PASSTKTA özniteisinde PassTicket ' un geçerliliği denetlenecek uygulama adını belirtin.

PASSTKTA değeri boş bırakılırsa, oluşturulan bir PassTicket ' ne sahip olmak için ayarlamalısınız. Bu durumda uygulama adı MVSxxxx biçiminde olmalıdır; burada xxxx, hedef kuyruk yöneticisinin çalıştığı z/OS sisteminin SMFID 'sidir.

PassTicket , bir kullanıcı kimliğinden, hedef uygulama adından ve gizli bir anahtardan oluşturulur. Bu, büyük harf alfabetik ve sayısal karakterler içeren 8 baytlık bir değerdir. Yalnızca bir kez kullanılabilir ve 20 dakikalık bir süre için geçerli olur. Bir PassTicket yerel bir RACF sistemi tarafından oluşturulduysa, RACF yalnızca profilin var olduğunu ve kullanıcının profil üzerinde yetkiye sahip olduğunu denetleyerek denetler. PassTicket uzak bir sistemde oluşturulduysa, RACF kullanıcı kimliğinin tanıtıma erişimini doğrular. PassTicketshakkında tam bilgi için, *z/OS SecureWay Security Server RACF Security Administrator's Guide*adlı yayına bakın.

PassTickets in IMS headers are given to RACF by IBM MQ, not IMS.

z/OS z/OS Kuyruk yöneticisinin büyük ve küçük harfe karışık olarak geçirilmesi

Bir kuyruk yöneticisini karma vaka güvenliğine geçirmek için bu adımları izleyin. Kullanmakta olduğunuz güvenlik ürünü düzeyini gözden geçirmenizi ve yeni IBM MQ dış güvenlik izleme sınıflarını etkinleştirmenizi sağlar. Karma vaka profillerini etkinleştirmek için **REFRESH SECURITY** komutunu çalıştırın.

Başlamadan önce

1. Tüm IBM MQ dış güvenlik izleyicisi sınıflarının etkinleştirildiğinden emin olun.
2. Kuyruk yöneticinizin başlatıldığından emin olun.

Bu görev hakkında

Bir kuyruk yöneticisini büyük ve küçük harfe dönüştürülecek şekilde dönüştürmek için aşağıdaki adımları izleyin.

Yordam

1. Var olan tüm profillerinizi ve erişim düzeylerinizi büyük harfli sınıflardan eşdeğer karma vaka dış güvenlik izleyici sınıfına kopyalayın.
   a) `MQADMIN` - `MXADMIN`.
   b) `MQPROC` - `MXPROC`.
   c) `MQNLIST` - `MXNLIST`.

d) MQQUEUE - MXQUEUE.

2. SCYCASE özniteliğinin değerini MIXEDolarak değiştirin.

```
ALTER QMGR SCYCASE(MIXED)
```

3. Var olan güvenlik profillerinizi etkinleştirin.

```
REFRESH SECURITY(*) TYPE(CLASSES)
```

4. Güvenlik profillerinizin doğru biçimde çalıştığını test edin.

Sonraki adım

Profiller uygulamasını etkinleştirmek için gerekli olan **REFRESH SECURITY** ' i kullanarak nesne tanımlarınızı gözden geçirin ve uygun şekilde yeni karışık vaka profilleri oluşturun.

IBM MQ MQI client güvenliğini ayarlama

İstemci uygulamalarının sunucudaki kaynaklara sınırsız erişimi olmadığından, IBM MQ MQI client güvenliğini göz önünde bulundurmanız gerekir.

Bir istemci uygulamasını çalıştırırken, uygulamayı gerekenden daha fazla erişim hakkına sahip olan bir kullanıcı kimliğini kullanarak çalıştırmayın; örneğin, mqm grubundaki bir kullanıcı ya da mqm kullanıcısının kendisi.

Bir uygulamayı çok fazla erişim hakkına sahip bir kullanıcı olarak çalıştırarak, yanlışlıkla ya da kötü bir şekilde kuyruk yöneticisinin bazı kısımlarıyla erişilmesine ilişkin riski de çalıştırıyorsunuz demektir.

Bir istemci uygulaması ile kuyruk yöneticisi sunucusu arasında güvenliğin iki yönü vardır: kimlik doğrulama ve erişim denetimi.

- Kimlik doğrulaması, istemci uygulamasının belirli bir kullanıcı olarak çalıştırılmasını sağlamak için kullanılabilir; bu kullanıcılar, bu uygulamanın ne olduğunu söylemekte olduğunu söyler. Kimlik doğrulamasını kullanarak, bir saldırganın uygulamalarınızdan birini taklit ederek kuyruk yöneticinize erişim kazanmasını önleyebilirsiniz.

  IBM MQ 8.0' tan, kimlik doğrulama iki seçenekten biri tarafından sağlanır:

  – Bağlantı kimlik doğrulaması özelliği.

    Bağlantı kimlik doğrulamasıyla ilgili daha fazla bilgi için bkz. “Bağlantı kimlik doğrulaması” sayfa 64.

  – TLS içinde karşılıklı kimlik doğrulaması kullanılıyor.

    TLS ' ye ilişkin daha fazla bilgi için bkz. “SSL/TLS ile çalışma” sayfa 261.

- Erişim denetimi, belirli bir kullanıcı ya da kullanıcı grubu için erişim hakları vermek ya da kaldırmak için kullanılabilir. Belirli bir kullanıcıyı (ya da belirli bir gruptaki bir kullanıcıya) içeren bir istemci uygulamasını çalıştırarak, uygulamanın kuyruk yöneticinizin bazı kısımlarıyla uygulamanın gerekmediği kısımlarına erişememesini sağlamak için erişim denetimlerini kullanabilirsiniz.

  Erişim denetimini ayarlarken, kanal doğrulama kurallarını ve bir kanaldaki MCAUSER alanını göz önünde bulundurmanız gerekir. Bu özelliklerin her ikisi de, erişim denetimi haklarını doğrulamak için hangi kullanıcı kimliğinin kullanıldığını değiştirebilme yeteneğine sahiptir.

  Erişim denetime ilişkin daha fazla bilgi için bkz. “Nesnelere erişim yetkisi verme” sayfa 335.

Sınırlı bir tanıtıcıya sahip belirli bir kanala bağlanmak için bir istemci uygulaması ayarladıysanız, ancak kanal, MCAUSER alanında bir yönetici kimliği ayarlandıysa, istemci uygulaması başarıyla bağlandığında, erişim denetimi denetimlerinde yönetici kimliği kullanılır. Bu nedenle, istemci uygulamasının kuyruk yöneticinize tam erişim hakları olacaktır.

MCAUSER özniteliği hakkında daha fazla bilgi için bkz. “İstemci kullanıcı kimliğinin MCAUSER kullanıcı kimliğiyle eşlenmesi” sayfa 372.

Kanal doğrulama kuralları, bir bağlantının kabul edilmesi için belirli kurallar ve ölçütler belirleyerek, bir kuyruk yöneticisine erişimi denetlemeye yönelik bir yöntem olarak da kullanılabilir.

Kanal doğrulama kurallarına ilişkin daha fazla bilgi için bkz. “Kanal doğrulama kayıtları” sayfa 47.

MQI istemcisinde çalıştırma zamanında yalnızca FIPS onaylı CipherSpecs kullanılmasının belirtilmesi

FIPS uyumlu yazılımı kullanarak anahtar havuzlarınızı oluşturun ve daha sonra, kanalın FIPS onaylı CipherSpecsözelliğini kullanması gerektiğini belirtin.

Çalıştırma zamanında FIPS uyumlu olabilmek için, anahtar havuzlarının yalnızca -fips seçeneğiyle runmqakm gibi FIPS uyumlu yazılımlar kullanılarak oluşturulmuş ve yönetilmiş olması gerekir.

TLS kanalının yalnızca FIPS onaylı CipherSpecs özelliğini öncelik sırasına göre listelenmiş üç şekilde kullanması gerektiğini belirtebilirsiniz:

1. MQSCO yapısındaki FipsRequired alanını MQSSL_FIPS_YES olarak ayarlayın.
2. MQSSLFIPS ortam değişkenini YES olarak ayarlayın.
3. İstemci yapılanış dosyasındaki SSLFipsRequired özniteliğini YES değerine ayarlayın.

Varsayılan olarak, FIPS onaylı CipherSpecs gerekmez.

Bu değerler, ALTER QMGR SSLFIPS ' deki eşdeğer parametre değerleriyle aynı anlamlara sahiptir (bkz. ALTER QMGR). İstemci işleminin etkin TLS bağlantısı yoksa ve SSL MQCONNX 'te geçerli bir FipsRequired değeri belirtildiyse, bu işlemle ilişkili sonraki tüm TLS bağlantıları yalnızca bu değerle ilişkilendirilmiş CipherSpecs kullanmalıdır. Bu, bu ve diğer tüm TLS bağlantıları duruncaya kadar geçerlidir; bu aşamada sonraki bir MQCONNX, FipsRequirediçin yeni bir değer sağlayabilir.

Şifreleme donanımı varsa, IBM MQ tarafından kullanılan şifreleme modülleri donanım ürünü tarafından sağlanan modüller olacak şekilde yapılandırılabilir ve bunlar belirli bir düzeyde FIPS onaylı olabilir. Yapılandırılabilir modüller ve bunların FIPS onaylı olup olmamaları, kullanılmakta olan donanım ürününe bağlıdır.

Mümkünse, FIPS-only CipherSpecs yapılandırılırsa, MQI istemcisi MQRC_SSL_INITIALIZATION_ERROR ile FIPS CipherSpec dışı bir CipherSpec belirten bağlantıları reddeder. IBM MQ , bu tür bağlantıların tümünü reddetmeyi garanti etmez ve IBM MQ yapılandırmanızın FIPS uyumlu olup olmadığını belirlemek sizin sorumluluğunuzdadır.

İlgili kavramlar

“UNIX, Linux, and Windows için Federal Bilgi İşleme Standartları (FIPS)” sayfa 32
Windows, UNIX and Linux sistemlerinde bir SSL/TLS kanalında şifreleme gerektiğinde IBM MQ , IBM Crypto for C (ICC) adlı bir şifreleme paketi kullanır. Windows, UNIX and Linux platformlarında, ICC yazılımı, ABD Ulusal Standartlar ve Teknoloji Enstitüsü 'nün Federal Bilgi İşleme Standartları (FIPS) Şifreleme Modülü Doğrulama Programı 'nı 140-2 düzeyinde geçmiştir.

İstemci yapılanış kütüğünün SSL kısmı

İlgili başvurular

FipsRequired (MQLONG)
MQSSLFIPS

AIX Running TLS client applications with multiple installations of GSKit V8.0 on AIX

TLS client applications on AIX might experience MQRC_CHANNEL_CONFIG_ERROR and error AMQ6175 when running on AIX systems with multiple GSKit V8.0 installations.

Birden çok GSKit V8.0 kurulumu içeren bir AIX sisteminde istemci uygulamaları çalıştırırken, istemci bağlanma çağrıları TLS kullanılırken MQRC_CHANNEL_CONFIG_ERROR değerini döndürebilir. The /var/mqm/errors logs record error AMQ6175 and AMQ9220 for the failing client application, for example:

```
09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
Host(machine.example.ibm.com) Installation(Installation1)
VRMF(7.1.0.0)
AMQ6175: The system could not dynamically load the shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so'. The system returned
error number '8' and error message 'Symbol resolution failed
for /usr/mqm/gskit8/lib64/libgsk8ssl_64.so because:
Symbol VALUE_EC_NamedCurve_secp256r1__9GSKASNOID (number 16) is not
exported from dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_NamedCurve_secp384r1__9GSKASNOID (number 17) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_NamedCurve_secp521r1__9GSKASNOID (number 18) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecPublicKey__9GSKASNOID (number 19) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecdsa_with_SHA1__9GSKASNOID (number 20) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
Symbol VALUE_EC_ecdsa__9GSKASNOID (number 21) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.'.

EXPLANATION:
This message applies to AIX systems. The shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed
to load correctly due to a problem with the library.
ACTION:
Check the file access permissions and that the file has not been corrupted.
----- amqxufnx.c : 1284 ---------------------------------------------------------
09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
Host(machine.example.ibm.com) Installation(Installation1)
VRMF(7.1.0.0)
AMQ9220: The GSKit communications program could not be loaded.

EXPLANATION:
The attempt to load the GSKit library or procedure
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed with error code
536895861.
ACTION:
Either the library must be installed on the system or the environment changed
to allow the program to locate it.
----- amqcgska.c : 836 ----------------------------------------------------------
```

Bu hatanın yaygın bir nedeni, LIBPATH ya da LD_LIBRARY_PATH ortam değişkeninin ayarının, IBM MQ istemcisinin iki farklı GSKit V8.0 kuruluşundan karışık bir kitaplık kümesi yüklemesine neden olmuştur. Db2 ortamında bir IBM MQ istemcisi uygulamasının yürütülmesi bu hataya neden olabilir.

Bu hatayı önlemek için, kitaplık yolunun önüne IBM MQ kitaplık dizinlerini ekleyin; böylece, IBM MQ kitaplıklarının önceliği olur. Bu, **-k** parametresiyle **setmqenv** komutu kullanılarak elde edilebilir; örneğin:

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

setmqenv komutunun kullanımı hakkında daha fazla bilgi için bkz. setmqenv (IBM MQ ortamını ayarla)

IBM i IBM iüzerinde SSL ya da TLS için iletişimi ayarlama

SSL ya da TLS şifreleme güvenlik iletişim kurallarını kullanan güvenli iletişim, iletişim kanallarının ayarlanmasını ve kimlik doğrulaması için kullanacağınız dijital sertifikaların yönetilmesini içerir.

SSL ya da TLS kuruluşunuzu ayarlamak için kanallarınızı SSL ya da TLS kullanacak şekilde tanımlamanız gerekir. Ayrıca, dijital sertifikalarınızı da oluşturmanız ve yönetmeniz gerekir. Bazı işletim sistemlerinde, sınamaları kendinden imzalı sertifikalarla gerçekleştirebilirsiniz. Ancak, IBM iüzerinde, yerel bir CA tarafından imzalanmış kişisel sertifikalar kullanmanız gerekir.

Sertifikaları oluşturma ve yönetme hakkında tam bilgi için bkz. “IBM iüzerinde SSL/TLS ile çalışma” sayfa 262.

Bu konular grubu, SSL ya da TLS iletişiminin ayarlanmasında yer alan bazı görevleri tanıtır ve bu görevlerin tamamlanmasına ilişkin adım adım yönergeler sağlar.

SSL ve TLS iletişim kurallarının isteğe bağlı kısımlarından oluşan SSL ya da TLS istemcisi kimlik doğrulamasını sınamak da isteyebilirsiniz. SSL ya da TLS anlaşması sırasında, SSL ya da TLS istemcisi

her zaman, sunucudan sayısal bir sertifika alır ve sayısal bir sertifikayı doğrular. IBM MQ uygulaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

IBM iüzerinde, SSL ya da TLS istemcisi yalnızca, doğru IBM MQ biçiminde bir etiketi varsa sertifika gönderir:

- Kuyruk yöneticisi için `ibmwebspheremq` , ardından kuyruk yöneticinizin adı küçük harfe çevrilerek değiştirildi. Örneğin, `QM1`için, `ibmwebspheremqqm1`.
- For an IBM MQ C Client for IBM i, `ibmwebspheremq` followed by your logon user ID changed to lowercase, for example `ibmwebspheremqmyuserid`.

IBM MQ , diğer ürünlere ilişkin sertifikalar ile karışıklığı önlemek için bir etikette `ibmwebspheremq` önekini kullanır. Sertifika etiketinin tamamını küçük harfli olarak belirtmeye dikkat edin.

SSL ya da TLS sunucusu, gönderildiyse istemci sertifikasının her zaman geçerliliğini denetler. SSL ya da TLS istemcisi bir sertifika göndermezse, kimlik doğrulaması yalnızca, SSL ya da TLS sunucusu olarak hareket eden kanal sonu, SSLCAUTH parametresiyle ya da REQUIRD ya da SSLPEER parametre değeri ayarında tanımlandıysa başarısız olur. Daha fazla bilgi için SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanmasıbaşlıklı konuya bakın.

ULW Setting up communications for SSL or TLS on UNIX, Linux or Windows

SSL ya da TLS şifreleme güvenlik iletişim kurallarını kullanan güvenli iletişim, iletişim kanallarının ayarlanmasını ve kimlik doğrulaması için kullanacağınız dijital sertifikaların yönetilmesini içerir.

SSL ya da TLS kuruluşunuzu ayarlamak için kanallarınızı SSL ya da TLS kullanacak şekilde tanımlamanız gerekir. Ayrıca, dijital sertifikalarınızı da oluşturmanız ve yönetmeniz gerekir. UNIX, Linux ve Windows sistemlerinde, kendinden imzalı sertifikalarla ilgili testleri gerçekleştirebilirsiniz.

Uyarı: TLS etkin kanallarını kullanarak birleştirmek istediğiniz kuyruk yöneticilerindeki Eliptik Eğri imzalı sertifikaların ve RSA imzalı sertifikaların bir karışımının kullanılması olanaklı değildir.

TLS etkin kanallarını kullanan kuyruk yöneticilerinin tümü RSA imzalı sertifikalar kullanmalı ya da her ikisinin bir karışımının değil, tüm EC imzalı sertifikalarını kullanmalıdır.

Ek bilgi için “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42 başlıklı konuya bakın.

Kendinden onaylı sertifikalar iptal edilemez; bu, bir saldırganın özel bir anahtarın gizliliğinin ihlal edilmesinden sonra bir kimliği bozmasına olanak verebilir. CU ' lar ihlal edilen bir sertifikayı iptal edebilir, bu da daha fazla kullanım yapılmasını önleyebilir. Bu nedenle, kendi kendine imzalanmış sertifikalar bir test sistemi için daha uygun olsa da, CA imzalı sertifikalar üretim ortamında kullanılmak üzere daha güvenli olur.

Sertifikaları oluşturma ve yönetme hakkında tam bilgi için bkz. “UNIX, Linux, and Windowsüzerinde SSL/TLS ile çalışma” sayfa 273.

Bu konular grubu, SSL iletişimini ayarlarken yer alan bazı görevleri tanıtır ve bu görevlerin tamamlanmasına ilişkin adım adım yönergeler sağlar.

Ayrıca, protokollerin isteğe bağlı bir parçası olan SSL ya da TLS istemcisi kimlik doğrulamasını sınamak da isteyebilirsiniz. SSL ya da TLS anlaşması sırasında, SSL ya da TLS istemcisi her zaman, sunucudan sayısal bir sertifika alır ve sayısal bir sertifikayı doğrular. IBM MQ uygulaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

UNIX, Linux, and Windowsüzerinde, SSL ya da TLS istemcisi yalnızca, doğru IBM MQ biçiminde bir etiketi varsa sertifika gönderir:

- Kuyruk yöneticisi için, biçim şöyledir: `ibmwebspheremq` , ardından kuyruk yöneticinizin adı küçük harfe çevrilir. Örneğin, `QM1`için, `ibmwebspheremqqm1`
- Bir IBM MQ istemcisi için `ibmwebspheremq` , ardından oturum açma kullanıcı kimliğiniz küçük harfe çevrilerek değiştirildi; örneğin, `ibmwebspheremqmyuserid`.

IBM MQ , diğer ürünlere ilişkin sertifikalar ile karışıklığı önlemek için bir etikette `ibmwebspheremq` önekini kullanır. Sertifika etiketinin tamamını küçük harfli olarak belirtmeye dikkat edin.

SSL ya da TLS sunucusu, gönderildiyse istemci sertifikasının her zaman geçerliliğini denetler. İstemci bir sertifika göndermezse, kimlik doğrulaması yalnızca, SSL ya da TLS sunucusu olarak hareket eden kanal sonu, REQUIRENLY ya da SSLPEER parametre değer kümesi için ayarlanmış SSLCAUTH parametresiyle tanımlandıysa başarısız olur. Daha fazla bilgi için SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanmasıbaşlıklı konuya bakın.

z/OSz/OSüzerinde SSL ya da TLS için iletişimi ayarlama

SSL ya da TLS şifreleme güvenlik iletişim kurallarını kullanan güvenli iletişim, iletişim kanallarının ayarlanmasını ve kimlik doğrulaması için kullanacağınız dijital sertifikaların yönetilmesini içerir.

SSL ya da TLS kuruluşunuzu ayarlamak için kanallarınızı SSL ya da TLS kullanacak şekilde tanımlamanız gerekir. Ayrıca, dijital sertifikalarınızı da oluşturmanız ve yönetmeniz gerekir. z/OS ' ta sınamaları kendinden onaylı sertifikalarla ya da yerel bir sertifika yetkilisi (CA) tarafından imzalanmış kişisel sertifikalarla gerçekleştirebilirsiniz.

Kendinden onaylı sertifikalar iptal edilemez; bu, bir saldırganın özel bir anahtarın gizliliğinin ihlal edilmesinden sonra bir kimliği bozmasına olanak verebilir. CU ' lar ihlal edilen bir sertifikayı iptal edebilir, bu da daha fazla kullanım yapılmasını önleyebilir. Bu nedenle, kendi kendine imzalanmış sertifikalar bir test sistemi için daha uygun olsa da, CA imzalı sertifikalar üretim ortamında kullanılmak üzere daha güvenli olur.

Sertifikaları oluşturma ve yönetme hakkında tam bilgi için bkz. “z/OSüzerinde SSL/TLS ile çalışma” sayfa 304.

Bu konu grubunda, SSL ya da TLS iletişimini ayarlarken yer alan bazı görevler tanıtılır ve bu görevlerin tamamlanmasına ilişkin adım adım yönergeler sağlanır.

Ayrıca, protokollerin isteğe bağlı bir parçası olan SSL ya da TLS istemcisi kimlik doğrulamasını sınamak da isteyebilirsiniz. SSL ya da TLS anlaşması sırasında, SSL ya da TLS istemcisi her zaman, sunucudan sayısal bir sertifika alır ve sayısal bir sertifikayı doğrular. IBM MQ uygulaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

On z/OS the SSL or TLS client sends a certificate only if it has one of the following certificates:

- Yalnızca paylaşılan bir kanal için, `ibmWebSphereMQ` biçiminde bir etiket ve ardından kuyruk paylaşım grubunuzun adı (örneğin, `ibmWebSphereMQQSG1`) olan bir sertifika.
- A certificate with a label in the format`ibmWebSphereMQ` followed by the name of your queue manager, for example `ibmWebSphereMQQM1`
- Varsayılan bir sertifika (`ibmWebSphereMQ` sertifikası olabilir).

Kanal paylaşılıyorsa, kanal ilk olarak kuyruk paylaşım grubu için bir sertifika bulmaya çalışır. Kuyruk paylaşım grubu için bir sertifika bulamazsa, kuyruk yöneticisi için bir sertifika bulmaya çalışır.

z/OSüzerinde, IBM MQ diğer ürünlerin sertifikalarıyla karışıklığı önlemek için bir etikette `ibmWebSphereMQ` önekini kullanır.

SSL ya da TLS sunucusu, gönderildiyse istemci sertifikasının her zaman geçerliliğini denetler. SSL ya da TLS istemcisi bir sertifika göndermezse, kimlik doğrulaması yalnızca, SSL ya da TLS sunucusu olarak hareket eden kanal sonu, SSLCAUTH parametresiyle ya da REQUIRD ya da SSLPEER parametre değeri ayarında tanımlandıysa başarısız olur. Daha fazla bilgi için SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanmasıbaşlıklı konuya bakın.

SSL/TLS ile çalışma

These topics give instructions for performing single tasks related to using TLS with IBM MQ.

Bunlardan çoğu, aşağıdaki bölümlerde açıklanan üst düzey görevlerde adım olarak kullanılır:

- “Kullanıcıların tanımlanması ve kimlik doğrulaması” sayfa 316

- “Nesnelere erişim yetkisi verme” sayfa 335
- “İletilerin gizliliği” sayfa 402
- “İletilerin veri bütünlüğü” sayfa 439
- “Kümeleri güvenli tutma” sayfa 440

IBM i IBM iüzerinde SSL/TLS ile çalışma

Bu konu derlemi, IBM MQ for IBM iiçinde TLS (Transport Layer Security; İletim Katmanı Güvenliği) ile çalışan her bir göreve ilişkin yönergeleri içerir.

IBM i için TLS desteği, işletim sisteminin ayrılmaz bir parçasıdır. Hardware and software requiress on IBM i(Donanım ve yazılım gereksinimleri) altında listelenen önkoşulları yüklediğinizden emin olun.

IBM i' ta, anahtarları ve dijital sertifikaları Digital Certificate Manager (DCM) aracı ile yönetir.

DCM Olanağına Erişilmesi

DCM arabirimine erişmek için bu yönergeleri izleyin.

Bu görev hakkında

Çerçeveleri destekleyen bir web tarayıcısında aşağıdaki adımları gerçekleştirin.

Yordam

1. `http://`*`machine`*`.domain:2001` ya da `https://`*`machine`*`.domain:2010`değerine gidin; burada *makine* , bilgisayarınızın adıdır.
2. İstendiğinde geçerli bir kullanıcı tanıtımı ve parola yazın.

   Yeni sertifika depoları yaratmanıza olanak sağlamak için kullanıcı tanıtımınızın *ALLOBJ ve *SECADM özel yetkilerine sahip olduğundan emin olun. Özel yetkileriniz yoksa, yalnızca kişisel sertifikalarınızı yönetebilir ya da yetkili olduğunuz nesneler için nesne imzalarını görüntüleyebilirsiniz. Bir nesne imzalama uygulaması kullanma yetkiniz varsa, nesneleri DCM ' den de imzalayabilirsiniz.
3. Internet Yapılandırmaları sayfasında **Dijital Certificate Manager**simgesini tıklatın.

   Digital Certificate Manager (Sertifika Yöneticisi) sayfası görüntülenir.

IBM i' ta bir kuyruk yöneticisine sertifika atama

Bir sertifika kuyruk yöneticisine bir sertifika atamak için DCM ' yi kullanın.

Bir sertifika kuyruk yöneticisine sertifika atamak için geleneksel IBM i dijital sertifika yönetimini kullanın. Bu, bir kuyruk yöneticisinin sistem sertifika deposunu kullandığını ve kuyruk yöneticisinin Digital Certificate Managerile uygulama olarak kullanılmak üzere kaydedildiğini belirtebileceğiniz anlamına gelir. Bunu yapmak için, kuyruk yöneticisi **SSLKEYR** özniteliğinin değerini *SYSTEMolarak değiştirin.

SSLKEYR parametresi *SYSTEMolarak değiştirildiğinde, IBM MQ kuyruk yöneticisini, QIBM_WEBSPHERE_MQ_QMGRNAME benzersiz uygulama etiketine sahip bir sunucu uygulaması olarak kaydeder ve Qmgrname (WMQ) açıklamasını içeren bir etiket olarak kaydeder. *SYSTEM sertifika deposunu kullanıyorsanız, kanal **CERTLABL** özniteliklerinin kullanılmadığını göz önünde bulundurun. Daha sonra, kuyruk yöneticisi, Digital Certificate Manager' da sunucu uygulaması olarak görünür ve bu uygulamaya, sistem deposunda herhangi bir sunucu ya da istemci sertifikası atayabilirsiniz.

Kuyruk yöneticisi bir uygulama olarak kayıtlı olduğundan, CA güvenilirlik listelerini tanımlama gibi, DCM ' nin gelişmiş özellikleri gerçekleştirilebilir.

SSLKEYR parametresi *SYSTEMdışında bir değer olarak değiştirilirse, IBM MQ , kuyruk yöneticisini Digital Certificate Manager' ın bulunduğu bir uygulama olarak kayıttan kaldırır. Bir kuyruk yöneticisi silinirse, DCM ' den de kayıt derli kaldırılır. Yeterli *SECADM yetkisi olan bir kullanıcı, DCM ' den uygulamaları el ile ekleyebilir ya da kaldırabilir.

IBM iüzerinde bir anahtar havuzu ayarlanıyor

Bağlantının her iki ucunda da bir anahtar havuzu ayarlamanız gerekir. Varsayılan sertifika depoları kullanılabilir ya da kendi kendinize ait bir sertifika yaratabilirsiniz.

TLS bağlantısı, bağlantının her iki ucunda bir *anahtar havuzu* gerektirir. Her kuyruk yöneticisinin ve IBM MQ MQI client ' in bir anahtar havuzuna erişimi olması gerekir. Anahtar havuzuna bir dosya adı ve parola kullanarak erişmek istiyorsanız (*SYSTEM seçeneğini kullanmayacaksa), QMQM kullanıcı tanıtımının aşağıdaki yetkiler olduğundan emin olun:

- Anahtar havuzunu içeren dizin için yürütme yetkisi
- Anahtar havuzu içeren dosyaya ilişkin okuma yetkinizin

Ek bilgi için "SSL/TLS anahtarı havuzu" sayfa 23 başlıklı konuya bakın. Note that channel **CERTLABL** attributes are not used if you use the *SYSTEM certificate store.

IBM iüzerinde, dijital sertifikalar DCM ile yönetilen bir sertifika deposuyla depolanır. Bu sayısal sertifikalar, bir sertifikayı kuyruk yöneticisi ya da IBM MQ MQI clientile ilişkilendiren etiketlere sahiptir. TLS, kimlik doğrulama amacıyla sertifikaları kullanır.

The label is either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or IBM MQ MQI client user logon ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

Kuyruk yöneticisi ya da IBM MQ MQI client sertifika deposu adı bir yol ve kök adını içerir. Varsayılan yol `/QIBM/UserData/ICSS/Cert/Server/` ve varsayılan kök adı `Default`' dir. IBM iüzerinde, varsayılan sertifika deposu (`/QIBM/UserData/ICSS/Cert/Server/Default.kdb`), `*SYSTEM`olarak da bilinir. İsteğe bağlı olarak, kendi yol ve kök adınızı tanımlayabilirsiniz.

Kendi yol ya da dosya adınızı tanımlarsanız, bu dosyaya erişimi sıkı bir şekilde denetlemek için izinleri dosya olarak ayarlayın.

"IBM iüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzu yerinin değiştirilmesi" sayfa 264 , size sertifika deposu adını belirtme hakkında bilgi verir. Sertifika deposunu yaratmadan önce ya da sonra sertifika deposu adını belirtebilirsiniz.

Not: DCM ile gerçekleştirebileceğiniz işlemler, kullanıcı tanıtımınızın yetkisiyle sınırlı olabilir. Örneğin, bir CA sertifikası yaratmak için *ALLOBJ ve *SECADM yetkileriniz gerekir.

IBM iüzerinde bir sertifika deposu oluşturma

Varsayılan sertifika deposunu kullanmak istemiyorsanız, bu mağazanızı kendiniz yaratmak için bu yordamı izleyin.

Bu görev hakkında

Yalnızca IBM i varsayılan sertifika deposunu kullanmak istemiyorsanız yeni bir sertifika deposu oluşturun.

IBM i sistem sertifika deposunun kullanılacağını belirtmek için, kuyruk yöneticisi SSLKEYR özniteliğinin değerini *SYSTEM olarak değiştirin. Bu değer, kuyruk yöneticisinin sistem sertifika deposunu kullandığını ve kuyruk yöneticisinin Digital Certificate Manager (DCM) ile bir uygulama olarak kullanılmak üzere kaydedildiğini belirtir.

Yordam

1. Access the DCM interface, as described in "DCM Olanağına Erişilmesi" sayfa 262
2. Gezinme panosunda **Create New Certificate Store**(Yeni Sertifika Deposu Oluştur) seçeneğini tıklatın. Yeni Sertifika Deposu Yarat sayfası görev çerçevesinde görüntülenir.
3. Görev çerçevesinde, **Other System Certificate Store** ' ı seçin ve **Continue**(Devam) seçeneğini tıklatın. Yeni Sertifika Deposu sayfasında bir Sertifika Yarat sayfası, görev çerçevesinde görüntülenir.
4. **Hayır-Sertifika deposunda sertifika yaratmayın** seçeneğini belirleyin ve **Devam**düğmesini tıklatın. Sertifika Deposu Adı ve Parola sayfası görev çerçevesinde görüntülenir.

5. **Sertifika deposu yolu ve dosya adı** alanında bir IFS yolu ve dosya adı yazın; örneğin, `/QIBM/UserData/mqm/qmgrs/qm1/key.kdb`
6. **Parola** alanına bir parola yazın ve **Parolayı Onayla** alanına parolayı yeniden yazın. **Devam**düğmesini tıklatın.

   Havuz anahtarını sakladığınızda gereken parolayı (büyük/küçük harfe duyarlı) not edin.
7. DCM ' den çıkmak için, tarayıcı pencerenizi kapatın.

Sonraki adım

When you have created the certificate store using DCM, ensure you stash the password, as described in “Stashing the certificate store password on IBM i systems” sayfa 264

İlgili görevler

“Importing a certificate into a key repository on IBM i” sayfa 269
Bir sertifikayı içe aktarmak için bu yordamı izleyin.

Stashing the certificate store password on IBM i systems
CL komutlarını kullanarak sertifika deposu parolasını saklar.

The following instructions apply to stashing the certificate store password on IBM i for a queue manager. Diğer bir seçenek olarak, bir IBM MQ MQI clientiçin, *SYSTEM sertifika deposunu kullanmıyorsa (yani, MQSSLKEYR ortamı *SYSTEM dışında bir değere ayarlanmışsa), “IBM iiçinIBM MQ SSL Client yardımcı programı (amqrsslc)” sayfa 271' un “Sertifika deposu parolasını saklar” sayfa 272 kısmında açıklanan yordamı izleyin.

*SYSTEM sertifika deposunun kullanılacağını belirtdiyseniz (kuyruk yöneticisinin SSLKEYR özniteliğinin değerini *SYSTEM olarak değiştirerek) bu adımları izlememeniz gerekir.

DCM kullanarak sertifika deposunu yarattığınız zaman, parolayı saklamak için aşağıdaki komutları kullanın:

```
STRMQM MQMNAME('queue_manager_name')
CHGMQM MQMNAME('queue_manager_name') SSLKEYRPWD('password')
```

Parola, büyük ve küçük harfe duyarlıdır. “IBM iüzerinde bir sertifika deposu oluşturma” sayfa 263' un 6. adımında girdiğinizde tam olarak tek tırnak içine girilmiş olmalıdır.

Not: Varsayılan sistem sertifika deposunu kullanmıyorsanız ve parolayı saklamadıysanız, sertifika deposuna erişmek için gereken parolayı alamayacakları için TLS kanallarını başlatma girişimleri başarısız olur.

IBM iüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzunun bulunması

Kuyruk yöneticinizin sertifika deposunun yerini almak için bu yordamı kullanın.

Yordam

1. Aşağıdaki komutu kullanarak kuyruk yöneticinizin özniteliklerini görüntüleyin:

   ```
   DSPMQM MQMNAME('queue manager name')
   ```
2. Sertifika deposunun yolu ve kök adı için komut çıkışını inceleyin.

   Örneğin: `/QIBM/UserData/ICSS/Cert/Server/Default`; burada `/QIBM/UserData/ICSS/Cert/Server` yol, `Default` ise kök adıdır.

IBM iüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzu yerinin değiştirilmesi

CHGMQM ya da ALTER QMGR kullanarak kuyruk yöneticinizin sertifika deposunun yerini değiştirin.

Yordam

Kuyruk yöneticinizin anahtar havuzu özniteliğini ayarlamak için, CHGMQM komutunu ya da ALTER QMGR MQSC komutunu kullanın.

a) CHGMQM kullanılıyor: `CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

b) ALTER QMGR kullanılıyor: `ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

Her iki durumda da, sertifika deposunun tam olarak nitelenmiş dosya adı vardır: `/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb`

Sonraki adım

Bir kuyruk yöneticisinin sertifika deposunun konumunu değiştirdiğinizde, sertifikalar eski konumdan aktarılmaz. If the CA certificates preinstalled when you create the certificate store are insufficient, you must populate the new certificate store with certificates, as described in "Importing a certificate into a key repository on IBM i" sayfa 269. Ayrıca, "Stashing the certificate store password on IBM i systems" sayfa 264içinde açıklandığı gibi, yeni konuma ilişkin parolayı da saklamanız gerekir.

IBM i' ta test için bir sertifika yetkilisi ve sertifika oluşturma

Sertifika isteklerini imzalamak ve CA sertifikasını yaratmak ve kurmak için yerel bir CA sertifikası oluşturmak için bu yordamı kullanın.

Başlamadan önce

Bu konudaki yönergelerde, yerel bir sertifika yetkilinin (CA) var olmadığı varsayılmıştır. Yerel bir sertifika kuruluşu (CA) varsa, "IBM iüzerinde bir sunucu sertifikası istenmesi" sayfa 266' a gidin.

Bu görev hakkında

TLS ' yi kurduğunuzda sağlanan CA sertifikaları, sertifika veren CA tarafından imzalanır. IBM i' ta, sisteminizdeki TLS iletişimlerini test etmek için sunucu sertifikalarını imzalayabilen yerel bir sertifika yetkilisi oluşturabilirsiniz. Yerel bir CA sertifikası yaratmak için bir Web tarayıcısında aşağıdaki adımları izleyin:

Yordam

1. Access the DCM interface, as described in "DCM Olanağına Erişilmesi" sayfa 262.
2. Gezinme panosunda **Create a Certificate Authority**(Sertifika Yetkilisi Oluştur) seçeneğini tıklatın.
   Bir Sertifika Yetkilisi Yarat sayfası, görev çerçevesinde görüntülenir.
3. **Sertifika deposu parolası** alanına bir parola yazın ve **Parolayı doğrulayın** alanına parolayı yeniden yazın.
4. **Sertifika Yetkilisi (CA) adı** alanında bir ad yazın (örneğin, `TLS Test Certificate Authority`).
5. **Ortak Ad** ve **Kuruluş** alanlarına uygun değerleri yazın ve bir ülke seçin. Kalan isteğe bağlı alanlar için, gereksinim duyduğunuz değerleri yazın.
6. **Geçerlilik süresi** alanında yerel sertifika kuruluşu (CA) için bir geçerlilik dönemi yazın.
   Varsayılan değer 1095 gündür.
7. **Devam**düğmesini tıklatın.
   CA yaratılır ve DCM, yerel CA ' niz için bir sertifika deposu ve CA sertifikası yaratır.
8. **Sertifika kur**seçeneğini tıklatın.
   Karşıdan yükleme yöneticisi iletişim kutusu görüntülenir.
9. CA sertifikasını saklamak istediğiniz geçici dosyanın tam yol adını yazın ve **Sakla**düğmesini tıklatın.
10. Karşıdan yükleme işlemi tamamlandığında **Aç**düğmesini tıklatın.
    Sertifika penceresi görüntülenir.
11. **Sertifika kur**seçeneğini tıklatın.

Sertifika İçe Aktarma sihirbazı görüntülenir.

12. **İleri**'yi tıklatın.
13. **Sertifika tipine dayalı olarak otomatik olarak sertifika deposunu seç** seçeneğini belirleyin ve **İleri**düğmesini tıklatın.
14. **Bitir**'i tıklatın.

    Bir doğrulama penceresi görüntülenir.
15. **Tamam**'ı tıklatın.
16. Sertifika penceresinde **Tamam**düğmesini tıklatın.
17. **Devam**düğmesini tıklatın.

    Sertifika Yetkilisi İlkesi sayfası görev çerçevesinde görüntülenir.
18. **Kullanıcı sertifikalarının oluşturulmasına izin ver** alanında **Evet**seçeneğini belirleyin.
19. **Geçerlilik dönemi** alanında, yerel CA ' niz tarafından yayınlanan sertifikaların geçerlilik süresini yazın.

    Varsayılan değer 365 gündür.
20. **Devam**düğmesini tıklatın.

    Yeni Sertifika Deposu sayfasında bir Sertifika Yarat sayfası, görev çerçevesinde görüntülenir.
21. Uygulamaların hiçbirinin seçilmediğini kontrol edin.
22. Yerel CA ' nın kuruluşunu tamamlamak için **Continue** (Devam) seçeneğini tıklatın.

IBM iüzerinde bir sunucu sertifikası istenmesi

Dijital sertifikalar, bir genel anahtarın belirtilen bir varlığa ait olduğunu onaylayan kişileştirmeye karşı koruma sağlar. Digital Certificate Manager (DCM) olanağını kullanarak sertifika yetkilisinden yeni bir sunucu sertifikası istenebilir.

Bu görev hakkında

Bir Web tarayıcısında aşağıdaki adımları gerçekleştirin:

Yordam

1. Access the DCM interface, as described in “DCM Olanağına Erişilmesi” sayfa 262.
2. Gezinme panosunda, **Select a Certificate Store**(Sertifika Deposu Seç) seçeneğini tıklatın.

   Bir Sertifika Deposu Seç sayfası, görev çerçevesinde görüntülenir.
3. Kullanmak istediğiniz sertifika deposunu seçin ve **Continue**(Devam) seçeneğini tıklatın.
4. İsteğe bağlı: 3. adımda ***SYSTEM** seçeneğini belirlediyseniz, sistem deposu parolasını girin ve **Continue**(Devam) seçeneğini tıklatın.
5. İsteğe bağlı: 3. adımda **Diğer Sistem Sertifikası Deposu** ' u seçtiyseniz, **Sertifika deposu yolu ve dosya adı** alanında, sertifika deponanızı yaratırken ayarladığınız IFS yolunu ve dosya adını yazın. Ayrıca, **Sertifika Deposu Parolası** alanına bir parola yazın. **Devam**düğmesini tıklatın.
6. Gezinme panosunda **Create Certificate**(Sertifika Oluştur) seçeneğini tıklatın.
7. Görev çerçevesinde, **Sunucu ya da istemci sertifikası** radyo düğmesini seçin ve **Devam**düğmesini tıklatın.

   Görev çerçevesinde bir Sertifika Yetkilisi Seç (CA) sayfası görüntülenir.
8. İş istasyonunuzda yerel bir sertifika kuruluşu (CA) varsa, sertifikayı imzalamak için yerel CA 'yı ya da ticari bir CA' yı seçmiş olun. İstediğiniz CA ' ya ilişkin radyo düğmesini seçin ve **Devam**düğmesini tıklatın.

   Bir Sertifika Yarat sayfası, görev çerçevesinde görüntülenir.
9. İsteğe bağlı: Kuyruk yöneticisi için, **Sertifika etiketi** alanında sertifika etiketini girin.

   Etiket, **CERTLABL** özniteliğinin değeri ya da ayarlandıysa, ya da sonuna kuyruk yöneticisi adı eklenmiş olarak varsayılan `ibmwebspheremq` olanlowercaseöznitelığinin küçük harflerinden biri olur. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

   Örneğin, kuyruk yöneticisi QM1için, varsayılan değeri kullanmak için `ibmwebspheremqqm1` yazın.

10. İsteğe bağlı: Bir IBM MQ MQI clientiçin, **Sertifika etiketi** alanında, oturum açma kullanıcı kimliğinizin ardından `ibmwebspheremq` yazın ve ardından küçük harfe bakın.
    Örneğin, şunları yazın `ibmwebspheremqmyuserID`
11. **Ortak Ad** ve **Kuruluş** alanlarına uygun değerleri yazın ve bir ülke seçin. Kalan isteğe bağlı alanlar için, gereksinim duyduğunuz değerleri yazın.

Sonuçlar

Sertifikanızı imzalamak için bir ticari sertifika kuruluşu seçtiyseniz DCM, PEM (Privacy-Enhanced Mail) biçiminde bir sertifika isteği yaratır. İsteğinizi seçtiğiniz CA ' ya iletin.

Sertifikanızı imzalamak için yerel CA ' yı seçtiyseniz DCM, sertifikanız sertifika deposunda yaratıldığını ve kullanılabileceğini bildirir.

IBM iüzerinde IBM Key Manager için sunucu sertifikası istenmesi

Yerel sertifika yetkiliniz (CA) tarafından imzalanmış bir sertifika yaratmak ya da IBM Key Management (iKeyman) yardımcı programına aktarmak üzere bir ticari CA tarafından imzalanmış bir sunucu sertifikasına başvurmak için bu yordamı izleyin.

Bu görev hakkında

Bir kullanıcı sertifikası, Digital Certificate Manager (DCM), birden çok altyapıda IBM MQ için sertifika yöneticisi olarak hizmet verdiğinde kullanılmalıdır. Diğer platformlara dağıtılan kişisel sertifikalar için ve iKeyman yardımcı programına aktarmak için bir Web tarayıcısında aşağıdaki adımları gerçekleştirin:

Yordam

1. Access the DCM interface, as described in “DCM Olanağına Erişilmesi” sayfa 262.
2. **Gezinme** bölmesinde **Sertifika Oluştur**seçeneğini tıklatın.
   Görev çerçevesinde **Sertifika Oluştur** sayfası görüntülenir.
3. **Sertifika Oluştur** panosunda, **Kullanıcı sertifikası** radyo düğmesini seçin ve **Devam**düğmesini tıklatın.
   Kullanıcı Sertifikası Yarat sayfası görüntülenir.
4. **Kullanıcı Sertifikası Yarat** panosunda, **Kuruluş adı**, **Eyalet** ya da **il**, **Ülke** ya da **bölge**için Sertifika Bilgileri altında gerekli alanları doldurun. İsteğe bağlı olarak, değerleri **Kuruluş birimi** ve **Yerellik** ya da **şehir** alanlarına yerleştirin. **Devam**düğmesini tıklatın.
   Ortak ad otomatik olarak, iSeries sisteminde oturum açtığınız kullanıcı kimliğine ayarlanır.
5. Sonraki **Kullanıcı Sertifikası Oluştur** panosunda **Sertifikayı Kur** seçeneğini tıklatın ve **Devam**düğmesini tıklatın.
   `Kişisel sertifikanız kurulu olduğunu belirten bir ileti görüntülenir. Bu sertifikana ilişkin yedek bir kopyasını alıkoymak gerekir.`
6. **Tamam**'ı tıklatın.
7. DCM ' ye erişmek için kullandığınız Internet tarayıcısına bağlı olarak, aşağıdaki adımları gerçekleştirin:
   a) Microsoft Edge için şu seçenekleri belirleyin: **Araçlar > Internet Seçenekleri > İçerik sekmesi > Sertifikalar düğmesi > Kişisel sekmesi >**. Sertifikayı seçin ve **Dışa Aktar**düğmesini tıklatın.
   b) Mozilla Firefox için şu seçenekleri belirleyin: **Tools> Options > Advanced> Encryption tab > View Certificates button > your Certificates tab >**. Sertifikayı seçin ve **Yedekle**düğmesini tıklatın. Yolu ve dosya adını seçin ve **Tamam**düğmesini tıklatın.
8. Dışa aktarılan sertifikayı, ikili biçimde FTP kullanarak uzak sisteme aktarın.
9. Dışa aktarılan sertifikayı 7. adımdan anahtar veri tabanındaki iKeyman yardımcı programına ekleyin.
   a) Sertifika Microsoft Edge kullanılarak kaydedildiyse, Microsoft `.pfx` dosyasındanImportingİçe aktarmainbaşlıklı konu anlatımında belirtilen yönergeleri kullanın.
   b) Sertifika, Mozilla Firefox kullanılarak kaydedildiyse, Kişisel bir sertifikayı anahtar havuzuna almabaşlıklı konu için açıklanan yönergeleri kullanın.

İçe aktarma sırasında, kişisel sertifikana ilişkin etiket adının ve imzalayıcı sertifikasının IBM MQ ' in beklediği şekilde değiştirildiğinden emin olun. The label must be either the value of the IBM MQ **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

Sunucu sertifikalarının IBM iüzerindeki bir anahtar havuzuna eklenmesi

Anahtar havuzuna istenen bir sertifika eklemek için bu yordamı izleyin.

Bu görev hakkında

CA, size yeni bir sunucu sertifikası gönderdikten sonra, isteği oluşturduğunuz sertifika deposuna ekliyorsunuz. CA, sertifikayı bir e-posta iletisinin bir parçası olarak gönderirse, sertifikayı ayrı bir dosyaya kopyalayın.

Not:

- Sunucu sertifikası yerel CA ' niz tarafından imzalandıysa, bu yordamı gerçekleştirmeniz gerekmez.
- PKCS #12 biçiminde bir sunucu sertifikasını DCM ' ye aktarmadan önce, ilgili CA sertifikasını içe aktarmanız gerekir.

Kuyruk yöneticisi sertifika deposuna bir sunucu sertifikası almak için aşağıdaki yordamı kullanın:

Yordam

1. Access the DCM interface, as described in “DCM Olanağına Erişilmesi” sayfa 262.
2. Gezinme panosundaki **Sertifikaları Yönet** görev kategorisinde **Sertifikayı İçe Aktar**seçeneğini tıklatın.

   Görevi İçe Aktar sayfası görev çerçevesinde görüntülenir.
3. Sertifika tipinize ilişkin radyo düğmesini seçin ve **Devam**düğmesini tıklatın.

   İçe Aktarma Sunucusu ya da İstemci Sertifikası sayfası ya da Sertifika Yetkilisi (CA) Sertifikası (Import Certificate Authority) Sertifikası sayfası görev çerçevesinde görüntülenir.
4. **İçe Aktarma Dosyası** alanında, içe aktarmak istediğiniz sertifikana ilişkin dosya adını yazın ve **Devam**düğmesini tıklatın.

   DCM, dosyanın biçimini otomatik olarak belirler.
5. Sertifika bir **Sunucu ya da istemci** sertifikaysa, görev çerçevesine parolayı yazın ve **Devam**düğmesini tıklatın.

   DCM, sertifikenin içe aktarıldığını size bildirir.

IBM iüzerindeki bir anahtar havuzundan sertifika verme

Bir sertifikayı dışa aktarma, hem genel hem de özel anahtarı dışa aktarır. Bu eylem, özel bir anahtara geçtiğinden, sizin güvenliğinizden tamamen ödün vereceğine ilişkin aşırı uyarılarla birlikte alınmalıdır.

Başlamadan önce

Bir kullanıcının sertifikasını başka bir kullanıcıyla paylaştığınızda, genel anahtarları değiştirirdiniz. Bu işlem, **Görev 5 'te açıklanmaktadır. Quick Start Guide for AMS on UNIXiçindeSertifikaları Paylaşma** . Burada açıklandığı gibi bir sertifikayı dışa aktardığınızda, hem genel hem de özel anahtarı dışa aktarıyorsunuz. Bu eylem, özel bir anahtara geçtiğinden, sizin güvenliğinizden tamamen ödün vereceğine ilişkin aşırı uyarılarla birlikte alınmalıdır.

Bu görev hakkında

Sertifikayı dışa aktarmak istediğiniz bilgisayarda aşağıdaki adımları gerçekleştirin:

Yordam

1. Access the DCM interface, as described in “DCM Olanağına Erişilmesi” sayfa 262.
2. Gezinme panosunda, **Select a Certificate Store**(Sertifika Deposu Seç) seçeneğini tıklatın.

Bir Sertifika Deposu Seç sayfası, görev çerçevesinde görüntülenir.

3. Kullanmak istediğiniz sertifika deposunu seçin ve **Continue**(Devam) seçeneğini tıklatın.
4. İsteğe bağlı: 3. adımda ***SYSTEM** seçeneğini belirlediyseniz, sistem deposu parolasını girin ve **Continue**(Devam) seçeneğini tıklatın.
5. İsteğe bağlı: 3. adımda **Diğer Sistem Sertifikası Deposu** ' u seçtiyseniz, **Sertifika deposu yolu ve dosya adı** alanında, sertifika deponanızı yaratırken ayarladığınız IFS yolunu ve dosya adını yazın ve **Sertifika Deposu Parolası** alanına bir parola yazın. **Devam**düğmesini tıklatın.
6. Gezinme panosundaki **Sertifikaları Yönet** görev kategorisinde **Sertifikayı Dışa Aktar**seçeneğini tıklatın.

   Bir Sertifikayı Dışa Aktar sayfası, görev çerçevesinde görüntülenir.
7. Sertifika tipinize ilişkin radyo düğmesini seçin ve **Devam**düğmesini tıklatın.

   Görev çerçevesinde Dışa Aktarma Sunucusu ya da İstemci Sertifikası sayfası ya da Sertifika Yetkilisi (CA) Sertifikası Sertifikası sayfası görüntülenir.
8. Dışa aktarmak istediğiniz sertifikayı seçin.
9. Sertifikayı bir dosyaya ya da doğrudan başka bir sertifika deposuna dışa aktarmak isteyip istemediğinizi belirlemek için radyo düğmesini seçin.
10. Bir dosyayı ya da istemci sertifikasını bir dosyaya dışa aktarmayı seçtiyseniz, aşağıdaki bilgileri sağlayın:
    - Dışa aktarılan sertifikayı saklamak istediğiniz konumun yolu ve dosya adı.
    - Kişisel bir sertifika için, dışa aktarılan sertifikayı ve hedef yayın düzeyini şifrelemek için kullanılan parola. CA sertifikaları için parolayı belirtmenize gerek yoktur.
11. Bir sertifikayı doğrudan başka bir sertifika deposuna dışa aktarmak için seçtiyseniz, hedef sertifika deposunu ve parolasını belirtin.
12. **Devam**düğmesini tıklatın.

Importing a certificate into a key repository on IBM i

Bir sertifikayı içe aktarmak için bu yordamı izleyin.

Başlamadan önce

Kişisel bir sertifikayı PKCS #12 biçiminde DCM ' ye aktarmadan önce, ilgili CA sertifikasını içe aktarmanız gerekir.

Bu görev hakkında

Sertifikayı aktarmak istediğiniz makineden bu adımları gerçekleştirin.

Yordam

1. Access the DCM interface, as described in “DCM Olanağına Erişilmesi” sayfa 262.
2. Gezinme panosunda, **Select a Certificate Store**(Sertifika Deposu Seç) seçeneğini tıklatın.

   Bir Sertifika Deposu Seç sayfası, görev çerçevesinde görüntülenir.
3. Kullanmak istediğiniz sertifika deposunu seçin ve **Continue**(Devam) seçeneğini tıklatın.
4. İsteğe bağlı: 3. adımda ***SYSTEM** seçeneğini belirlediyseniz, sistem deposu parolasını girin ve **Continue**(Devam) seçeneğini tıklatın.
5. İsteğe bağlı: 3. adımda **Diğer Sistem Sertifikası Deposu** ' u seçtiyseniz, **Sertifika deposu yolu ve dosya adı** alanında, sertifika deponanızı yaratırken ayarladığınız IFS yolunu ve dosya adını yazın ve **Sertifika Deposu Parolası** alanına bir parola yazın. **Devam**düğmesini tıklatın.
6. Gezinme panosundaki **Sertifikaları Yönet** görev kategorisinde **Sertifikayı İçe Aktar**seçeneğini tıklatın.

   Sertifika Al sayfası, görev çerçevesinde görüntülenir.
7. Sertifika tipinize ilişkin radyo düğmesini seçin ve **Devam**düğmesini tıklatın.

   İçe Aktarma Sunucusu ya da İstemci Sertifikası sayfası ya da Sertifika Yetkilisi (CA) Sertifikası Sertifikası (Import Certificate Authority; CA) Sertifikası sayfası görev çerçevesinde görüntülenir

8. **İçe Aktarma Dosyası** alanında, içe aktarmak istediğiniz sertifikana ilişkin dosya adını yazın ve **Devam**düğmesini tıklatın.

   DCM, dosyanın biçimini otomatik olarak belirler.
9. Sertifika bir **Sunucu ya da istemci** sertifikaysa, görev çerçevesine parolayı yazın ve **Devam**düğmesini tıklatın. DCM, sertifikenin içe aktarıldığını size bildirir.

Removing certificates in IBM i

Kişisel sertifikaları kaldırmak için bu yordamı kullanın.

Yordam

1. Access the DCM interface, as described in "DCM Olanağına Erişilmesi" sayfa 262.
2. Gezinme panosunda, **Select a Certificate Store**(Sertifika Deposu Seç) seçeneğini tıklatın.

   Bir Sertifika Deposu Seç sayfası, görev çerçevesinde görüntülenir.
3. **Diğer Sistem Sertifika Deposu** onay kutusunu seçin ve **Devam**düğmesini tıklatın.

   Sertifika Deposu ve Parola sayfası görüntülenir.
4. **Sertifika deposu yolu ve dosya adı** alanında, sertifika deposunu yaratırken ayarladığınız IFS yolunu ve dosya adını yazın.
5. **Certificate Store Password** (Sertifika Deposu Parolası) alanına bir parola yazın. **Devam**düğmesini tıklatın.

   Geçerli Sertifika Deposu sayfası, görev çerçevesinde görüntülenir.
6. Gezinme panosundaki **Sertifikaları Yönet** görev kategorisinde **Sertifikayı Sil**seçeneğini tıklatın.

   Görev çerçevesinde Sertifika Silme İşleminin Doğrulanması sayfası görüntülenir.
7. Silmek istediğiniz sertifikayı seçin. **Sil** düğmesini tıklatın.
8. Sertifikayı silmek istediğinizi onaylamak için **Yes** (Evet) düğmesini tıklatın. Tersi durumda, **Hayır**' ı tıklatın.

   DCM, sertifikayı silmiş olup olmadığını bildirir.

*IBM iüzerinde tek yönlü kimlik doğrulaması için *SYSTEM sertifika deposunu kullanma*

Tek yönlü kimlik doğrulaması ayarlamak için bu yönergeleri izleyin.

Başlamadan önce

- Kuyruk yöneticisi, kanallar ve iletim kuyrukları yaratın.
- Sunucu kuyruk yöneticisinden bir sunucu ya da istemci sertifikası yaratın.
- CA sertifikasını istemci kuyruk yöneticisine aktarın ve anahtar havuzuna içe aktarın.
- Sunucuda ve istemci kuyruk yöneticilerindeki bir dinleyici başlatın.

Bu görev hakkında

Tek yönlü kimlik doğrulamasını kullanmak için, TLS sunucusu olarak IBM i çalıştıran bir bilgisayar kullanarak, SSL Key Repository (SSLKEYR) parametresini *SYSTEM olarak ayarlayın. This setting registers the IBM MQ queue manager as an application. Daha sonra, tek yönlü kimlik doğrulamasını etkinleştirmek için kuyruk yöneticisine bir sertifika atayabilirsiniz.

Özel anahtar depolarını, anahtar havuzunda istemci kuyruk yöneticisi için kukla sertifika yaratarak tek yönlü kimlik doğrulamasını gerçekleştirmek için de kullanabilirsiniz.

Yordam

1. Sunucuda ve istemci kuyruğu yöneticilerindeki aşağıdaki adımları izleyin:

a) Alter the queue manager to set the SSLKEYR parameter by issuing the command `CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM)`.

b) Stash the password for the default key repository by issuing the command `CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx')`.

Parola tek tırnak işareti içinde olmalıdır.

c) Kanalların SSLCIPO parametresinde doğru CipherSpec ' e sahip olmasını sağlar.

d) `RFRMQMAUT QMNAME(QMGRNAME) TYPE(*SSL)` komutunu vererek TLS güvenliğini yenileyin.

2. Sertifikayı sunucu kuyruk yöneticisine DCM kullanarak aşağıdaki gibi atayın:

a) Access the DCM interface, as described in "DCM Olanağına Erişilmesi" sayfa 262.

b) Gezinme panosunda, **Select a Certificate Store**(Sertifika Deposu Seç) seçeneğini tıklatın.

Bir Sertifika Deposu Seç sayfası, görev çerçevesinde görüntülenir.

c) *SYSTEM sertifika deposunu seçin ve **Continue**(Devam) öğesini tıklatın.

d) Sol panoda **Manage Applications**(Uygulamaları Yönet) öğesini genişletin.

e) Kuyruk yöneticisinin bir uygulama olarak kayıtlı olup olmadığını denetlemek için **Uygulamayı Görüntüle** tanımlamasını seçin.

`SSL (WMQ)` , çizelgede listelenir.

f) **Sertifika Atamasını Güncelle**seçeneğini belirleyin.

g) **Sunucu** seçeneğini belirleyin ve **Devam**düğmesini tıklatın.

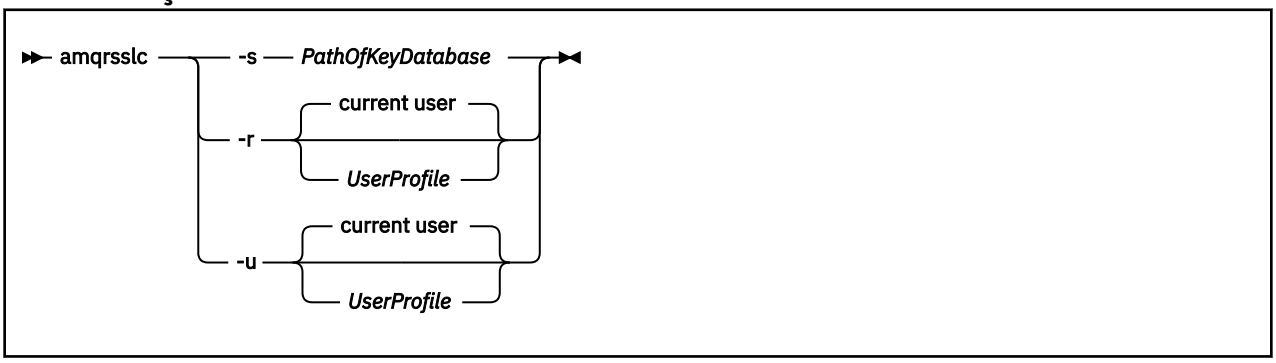
h) QMGRNAME (WMQ) öğesini seçin ve **Sertifika atamasını güncelle**düğmesini tıklatın.

i) Sertifikayı seçin ve **Yeni Sertifika Ata**düğmesini tıklatın. Sertifikayın uygulamaya atandığını belirten bir pencere açılır.

IBM iiçinIBM MQ SSL Client yardımcı programı (amqrsslc)

The IBM MQ SSL Client utility (amqrsslc) for IBM i is used by the IBM MQ MQI client on IBM i systems to register or unregister the client user profile, or stash the certificate store password. Yardımcı program yalnızca, *ALLOBJ özel yetkisine sahip bir kullanıcı ya da Digital Certificate Manager (DCM) içinde uygulama kayıtları yaratma ya da silme seçenekleri bulunan bir QMQMADM üyesiyle çalıştırılabilir.

Sözdizimi şeması



İstemci kullanıcı tanıtımını kaydettirin

IBM MQ MQI client , *SYSTEM sertifika deposunu kullanıyorsa, istemci kullanıcı tanıtımını (oturum açma kullanıcısı) Dijital Certificate Manager (DCM)ile uygulama olarak kullanılmak üzere kaydettirmeniz gerekir.

If you want to register the client user profile, run the **`amqrsslc`** program with the `-r` option with *UserProfile*. **`amqrsslc`** çağrılırken kullanılan kullanıcı tanıtımının *USE yetkisi olması gerekir. *UserProfile* seçeneği, `-r` seçeneği ile *UserProfile* öğesini, QIBM_WEBSPHERE_MQ_*UserProfile* benzersiz uygulama etiketine sahip bir sunucu uygulaması olarak kaydettirir ve *UserProfile* (WMQ) açıklamasını içeren bir etiket sağlar. Daha sonra bu sunucu uygulaması DCM ' de görüntülenir ve bu uygulamaya, sistem deposunda herhangi bir sunucu ya da istemci sertifikası atayabilirsiniz.

Not: Bir kullanıcı tanıtımı `-r` seçeneğiyle belirtilmediyse, **amqrsslc** aracını çalıştıran kullanıcının kullanıcı profili kayıtlıdır.

Aşağıdaki kod, bir kullanıcı profilini kaydetmek için **amqrsslc** ' i kullanır. İlk örnekte, belirtilen kullanıcı tanıtımı kaydedilmektedir; ikinci olarak, oturum açan kullanıcının tanıtımsıdır:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

İstemci kullanıcı profilinin kaydını kaldırın

To unregister the client profile, run the **amqrsslc** program with the `-u` option with *UserProfile*. **amqrsslc** çağrılırken kullanılan kullanıcı tanıtımının *USE yetkisi olması gerekir. Providing the *UserProfile* with the `-u` option unregisters *UserProfile* with label QIBM_WEBSPHERE_MQ_*UserProfile* from the DCM.

Not: Bir kullanıcı tanıtımı `-u` seçeneğiyle belirtilmediyse, **amqrsslc** aracını çalıştıran kullanıcının kullanıcı profilinin kaydı kaldırılmış olur.

Aşağıdaki kod, kullanıcı profilinin kaydını kaldırmak için **amqrsslc** ' i kullanır. İlk örnekte, belirtilen kullanıcı tanıtımının kaydedilmemiş olması gerekir; ikinci olarak, oturum açan kullanıcının tanıtımsıdır:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

Sertifika deposu parolasını saklar

IBM MQ MQI client , *SYSTEM sertifika deposunu kullanmıyorsa ve başka bir sertifika deposu kullanmıyorsa (yani, MQSSLKEYR, *SYSTEM dışında bir değer olarak ayarlandıysa), anahtar veri tabanının parolasının saklanmaması gerekir. Anahtar veri tabanının parolasını yığmak için `-s` seçeneğini kullanın.

Aşağıdaki kodda, sertifika deposunun tam olarak nitelenmiş dosya adı şudur: `/Path/Of/KeyDatabase/MyKey.kdb`:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Bu kod, bu anahtar veri tabanının parolasına ilişkin bir istekle sonuçlanır. Bu parola, .sth uzantılı anahtar veri tabanı ile aynı adı taşıyan bir dosyaya saklanır. Bu dosya, anahtar veri tabanından aynı yolda saklanır. Kod örneği, `/Path/Of/KeyDatabase/MyKey.sth`parola saklama dosyası oluşturur. QMQM, bu dosyanın kullanıcı sahibi ve QMQMADM grup sahibidir. QMQM ve QMQMADM okuma, yazma iznine ve diğer tanıtımlara yalnızca okuma izni vardır.

Sertifikalar üzerindeki değişiklikler ya da sertifika deposu IBM iüzerinde etkili olduğunda

Bir sertifika deposındaki sertifikaları ya da sertifika deposunun yerini değiştirdiğinizde, kanal tipine ve kanalın nasıl çalıştırıldığı bağlı olarak değişiklikler yürürlüğe girmektedir.

Aşağıdaki durumlarda, sertifika depoundaki sertifikalar ve anahtar havuzu özniteliğe ilişkin değişiklikler geçerli olur:

- Yeni bir giden tek kanal işlemi önce bir TLS kanalı çalıştırdığında.
- Yeni bir gelen TCP/IP tek kanal işlemi, ilk olarak TLS kanalı başlatma isteği alır.
- When the MQSC command REFRESH SECURITY TYPE(SSL) is issued to refresh the IBM MQ TLS environment.
- İstemci uygulaması işlemleri için, süreçteki son TLS bağlantısı kapatılır. Sonraki TLS bağlantısı, sertifika değişikliklerini alır.
- Bir süreç havuzlama işleminin (amqrmppa) iş parçacığı olarak çalışan kanallar için, süreç havuzlama işlemi başlatıldığında ya da yeniden başlatıldığında ve ilk olarak TLS kanalı çalıştırır. Süreç havuzlama

işlemi bir TLS kanalını çalıştıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH Security TYPE (SSL) komutunu çalıştırın.

- Kanal başlatıcının iş parçacığı olarak çalışan kanallar için, kanal başlatıcı başlatıldığında ya da yeniden başlatıldığında ve ilk olarak bir TLS kanalı çalıştırılır. Kanal başlatıcı işlemi zaten bir TLS kanalını çalıştırdıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH Security TYPE (SSL) komutunu çalıştırın.
- Bir TCP/IP dinleyicisinin iş parçacığı olarak çalışan kanallar için, dinleyici başlatıldığında ya da yeniden başlatıldığında ve ilk olarak TLS kanalı başlatma isteği alır. Dinleyici zaten bir TLS kanalı çalıştırdıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH SECURITY TYPE (SSL) çalıştırın.

IBM iişletim sistemi üzerinde şifreleme donanımını yapılandırma

IBM iüzerinde Cryptographic Coprocessor olanağını yapılandırmak için bu yordamı kullanın.

Başlamadan önce

Kullanıcı tanıtımınızın, yardımcı işlemci ya da donanımı yapılandırmanızı sağlamak için *ALLOBJ ve *SECADM özel yetkilerine sahip olduğundan emin olun.

Yordam

1. `http://machine.domain:2001` ya da `https://machine.domain:2010`değerine gidin; burada *makine* , bilgisayarınızın adıdır.

   Bir kullanıcı adı ve parola istenmesi için bir iletişim kutusu görüntülenir.
2. Geçerli bir IBM i kullanıcı tanıtımı ve parolası girin.
3. Cryptography (Şifreleme) bağlantısını tıklatın ve daha fazla bilgi için uygun bağlantıları izleyin.

Sonraki adım

4767 Cryptographic Coprocessor' un yapılandırılmasıyla ilgili daha ayrıntılı bilgi için 4767 Cryptographic Coprocessorbaşlıklı konuya bakın.

ULW UNIX, Linux, and Windowsüzerinde SSL/TLS ile çalışma

UNIX, Linux, and Windows sistemlerinde, Transport Layer Security (TLS) desteği IBM MQile kurulur.

Sertifika doğrulama ilkeleriyle ilgili daha ayrıntılı bilgi için Sertifika doğrulama ve güvenilirlik ilkesi tasarımıbaşlıklı konuya bakın.

ULW *Dijital sertifikaları yönetmek için `runmqckm`, `runmqakm`ve `strmqikm` 'nin kullanılması*

On UNIX, Linux, and Windows systems, manage keys and digital certificates with the **strmqikm** (iKeyman) GUI, or from the command line using **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd).

V 9.1.0

Uyarı: Both the **runmqckm** and **strmqikm** commands rely on the IBM MQ Java Runtime Environment (JRE). IBM MQ 9.1olanağından, JRE kurulu değilse, AMQ9183iletisini alırsınız.

- **UNIX and Linux** sistemleri için:
  - iKeyman GUI 'sini başlatmak için **strmqikm** (iKeyman) komutunu kullanın.
  - Use the **runmqckm** (iKeycmd) command to perform tasks with the iKeycmd command line interface.
  - Runmqakm komut satırı arabirimiyle görevleri gerçekleştirmek için **runmqakm** (GSKCapiCmd) komutunu kullanın. **runmqakm** için komut sözdizimi, **runmqckm**ile ilgili sözdizimiyle aynıdır.

    TLS sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqckm** ya da **strmqikm** komutları yerine **runmqakm** komutunu kullanın.

runmqckm ve **runmqakm** komutlarına ilişkin komut satırı arabirimlerinin tam açıklaması için Anahtarların ve sertifikaların yönetilmesi başlıklı konuya bakın.

PKCScryptographicşifreleme donanımlarında saklanan sertifikaları ya da anahtarları kullanıyorsanız, iKeycmd ve iKeyman ' ın 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gereken dış modüller 64 bit bir sürece yüklenecektir; bu nedenle, şifreleme donanımını yönetmeniz için 64 bit PKCS #11 kitaplığınız kurulu olmalıdır. The Windows and Linux x86 32-bit platforms are the only exceptions, as the iKeyman and iKeycmd programs are 32-bit on those platforms.

Ek bilgi için bkz. GSKit: PKCS#11 ve IBM MQ JRE adresleme kipi .

iKeyman GUI 'sini başlatmak için **strmqikm** komutunu çalıştırmadan önce, X Window System 'ı çalıştırabilen bir makine üzerinde çalıştığınızdan ve aşağıdakileri yaptığınızdan emin olun:

– DISPLAY ortam değişkenini ayarlayın; örneğin:

```
export DISPLAY=mypc:0
```

– PATH ortam değişkeninizin **/usr/bin** ve **/bin**' yi içerdiğinden emin olun. Bu, **runmqckm** ve **runmqakm** komutları için de gereklidir. Örneğin:

```
export PATH=$PATH:/usr/bin:/bin
```

- **Windows** sistemleri için:
  – iKeyman GUI 'sini başlatmak için **strmqikm** komutunu kullanın.
  – Use the **runmqckm** command to perform tasks with the iKeycmd command line interface.

    TLS sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqckm** ya da **strmqikm** komutları yerine **runmqakm** komutunu kullanın.
  – **runmqakm -keydb** komutunu, *stashpw* ya da *zula* seçeneğiyle birlikte kullanın.

    runmqakm -keydb komutunu bu şekilde kullanırken, örneğin:

```
runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
```

    the resultant `.sth` file does not have read permission enabled for the `mqm` group.

    Dosyayı yalnızca yaratan kişi okuyabilir. **runmqakm** komutunu kullanarak bir parola saklama dosyası yarattıktan sonra, dosya izinlerini denetleyin ve kuyruk yöneticisini çalıştıran hizmet hesabına ya da yerel `mqm`gibi bir gruba izin verin.

UNIX, Linux ya da Windows sistemlerinde TLS izlemesi istemek için bkz. strmqtrc.

İlgili başvurular

runmqckm ve runmqakm komutları
Bu kısım, komutun nesnesine göre runmqckm ve runmqakm komutlarını açıklar.

ULW *UNIX, Linux, and Windowsüzerinde bir anahtar havuzu ayarlanıyor*

You can set up a key repository by the using **strmqikm** (iKeyman) GUI, or from the command line using **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd) commands.

Bu görev hakkında

TLS bağlantısı, bağlantının her iki ucunda bir *anahtar havuzu* gerektirir. Her IBM MQ kuyruk yöneticisinin ve IBM MQ MQI client ' in bir anahtar havuzuna erişimi olması gerekir. Daha fazla bilgi için bkz “SSL/TLS anahtarı havuzu” sayfa 23.

UNIX, Linux, and Windows sistemlerinde, dijital sertifikalar **strmqikm** kullanıcı arabirimi kullanılarak ya da **runmqckm** ya da **runmqakm** komutları kullanılarak yönetilen bir anahtar veritabanı dosyasında depolanır. Bu dijital sertifikaların etiketleri var. Belirli bir etiket, kişisel bir sertifikayı kuyruk yöneticisi ya da IBM MQ MQI clientile ilişkilendirir. TLS, kimlik doğrulama amacıyla bu sertifikayı kullanır. On UNIX, Linux,

and Windows systems, IBM MQ uses either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or IBM MQ MQI client user logon ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

Anahtar veri tabanı dosyası adı, bir yol ve kök adından oluşur:

- UNIX and Linux sistemlerinde, bir kuyruk yöneticisi için varsayılan yol (kuyruk yöneticisini yarattığınız zaman ayarlanır) `/var/mqm/qmgrs/`*`queue_manager_name`*`/ssl`.

  Windows sistemlerinde varsayılan yol şöyledir: *`MQ_INSTALLATION_PATH`*`\Qmgrs\`*`queue_manager_name`*`\ssl`; burada *`MQ_INSTALLATION_PATH`* , IBM MQ ' in kurulu olduğu dizindir. Örneğin, `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl`.

  Varsayılan kök adı `key`' dir. İsteğe bağlı olarak, kendi yolunuzu ve kök adınızı seçebilirsiniz, ancak uzantı `.kdb`olmalıdır.

  Kendi yol ya da dosya adınızı seçerseniz, erişimi sıkı bir şekilde denetlemek için, bu dosyaya ilişkin izinleri ayarlayın.
- Bir IBM MQ istemcisi için varsayılan yol ya da kök adı yoktur. Bu dosyaya erişimi sıkı bir şekilde denetleyin. Uzantı `.kdb`olmalıdır.

Dosya düzeyi kilitlerini desteklemeyen bir dosya sisteminde anahtar havuzları yaratmayın; örneğin, Linux sistemlerinde NFS sürüm 2.

Anahtar veritabanı kütüğü adının denetlenmesi ve belirtilmesiyle ilgili bilgi edinmek için “UNIX, Linux, and Windowsüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzu yerinin değiştirilmesi” sayfa 279 dosyasına bakın. Anahtar veri tabanı kütüğünü yaratmadan önce ya da sonra, anahtar veri tabanı dosyası adını belirtebilirsiniz.

strmqikm ya da **runmqckm** komutlarını çalıştırdığınız kullanıcı kimliğinin, anahtar veri tabanı dosyasının yaratıldığı ya da güncellendiği dizin için yazma iznine sahip olması gerekir. Varsayılan `ssl` dizinini kullanan bir kuyruk yöneticisi için, **strmqikm** ya da **runmqckm** çalıştırdığınız kullanıcı kimliğinin mqm grubunun bir üyesi olması gerekir. For an IBM MQ MQI client, if you run **strmqikm** or **runmqckm** from a user ID different from that under which the client runs, you must alter the file permissions to enable the IBM MQ MQI client to access the key database file at run time. Daha fazla bilgi için bkz. “Windowsüzerindeki anahtar veri tabanı dosyalarınıza erişilmesi ve güvenceye alınması” sayfa 277 ya da “UNIX and Linux sistemlerindeki anahtar veri tabanı dosyalarınızın erişilmesi ve güvenliğinin sağlanması” sayfa 277.

strmqikm için ya da IBM WebSphere MQ 7.0için **runmqckm** içinde, yeni anahtar veritabanları otomatik olarak önceden tanımlanmış bir sertifika yetkilisi (CA) sertifikasıyla doldurulur. In **strmqikm** or **runmqckm** for IBM MQ 8.0, key databases are not automatically populated, making the initial setup more secure because you include only the CA certificates that you want, in your key database file.

Not: CA sertifikalarıyla sonuçlanan GSKit 8.0 davranışındaki bu değişiklik nedeniyle artık havuza otomatik olarak eklenmiyor, tercih ettiğiniz CA sertifikalarını el ile eklemelisiniz. Bu davranış değişikliği, kullanılan CA sertifikaları üzerinde daha fazla ayrıntı denetimi sağlar. Bkz. “Adding default CA certificates into an empty key repository on UNIX, Linux, and Windows with GSKit 8.0” sayfa 277.

Anahtar veritabanını, komut satırını kullanarak ya da **strmqikm** (iKeyman) kullanıcı arabirimini kullanarak yaraladınız.

Not: TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** kullanıcı arabirimi FIPS uyumlu bir seçenek sunmaz.

Yordam

Komut satırını kullanarak bir anahtar veritabanı yaratın.

1. Aşağıdaki komutlardan birini çalıştırın:
   - **runmqckm**komutunu kullanma:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

- **runmqakm**komutunu kullanma:

```
runmqakm -keydb -create -db filename -pw password -type cms
-stash -fips -strong
```

Burada:

-db *kütükadı*
Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirler ve `.kdb`dosya uzantısına sahip olmalıdır.

-pw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

-type *cms*
Veri tabanının tipini belirtir. (IBM MQiçin, `cms`olmalıdır.)

-stash
Anahtar veritabanı parolasını bir dosyaya kaydeder.

-fips.
Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

-Güçlü
Girilen parolanın, parola güvenlik düzeyi için gereken minimum gereksinimleri karşıladığını denetler. Bir parolaya ilişkin minimum gereksinimler aşağıdaki gibidir:

- Parola en az 14 karakter uzunluğunda olmalıdır.
- Parola, en az bir küçük harf, bir büyük harf ve bir rakam ya da özel karakter içermelidir. Özel karakterler, yıldız işareti (*), dolar işareti ($), sayı işareti (#) ve yüzde işareti (%) içerir. Boşluk, özel karakter olarak sınıflandırılır.
- Her karakter, bir parolada en çok üç kez oluşabilir.
- Parolada art arda en çok iki karakter aynı olabilir.
- Tüm karakterler standart ASCII yazdırılabilir karakter takımında, 0x20 - 0x7Earalığında yer alıyor.

Diğer bir seçenek olarak, **strmqikm** (iKeyman) kullanıcı arabirimini kullanarak bir anahtar veritabanı yaratın.

2. UNIX and Linux sistemlerinde, kök kullanıcı olarak oturum açın. Windows sistemlerinde, Yönetici olarak ya da MQM grubunun bir üyesi olarak oturum açın.
3. **strmqikm** komutunu çalıştırarak kullanıcı arabirimini başlatın.
4. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **New**(Yeni) seçeneğini tıklatın.
   Yeni pencere açılır.
5. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
6. **File Name** (Dosya Adı) alanına bir dosya adı yazın.
   Bu alan `key.kdb`metnini zaten içeriyor. Kök adınız `key`ise, bu alanı değiştirmeden bırakın. Farklı bir kök adı belirtdiyseniz, `key` yerine kök adınızı koyun. Ancak, `.kdb` uzantısını değiştirmemelisiniz.
7. **Konum** alanına yolu yazın.
   Örneğin:
   - Kuyruk yöneticisi için: `/var/mqm/qmgrs/QM1/ssl` (UNIX and Linux sistemlerinde) ya da `C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl` (Windows sistemlerinde).
     Yol, kuyruk yöneticisinin **SSLKeyRepository** özniteliğinin değeriyle eşleşmelidir.
   - Bir IBM MQ istemcisi için: `/var/mqm/ssl` (UNIX and Linux sistemlerinde) ya da `C:\mqm\ssl` (Windows sistemlerinde).
8. **Tamam**'ı tıklatın.

Parola İstemi penceresi açılır.

9. **Parola** alanına bir parola yazın ve **Parolayı Onayla** alanına parolayı yeniden yazın.
10. **Parola dosyaya girin** onay kutusunu seçin.

    Not: Parolayı saklamadıysanız, anahtar veritabanı dosyasına erişmek için gereken parolayı elde edemedikleri için TLS kanallarını başlatma girişimleri başarısız olur.
11. **Tamam**'ı tıklatın.

    Kişisel Sertifikalar penceresi açılır.
12. Set the access permissions as described in “Windowsüzerindeki anahtar veri tabanı dosyalarınıza erişilmesi ve güvenceye alınması” sayfa 277 or “UNIX and Linux sistemlerindeki anahtar veri tabanı dosyalarınızın erişilmesi ve güvenliğinin sağlanması” sayfa 277.

Windows *Windowsüzerindeki anahtar veri tabanı dosyalarınıza erişilmesi ve güvenceye alınması*

Anahtar veritabanı dosyaları uygun erişim izinlerine sahip olmayabilir. Bu dosyalara uygun erişimi ayarlamalısınız.

Erişim denetimini *key*.kdb, *key*.sth, *key*.crlve *key*.rdbkütüklerine ayarlayın; burada *anahtar* , sınırlı bir kullanıcı kümesine yetki vermek için, anahtar veritabanınızın kök adıdır.

Erişim vermeyi aşağıdaki gibi dikkate alın:

tam yetki
BUILTIN\Administrators, NT AUTHORITY\SYSTEM ve veri tabanı dosyalarını yaratan kullanıcı.

okuma yetkisi
Kuyruk yöneticisi için, yalnızca yerel mqm grubu için. Bu, MCA ' nın mqm grubundaki bir kullanıcı kimliği altında çalışmakta olduğunu varsayar.

Bir istemci için, istemci işleminin altında çalıştığı kullanıcı kimliği.

Linux UNIX *UNIX and Linux sistemlerindeki anahtar veri tabanı dosyalarınızın erişilmesi ve güvenliğinin sağlanması*

Anahtar veritabanı dosyaları uygun erişim izinlerine sahip olmayabilir. Bu dosyalara uygun erişimi ayarlamalısınız.

Kuyruk yöneticisi için, anahtar veritabanı kütüklerine ilişkin izinleri ayarlayın; böylece kuyruk yöneticisi ve kanal işlemleri gerektiğinde bunları okuyabilirler, ancak diğer kullanıcılar bunları okuyamaz ya da değiştiremezler. Olağan durumda, mqm kullanıcısının okuma izinleri gerekir. Anahtar veritabanı dosyasını mqm kullanıcısı olarak oturum açarak yaratdıysanız, izinler büyük olasılıkla yeterlidir; mqm kullanıcısı değilseniz, ancak mqm grubundaki başka bir kullanıcı değilseniz, büyük olasılıkla mqm grubundaki diğer kullanıcılara okuma izinleri vermeniz gerekir.

Bir istemci için de benzer şekilde, anahtar veritabanı kütüklerine ilişkin izinleri ayarlayın; böylece, istemci uygulaması işlemleri gerektiğinde bunları okuyabilirler, ancak diğer kullanıcılar bunları okuyamaz ya da değiştiremez. Olağan durumda, istemci işleminin çalıştığı kullanıcının okuma izinlerine gerek vardır. Anahtar veritabanı dosyasını kullanıcı olarak oturum açarak yarattıktan sonra izinler yeterli olur; istemci işlemi kullanıcısı değilseniz, ancak gruptaki başka bir kullanıcı ise, gruptaki diğer kullanıcılara okuma izinleri vermeniz gerekebilir.

key.kdb, *key*.sth, *key*.crlve *key*.rdbdosyalarındaki izinleri ayarlayın; burada *anahtar* , anahtar veritabanınızın kök adıdır, dosya sahibi için okuma ve yazma ve mqm ya da istemci kullanıcı grubu için okuma olarak ayarlanır.

ULW *Adding default CA certificates into an empty key repository on UNIX, Linux, and Windows with GSKit 8.0*

GSKit sürüm 8 ile boş bir anahtar havuzuna varsayılan CA sertifikalarından birini ya da birkaçını eklemek için bu yordamı izleyin.

GSKit 7.0' ta, yeni bir anahtar havuzu oluştururken davranış, genel olarak kullanılan Sertifika Yetkilileri için bir varsayılan sertifika kuruluşu (CA) sertifikası kümesinde otomatik olarak eklenmeye başlanmdandı.

GSKit sürüm 8 için bu davranış, CA sertifikalarının artık otomatik olarak havuza eklenmeyecek şekilde değişmiştir. Kullanıcı şimdi anahtar deposuna CA sertifikalarını el ile eklemek için gereklidir.

Kullanılan `strmqikm`

CA sertifikasını eklemek istediğiniz makine üzerinde aşağıdaki adımları gerçekleştirin:

1. Start the GUI using the **strmqikm** command (on UNIX, Linux, and Windows).
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı eklemek istediğiniz anahtar veritabanı dosyasını seçin (örneğin, `key.kdb`).
6. **Aç**düğmesini tıklatın. Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. **Anahtar veritabanı içeriği** alanında **İmzalayıcı Sertifikaları**öğesini seçin.
9. **Veri Yerleştir**' i tıklatın. Add CA ' nın Sertifika penceresi açılır.
10. Havuza eklenebilecek CA sertifikaları, sıradüzensel bir ağaç yapısında görüntülenir. Geçerli CA sertifikalarının tam listesini görüntülemek için CA sertifikalarını güvenmek istediğiniz kuruluş için en üst düzey girdisini seçin.
11. Listeden güvenmek istediğiniz CA sertifikalarını seçin ve **Tamam**' ı tıklatın. Sertifikalar anahtar havuzuna eklenir.

Komut satırını kullanma

Aşağıdaki komutları listelemek için kullanın, ardından **runmqckm**kullanarak CA sertifikalarını ekleyin:

- Varsayılan CA sertifikalarını listeleyen kuruluşlarla birlikte listelemek için aşağıdaki komutu verin:

```
runmqckm -cert -listsigners
```

- *etiket* alanında belirtilen kuruluşa ilişkin tüm sertifika kuruluşu (CA) sertifikalarını eklemek için aşağıdaki komutu verin:

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

Burada:

`-db` *filename*	anahtar veri tabanının tam olarak nitelenmiş yol adıdır.
`-pw` *password*	Anahtar veri tabanının parolasıdır.
`-label` *label*	sertifikaya eklenen etikettir.

Not: Adding a CA certificate to a key repository results in IBM MQ trusting all personal certificates signed by that CA certificate. Güvenmek istediğiniz Sertifika Yetkililerini dikkate alın ve yalnızca istemci ve yöneticilerinizi doğrulamak için gereken CA sertifikalarının kümesini ekleyin. Bu, güvenlik ilkeniz için kesin bir gereksinim olmadıkça, varsayılan CA sertifikalarının tam kümesinin eklenmesi önerilmez.

ULW *UNIX, Linux, and Windowsüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzunun bulunması*

Kuyruk yöneticinizin anahtar veritabanı dosyasının yerini almak için bu yordamı kullanın.

Yordam

1. Aşağıdaki MQSC komutlarından birini kullanarak kuyruk yöneticinizin özniteliklerini görüntüleyin:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

   Kuyruk yöneticinizin özniteliklerini IBM MQ Explorer ya da PCF komutlarını kullanarak da görüntüleyebilirsiniz.
2. Anahtar veri tabanı dosyasının yol ve kök adını saptamak için komut çıkışını inceleyin.
   Örneğin,

   a. UNIX and Linux: `/var/mqm/qmgrs/QM1/ssl/key`üzerinde; burada `/var/mqm/qmgrs/QM1/ssl` yolu ve `key` kök adıdır.

   b. Windows: *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl\key`üzerine, burada *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl` yol ve `key` kök adıdır. *MQ_INSTALLATION_PATH* , IBM MQ ' in kurulu olduğu üst düzey dizini temsil eder.

ULW UNIX, Linux, and Windowsüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzu yerinin değiştirilmesi

MQSC komutu ALTER QMGR de dahil olmak üzere, kuyruk yöneticinizin anahtar veritabanı dosyasının yerini çeşitli yollarla değiştirebilirsiniz.

Kuyruk yöneticinizin anahtar havuzu özniteliğini ayarlamak için, ALTER QMGR komutunu kullanarak, kuyruk yöneticisi anahtar veri tabanı dosyasının yerini değiştirebilirsiniz. Örneğin, UNIX and Linuxüzerinde:

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey')
```

Anahtar veritabanı dosyası tam olarak nitelenmiş dosya adına sahip: `/var/mqm/qmgrs/QM1/ssl/MyKey.kdb`

Windows'ta:

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey')
```

Anahtar veritabanı dosyası tam olarak nitelenmiş dosya adına sahip: `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb`

Uyarı: Kuyruk yöneticisi bu uzantıyı otomatik olarak eklediği için, SSLKEYR anahtar sözcüğündeki dosya adına `.kdb` uzantısını eklediğinizden emin olun.

Ayrıca, kuyruk yöneticinizin özniteliklerini IBM MQ Explorer ya da PCF komutlarını kullanarak da değiştirebilirsiniz.

Bir kuyruk yöneticisinin anahtar veri tabanı dosyasının yerini değiştirdiğinizde, sertifikalar eski konumdan aktarılmaz. If the key database file you are now accessing is a new key database file, you must populate it with the CA and personal certificates you need, as described in “Kişisel bir sertifikin UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna aktarılması” sayfa 294.

ULW UNIX, Linux, and Windowsüzerinde bir IBM MQ MQI client için anahtar havuzunun bulunması

Anahtar havuzunun yeri MQSSLKEYR değişkeniyle verilir ya da MQCONNX çağrısında belirtilir.

IBM MQ MQI clientile ilgili anahtar veri tabanı dosyasının yerini bulmak için MQSSLKEYR ortam değişkenini inceleyin. Örneğin:

```
echo $MQSSLKEYR
```

Ayrıca, anahtar veritabanı dosyası adının bir MQCONNX çağrısında da (“UNIX, Linux, and Windowsüzerinde bir IBM MQ MQI client için anahtar havuzu yerini belirtme” sayfa 280) açıklandığı şekilde ayarlanabileceği için uygulamanızı da denetleyin. Bir MQCONNX çağrısındaki değer kümesi, MQSSLKEYR değerini geçersiz kılar.

ULW *UNIX, Linux, and Windowsüzerinde bir IBM MQ MQI client için anahtar havuzu yerini belirtme*

IBM MQ MQI clientiçin varsayılan anahtar havuzu yok. Konumunu iki şekilde belirtebilirsiniz. Diğer sistemlere yetkisiz kopyalamayı önlemek için anahtar veritabanı dosyasına yalnızca amaçlanan kullanıcılar ya da denetimciler tarafından erişilebildiğinden emin olun.

IBM MQ MQI client ' niz için anahtar veri tabanı dosyasının yerini iki şekilde belirtebilirsiniz:

- MQSSLKEYR ortam değişkeni ayarlanıyor. Örneğin, UNIX and Linuxüzerinde:

  ```
  export MQSSLKEYR=/var/mqm/ssl/key
  ```

  Anahtar veri tabanı dosyası, tam olarak nitelenmiş dosya adını içerir:

  ```
  /var/mqm/ssl/key.kdb
  ```

  Windows'ta:

  ```
  set MQSSLKEYR=C:\Program Files\IBM\MQ\ssl\key
  ```

  Anahtar veri tabanı dosyası, tam olarak nitelenmiş dosya adını içerir:

  ```
  C:\Program Files\IBM\MQ\ssl\key.kdb
  ```

  Not: **.** kdb uzantısı, dosya adının zorunlu bir parçasıdır, ancak ortam değişkeninin değerinin bir parçası olarak içerilmez.
- Bir uygulama MQCONNX çağrısı yaptığında, MQSCO yapısının *KeyRepository* alanında anahtar veri tabanı dosyasının yol ve kök adını sağlar. MQCONNX içinde MQSCO yapısının kullanılmasına ilişkin ek bilgi için Overview for MQSCObaşlıklı konuya bakın.

ULW *Sertifikalar üzerindeki değişiklikler ya da sertifika deposu UNIX, Linux, and Windowsüzerinde etkili olduğunda*

Bir sertifika deposındaki sertifikaları ya da sertifika deposunun yerini değiştirdiğinizde, kanal tipine ve kanalın nasıl çalıştırıldığı bağlı olarak değişiklikler yürürlüğe girmektedir.

Anahtar veri tabanı dosyasındaki sertifikalar ve anahtar havuzu özniteliği aşağıdaki durumlarda etkinleşir:

- Yeni bir giden tek kanal işlemi önce bir TLS kanalı çalıştırdığında.
- Yeni bir gelen TCP/IP tek kanal işlemi, ilk olarak TLS kanalı başlatma isteği alır.
- TLS ortamını yenilemek için MQSC komutu REFRESH SECURITY TYPE (SSL) yayınlandığında.
- İstemci uygulaması işlemleri için, süreçteki son TLS bağlantısı kapatılır. Sonraki TLS bağlantısı, sertifika değişikliklerini alır.
- Bir süreç havuzlama işleminin (amqrmppa) iş parçacığı olarak çalışan kanallar için, süreç havuzlama işlemi başlatıldığında ya da yeniden başlatıldığında ve ilk olarak TLS kanalı çalıştırır. Süreç havuzlama işlemi bir TLS kanalını çalıştıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH Security TYPE (SSL) komutunu çalıştırın.
- Kanal başlatıcının iş parçacığı olarak çalışan kanallar için, kanal başlatıcı başlatıldığında ya da yeniden başlatıldığında ve ilk olarak bir TLS kanalı çalıştırılır. Kanal başlatıcı işlemi zaten bir TLS kanalını çalıştırdıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH Security TYPE (SSL) komutunu çalıştırın.

- Bir TCP/IP dinleyicisinin iş parçacığı olarak çalışan kanallar için, dinleyici başlatıldığında ya da yeniden başlatıldığında ve ilk olarak TLS kanalı başlatma isteği alır. Dinleyici zaten bir TLS kanalı çalıştırdıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH SECURITY TYPE (SSL) çalıştırın.

You can also refresh the IBM MQ TLS environment using the IBM MQ Explorer or PCF commands.

ULW *UNIX, Linux, and Windows üzerinde kendinden onaylı kişisel sertifika oluşturma*

strmqikm (iKeyman) öğesini kullanarak kendinden onaylı bir sertifika yaratabilirsiniz. GUI ya da **runmqckm** (iKeycmd) ya da **runmqakm** (GSKCapiCmd) komutunu kullanarak komut satırından.

Not: IBM MQ , SHA-3 ya da SHA-5 algoritmalarını desteklemez. Her iki algoritma da SHA-2 ailesinin üyesi olduğundan, SHA384WithRSA ve SHA512WithRSA dijital imza algoritması adlarını kullanabilirsiniz.

Sayısal imza algoritması adları SHA3WithRSA ve SHA5WithRSA , sırasıyla SHA384WithRSA ve SHA512WithRSA kısaltması oldukları için kullanımdan kaldırılmıştır.

Kendinden onaylı sertifikaları neden kullanmak isteyebileceğinize ilişkin ek bilgi için İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için kendinden onaylı sertifikaları kullanmabaşlıklı konuya bakın.

Tüm dijital sertifikalar tüm CipherSpecsile birlikte kullanılamaz. Kullanmanız gereken CipherSpecs ile uyumlu bir sertifika yarattığınızdan emin olun. IBM MQ , üç farklı CipherSpectipini destekler. Ayrıntılar için “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42 başlıklı konudaki “Eliptik Eğri ve RSA CipherSpecs Birlikte Çalışabilirlik” sayfa 43 konusuna bakın.

Tip 1 CipherSpecs ' i (ECDHE_ECDSA_ile başlayan adları olanlar) kullanmak için sertifikayı yaratmak üzere **runmqakm** komutunu kullanmanız ve bir Eliptik Eğri ECDSA imza algoritması parametresi belirtmeniz gerekir; örneğin, **-sig_alg** EC_ecdsa_with_SHA384.

-sig_alg hash algoritması ile kullanılabilen seçeneklerin bir listesi için bkz. “UNIX, Linux, and Windows üzerinde runmqckm ve runmqakm seçenekleri” sayfa 509 .

Aşağıdaki işlemleri kullanıyorsanız:

- GUI, bkz. “strmqikm kullanıcı arabirimini kullanma” sayfa 281
- Komut satırı, bkz. “Komut satırını kullanma” sayfa 282

ULW *strmqikm kullanıcı arabirimini kullanma*

strmqikm (iKeyman) olanağını kullanarak kişisel bir sertifika yaratabilirsiniz. GUI.

Bu görev hakkında

strmqikm , FIPS uyumlu bir seçenek sunmaz. TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Yordam

Grafik kullanıcı arabirimini kullanarak, kuyruk yöneticinizin ya da IBM MQ MQI client ' ın kişisel sertifikasını yaratmak için aşağıdaki adımları tamamlayın:

1. **strmqikm** komutunu kullanarak GUI ' yi başlatın.
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın.
   Aç penceresi görüntülenir.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. İsteğiniz oluşturmak istediğiniz anahtar veritabanı dosyasını seçin; örneğin, key . kdb.
6. **Tamam**'ı tıklatın.
   Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın.

Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında gösterilir.

8. **Yarat** menüsünden, **Kendinden onaylı yeni sertifika**öğesini tıklatın. Yeni Kendinden Onaylı Sertifika Yarat penceresi görüntülenir.
9. **Key Label** (Anahtar Etiketi) alanına sertifika etiketini girin.

   The label is either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or IBM MQ MQI client logon user ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.
10. **Ayırt edici ad** alanında herhangi bir alan için ya da **Konu diğer adı** alanlarından herhangi biri için bir değer yazın ya da seçin.
11. Kalan alanlar için, varsayılan değerleri kabul edin ya da yeni değerleri yazın ya da seçin.

    Ayırt Edici Adlar hakkında daha fazla bilgi için bkz. “Belirleyici Adlar” sayfa 11.
12. **Tamam**'ı tıklatın.

    Kişisel Sertifikalar listesinde, yarattığınız kendinden onaylı kişisel sertifikana ilişkin etiket gösterilir.

Sonraki adım

Sertifika isteği (CA) için gönderin. Ek bilgi için “Kişisel sertifikaların UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna alınması” sayfa 288 ' e bakın.

ULW *Komut satırını kullanma*

You can create a personal certificate from the command line using the **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd) commands. SSL ya da TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Yordam

runmqckm ya da **runmqakm** (GSKCapiCmd) komutunu kullanarak kendinden onaylı bir kişisel sertifika yaratın.

- UNIX, Linux, and Windowsüzerinde **runmqckm** kullanılıyor:

```
runmqckm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days
 -sig_alg algorithm
```

  -dn *distinguished_name*yerine, -san_dnsname *DNS_names*, -san_emailaddr *email_addresses*ya da -san_ipaddr *IP_addresses*' yi kullanabilirsiniz.

- **runmqakm**komutunu kullanma:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days

        -fips -sig_alg algorithm
```

Burada:

-db *kütükadı*
Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirtir.

-pw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

-label *etiket*
Sertifikaya eklenen anahtar etiketini belirtir. The label is either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or the IBM MQ

MQI client logon user ID appended, all in lowercase. Ayrıntılar için bkz. “Dijital sertifika etiketleri, gereksinimleri anlama” sayfa 25.

-dn ***ayırt edici ayırt edici ad***
Çift tırnak işareti içine alınmış X.500 ayırt edici adını belirtir. En az bir öznitelik gerekli. Birden çok OU ve DC özniteliği sağlayabilirsiniz.

Not: The **runmqckm** and **runmqakm** tools refer to the postal code attribute as POSTALKOD, not PC. Sertifikaları bir posta kodu ile istemek için bu sertifika yönetimi komutlarını kullandığınızda her zaman **-dn** parametresindeki POSTALCODE değerini belirtin.

-size ***anahtar_büyüklüğü***
Anahtar büyüklüğünü belirler. **runmqckm**kullanıyorsanız, değer 512 ya da 1024olabilir. **runmqakm**kullanıyorsanız, bu değer 512, 1024ya da 2048olabilir.

x509version ***sürüm***
Yaratılacak X.509 sertifikasının sürümü. Değer 1, 2 ya da 3 olabilir. Varsayılan 3'tür.

-file ***kütükadı***
Sertifika isteğine ilişkin dosya adını belirler.

-süresinin dolması ***gün***
Sertifikana ilişkin geçerlilik süresi (gün olarak) Varsayılan değer, sertifika için 365 gündür.

-fips.
Komutun FIPS kipinde çalıştırıldığını belirtir. Yalnızca FIPS ICC bileşeni kullanılır ve bu bileşen FIPS kipinde başarıyla kullanıma hazırlanmalıdır. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqaqm** komutu başarısız olur.

-sig_alg
runmqckmiçin, girişin anahtar çiftinin oluşturulması için kullanılan asimetrik imza algoritmasını belirtir. Değer şu şekilde olabilir: 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. Varsayılan değer SHA1WithRSA' dır.

-sig_alg
runmqakmiçin, bir sertifika isteğinin oluşturulması sırasında kullanılan HASH algoritmasını belirtir. Bu hash algoritması, yeni yaratılan sertifika isteğiyle ilişkilendirilmiş imzayı yaratmak için kullanılır. The value can be md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WIT_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. Varsayılan değer SHA1WithRSA' dır.

-san_dnsname ***DNS_ads***
Yaratılmakta olan girişle ilgili DNS adlarının virgülle sınırlanmış ya da boşlukla ayrılmış listesini belirtir.

-san_emailaddr ***email_adress***
Yaratılmakta olan girişe ilişkin e-posta adreslerinin virgülle sınırlanmış ya da boşlukla ayrılmış bir listesini belirtir.

-san_ipaddr ***IP_adresleri***
Yaratılmakta olan girişle ilgili IP adreslerinin virgülle sınırlanmış ya da boşlukla ayrılmış listesini belirtir.

Sonraki adım

Sertifika isteği (CA) için gönderin. Ek bilgi için “Kişisel sertifikaların UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna alınması” sayfa 288 ' e bakın.

ULW *UNIX, Linux, and Windows üzerinde kişisel sertifika isteme*

strmqikm (iKeyman) kullanarak kişisel sertifika isteyebilirsiniz. GUI ya da **runmqckm** (iKeycmd) ya da **runmqakm** (GSKCapiCmd) komutlarını kullanarak komut satırından. SSL ya da TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın.

Bu görev hakkında

strmqikm GUI 'sini kullanarak ya da komut satırından aşağıdaki noktalara bağlı olarak kişisel sertifika isteyebilirsiniz:

- IBM MQ , SHA-3 ya da SHA-5 algoritmalarını desteklemez. Her iki algoritma da SHA-2 ailesinin üyesi olduğundan, SHA384WithRSA ve SHA512WithRSA dijital imza algoritması adlarını kullanabilirsiniz.
- Sayısal imza algoritması adları SHA3WithRSA ve SHA5WithRSA , sırasıyla SHA384WithRSA ve SHA512WithRSA kısaltması oldukları için kullanımdan kaldırılmıştır.
- Tüm dijital sertifikalar tüm CipherSpecsile birlikte kullanılamaz. Kullanmanız gereken CipherSpecs ile uyumlu bir sertifika isteğinde bulunduğunuzdan emin olun. IBM MQ , üç farklı CipherSpectipini destekler. Ayrıntılar için “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42 başlıklı konudaki “Eliptik Eğri ve RSA CipherSpecs Birlikte Çalışabilirlik” sayfa 43 konusuna bakın.
- Tip 1 CipherSpecs ' i (adları ECDHE_ECDSA_ile başlayan) kullanmak için sertifikayı istemek için **runmqakm** komutunu kullanmanız ve bir Eliptik Eğri ECDSA imza algoritması parametresi belirtmeniz gerekir; örneğin, **-sig_alg** EC_ecdsa_with_SHA384.

  -sig_alg hash algoritması ile kullanılabilen seçeneklerin bir listesi için bkz. “UNIX, Linux, and Windows üzerinde runmqckm ve runmqakm seçenekleri” sayfa 509 .
- Yalnızca **runmqakm** komutu FIPS uyumlu bir seçenek sağlar.
- Şifreleme donanımı kullanıyorsanız, bkz. “PKCS #11 donanımınıza ilişkin kişisel bir sertifika istenmesi” sayfa 302.

Aşağıdaki işlemleri kullanıyorsanız:

- GUI, bkz. “strmqikm kullanıcı arabirimini kullanma” sayfa 284
- Komut satırı, bkz. “Komut satırını kullanma” sayfa 285

ULW *strmqikm kullanıcı arabirimini kullanma*

You can request a personal certificate by using the **strmqikm** (iKeyman) GUI, or from the command line using the **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd) commands. SSL ya da TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Bu görev hakkında

strmqikm , FIPS uyumlu bir seçenek sunmaz. TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Yordam

iKeyman kullanıcı arabirimini kullanarak kişisel bir sertifika için geçerli olmak üzere aşağıdaki adımları tamamlayın:

1. **strmqikm** komutunu kullanarak kullanıcı arabirimini başlatın.
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın.

   Aç penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.

5. İsteğiniz oluşturmak istediğiniz anahtar veritabanı dosyasını seçin; örneğin, `key.kdb`.
6. **Aç**'ı tıklatın.

   Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın.

   Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında gösterilir.
8. **Yarat** menüsünden **Yeni Sertifika İsteği**öğesini tıklatın. **Yeni Anahtar ve Sertifika İsteği Oluştur** penceresi açılır.
9. **Key Label** (Anahtar Etiketi) alanına sertifika etiketini girin.

   The label is either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or IBM MQ MQI client logon user ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.
10. **Ayırt edici ad** alanında herhangi bir alan için ya da **Konu diğer adı** alanlarından herhangi biri için bir değer yazın ya da seçin. Kalan alanlar için, varsayılan değerleri kabul edin ya da yeni değerleri yazın ya da seçin.

    Ayırt Edici Adlar hakkında daha fazla bilgi için bkz. “Belirleyici Adlar” sayfa 11.
11. **Sertifika isteği saklanacak bir dosyanın adını girin** alanında, varsayılan `certreq.arm`değerini kabul edin ya da tam yolu olan yeni bir değer yazın.
12. **Tamam**'ı tıklatın.

    Bir doğrulama penceresi görüntülenir.
13. **Tamam**'ı tıklatın.

    Kişisel Sertifika İstekleri listesinde, yarattığınız yeni kişisel sertifika isteğinin etiketi gösterilir. Sertifika isteği, “11” sayfa 285adımında seçtiğiniz dosyada saklanır.
14. Yeni kişisel sertifikayı, dosyayı sertifika yetkilisine (CA) göndererek ya da dosyayı CA için web sitesindeki istek formuna kopyalayarak isteyin.

ULW *Komut satırını kullanma*

You can request a personal certificate from the command line using the **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd) commands. SSL ya da TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Yordam

runmqckm ya da **runmqakm** (GSKCapiCmd) komutunu kullanarak kişisel bir sertifika isteyin.

- **runmqckm**komutunu kullanma:

```
runmqckm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
        -file filename -sig_alg algorithm
```

  -dn *distinguished_name*yerine, -san_dsname *DNS_names*, -san_emailaddr *email_addresses*ya da -san_ipaddr *IP_addresses*' yi kullanabilirsiniz.
- **runmqakm**komutunu kullanma:

```
runmqakm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
         -file filename -fips -sig_alg algorithm
```

Burada:

-db *kütükadı*
Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirtir.

-pw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

-label *etiket*
Sertifikaya eklenen anahtar etiketini belirtir. The label is either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or the IBM MQ MQI client logon user ID appended, all in lowercase. Ayrıntılar için bkz. "Dijital sertifika etiketleri, gereksinimleri anlama" sayfa 25.

-dn *ayırt edici ayırt edici ad*
Çift tırnak işareti içine alınmış X.500 ayırt edici adını belirtir. En az bir öznitelik gerekli. Birden çok OU ve DC özniteliği sağlayabilirsiniz.

Not: The **runmqckm** and **runmqakm** tools refer to the postal code attribute as POSTALKOD, not PC. Sertifikaları bir posta kodu ile istemek için bu sertifika yönetimi komutlarını kullandığınızda her zaman **-dn** parametresindeki POSTALCODE değerini belirtin.

-size *anahtar_büyüklüğü*
Anahtar büyüklüğünü belirler. **runmqckm**kullanıyorsanız, değer 512 ya da 1024olabilir. **runmqakm**kullanıyorsanız, bu değer 512, 1024ya da 2048olabilir.

-file *kütükadı*
Sertifika isteğine ilişkin dosya adını belirler.

-fips.
Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

-sig_alg
runmqckmiçin, girişin anahtar çiftinin oluşturulması için kullanılan asimetrik imza algoritmasını belirtir. Değer şu şekilde olabilir: `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`. Varsayılan değer `SHA1WithRSA`' dır.

-sig_alg
runmqakmiçin, bir sertifika isteğinin oluşturulması sırasında kullanılan HASH algoritmasını belirtir. Bu hash algoritması, yeni yaratılan sertifika isteğiyle ilişkilendirilmiş imzayı yaratmak için kullanılır. The value can be `md5`, `MD5_WITH_RSA`, `MD5WithRSA`, `SHA_WITH_DSA`, `SHA_WIT_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`. Varsayılan değer `SHA1WithRSA`' dır.

-san_dnsname *DNS_ads*
Yaratılmakta olan girişle ilgili DNS adlarının virgülle sınırlanmış ya da boşlukla ayrılmış listesini belirtir.

-san_emailaddr *email_adress*
Yaratılmakta olan girişe ilişkin e-posta adreslerinin virgülle sınırlanmış ya da boşlukla ayrılmış bir listesini belirtir.

-san_ipaddr *IP_adresleri*
Yaratılmakta olan girişle ilgili IP adreslerinin virgülle sınırlanmış ya da boşlukla ayrılmış listesini belirtir.

Sonraki adım

Sertifika isteği (CA) için gönderin. Ek bilgi için "Kişisel sertifikaların UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna alınması" sayfa 288 ' e bakın.

ULW *UNIX, Linux, and Windowsüzerinde var olan bir kişisel sertifikana ilişkin yenileme*

You can renew a personal certificate by using the **strmqikm** (iKeyman) GUI, or from the command line using the **runmqckm** (iKeycmd) or **runmqakm** (GSKCapiCmd) commands.

Bu görev hakkında

Kişisel sertifikalarınız için daha büyük anahtar boyutları kullanma zorunluluğunuz varsa, var olan bir sertifikayı yenileyemezsiniz. Gereksinim duyduğunuz anahtar boyutlarını kullanan yeni bir sertifika isteği oluşturmak için, “UNIX, Linux, and Windows üzerinde kişisel sertifika isteme” sayfa 284 içinde açıklanan adımları izleyerek var olan anahtarınızı değiştirmeniz gerekir.

Kişisel sertifikanda bir süre bitim tarihi vardır ve bu tarihten sonra sertifikanda kullanılabilir. Bu görev, var olan bir kişisel sertifikanının süresi dolmadan önce nasıl yenileneceğini açıklar.

***strmqikm** kullanıcı arabirimini kullanma*

Bu görev hakkında

strmqikm , FIPS uyumlu bir seçenek sunmaz. TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Yordam

strmqikm kullanıcı arabirimini kullanarak kişisel bir sertifika için geçerli olmak üzere aşağıdaki adımları tamamlayın:

1. UNIX, Linux, and Windowsüzerinde **strmqikm** komutunu kullanarak kullanıcı arabirimini başlatın.
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın.
   Aç penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. İsteğiniz oluşturmak istediğiniz anahtar veritabanı dosyasını seçin; örneğin, `key.kdb`.
6. **Aç**'ı tıklatın.
   Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın.
   Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında gösterilir.
8. Açılan seçim menüsünden **Kişisel sertifikalar** seçeneğini belirleyin ve yenilemek istediğiniz listeden sertifikayı seçin.
9. **İsteği Yeniden Oluştur ...**düğmesini tıklatın. emin olun.
   Dosya adı ve dosya konumu bilgilerini girmeniz için bir pencere açılır.
10. **Dosya adı** alanında, varsayılan `certreq.arm`değerini kabul edin ya da tam dosya yolu da içinde olmak üzere yeni bir değer yazın.
11. **Tamam**'ı tıklatın. Sertifika isteği, “9” sayfa 287adımında seçtiğiniz dosyada saklanır.
12. Yeni kişisel sertifikayı, dosyayı sertifika yetkilisine (CA) göndererek ya da dosyayı CA için web sitesindeki istek formuna kopyalayarak isteyin.

Komut satırını kullanma

Yordam

Use the following commands to request a personal certificate by using either the **runmqckm** or **runmqakm** command:

- Using **runmqckm** on UNIX, Linux, and Windows systems:

```
runmqckm -certreq -recreate -db filename -pw
password -label label
-target filename
```

- runmqakm komutunu kullanarak:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
-target filename
```

Burada:

-db *kütükadı*
Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirtir.

-pw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

-target *kütükadı*
Sertifika isteğine ilişkin dosya adını belirler.

Sonraki adım

Sertifika yetkilisinden imzalanmış kişisel sertifikayı aldıktan sonra, “Kişisel sertifikaların UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna alınması” sayfa 288içinde açıklanan adımları kullanarak bunu anahtar veritabanınıza ekleyebilirsiniz.

ULW *Kişisel sertifikaların UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna alınması*

Anahtar veri tabanı dosyasına kişisel bir sertifika almak için bu yordamı kullanın. Anahtar havuzu, sertifika isteğini oluşturduğunuz havuzla aynı olmalıdır.

CA, size yeni bir kişisel sertifika gönderdikten sonra, yeni sertifika isteğini oluşturduğunuz anahtar veritabanı dosyasına ekliyorsunuz. CA, sertifikayı bir e-posta iletisinin bir parçası olarak gönderirse, sertifikayı ayrı bir dosyaya kopyalayın.

Kullanılan **strmqikm**

TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** , FIPS uyumlu bir seçenek sunmaz.

İçe aktarılacak sertifika dosyasının geçerli kullanıcı için yazma iznine sahip olduğundan emin olun ve daha sonra, anahtar veritabanı dosyasına kişisel bir sertifika almak için kuyruk yöneticisi ya da IBM MQ MQI client için aşağıdaki yordamı kullanın:

1. Start the GUI using the **strmqikm** command (on Windows UNIX and Linux).
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı eklemek istediğiniz anahtar veritabanı dosyasını seçin (örneğin, key . kdb).
6. **Aç**'ı ve sonra **Tamam**' ı tıklatın. Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir. **Kişisel Sertifikalar** görünümünü seçin.
8. **Al**düğmesini tıklatın. Bir Dosya penceresindeki Sertifika Al penceresi açılır.
9. Yeni kişisel sertifikana ilişkin sertifika dosyası adını ve yerini yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.

10. **Tamam** düğmesini tıklatın. Anahtar veri tabanınızda zaten kişisel bir sertifikanız varsa, bir pencere açılır ve veritabanında varsayılan anahtar olarak eklemediğiniz anahtarı ayarlamak isteyip istemediğinizi soran bir pencere açılır.
11. **Evet** ya da **Hayır**' ı tıklatın. Bir Etiket Girin penceresi açılır.
12. **Tamam** düğmesini tıklatın. **Kişisel Sertifikalar** alanı, eklediğiniz yeni kişisel sertifikana ilişkin etiketi gösterir.

Komut satırını kullanma

Bir anahtar veritabanı dosyasına kişisel sertifika eklemek için aşağıdaki komutlardan birini kullanın:

- **runmqckm**komutunu kullanma:

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

- **runmqakm**komutunu kullanma:

```
runmqakm -cert -receive -file filename -db filename -pw password -fips
```

Burada:

-file *kütükadı*
Kişisel sertifikana ilişkin tam olarak nitelenmiş dosya adını belirler.

-db *kütükadı*
Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirtir.

-pw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

-format *ascii*
Sertifikana ilişkin biçimi belirler. The value can be `ascii` for Base64-encoded ASCII or `binary` for Binary DER data. Varsayılan değer `ascii`' dir.

-fips.
Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

Şifreleme donanımı kullanıyorsanız, “PKCShardwaredonanımınıza kişisel bir sertifika alma” sayfa 303' a bakın.

ULW *Extracting a CA certificate from a key repository on UNIX, Linux, and Windows*

CA sertifikasını almak için bu yordamı izleyin.

Kullanılan `strmqikm`

TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** (iKeyman) FIPS uyumlu bir seçenek sunmaz.

CA sertifikasını almak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. Start the GUI using the **strmqikm** command..
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Ayıklamak istediğiniz anahtar veritabanı dosyasını seçin; örneğin, `key.kdb`.
6. **Aç**düğmesini tıklatın. Parola İstemi penceresi açılır.

7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. **Anahtar veritabanı içeriği** alanında **İmzalayıcı Sertifikaları** öğesini seçin ve almak istediğiniz sertifikayı seçin.
9. **Çıkar**' ı tıklatın. Bir Sertifikayı Dosya Aç penceresi açılır.
10. Sertifikenin **Veri tipi** değerini seçin; örneğin, `.arm` uzantılı bir dosya için **Base64-encoded ASCII verileri** .
11. Sertifikayı saklamak istediğiniz sertifika dosyası adını ve yerini yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
12. **Tamam** düğmesini tıklatın. Sertifika, belirttiğiniz kütükaya yazılır.

Komut satırını kullanma

Bir CA sertifikasını **runmqckm**kullanarak çıkarmak için aşağıdaki komutları kullanın:

- UNIX, Linux, and Windows'ta:

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

Burada:

`-db` *filename*	CMS anahtar veri tabanının tam olarak nitelenmiş yol adıdır.
`-pw` *password*	CMS anahtar veri tabanının parolasıdır.
`-label` *label*	sertifikaya eklenen etikettir.
`-target` *filename*	hedef dosyanın adıdır.
`-format` *ascii*	sertifikının biçimidir. The value can be `ascii` for Base64-encoded ASCII or `binary` for Binary DER data. Varsayılan değer `ascii`' dir.
`-fips`	Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

ULW *Extracting the public part of a self-signed certificate from a key repository on UNIX, Linux, and Windows*

Kendinden onaylı sertifikana ilişkin genel bölümü çıkarmak için bu yordamı izleyin.

Kullanılan `strmqikm`

TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** (iKeyman) FIPS uyumlu bir seçenek sunmaz.

Kendinden imzalı bir sertifikana ilişkin genel kısmını çıkarmak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. Start the GUI using the **strmqikm** command (on UNIX, Linux, and Windows).
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı almak istediğiniz anahtar veritabanı dosyasını seçin (örneğin, `key.kdb`).
6. **Tamam** düğmesini tıklatın. Parola İstemi penceresi açılır.

7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. **Anahtar veritabanı içeriği** alanında, **Kişisel Sertifikalar** ' ı seçin ve sertifikayı seçin.
9. **Sertifika çek**' i tıklatın. Bir Sertifikayı Dosya Aç penceresi açılır.
10. Sertifikenin **Veri tipi** değerini seçin; örneğin, `.arm` uzantılı bir dosya için **Base64-encoded ASCII verileri** .
11. Sertifikayı saklamak istediğiniz sertifika dosyası adını ve yerini yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
12. **Tamam** düğmesini tıklatın. Sertifika, belirttiğiniz kütükaya yazılır. Bir sertifikayı çıkardığınızda (dışa aktarma yerine), sertifikana yalnızca genel bir kısmı dahil edildiğine dikkat edin; bu nedenle bir parola gerekmez.

Komut satırını kullanma

Use the following commands to extract the public part of a self-signed certificate using **runmqckm** or **runmqakm**:

- UNIX, Linux, and Windows'ta:

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

- runmqakm komutunu kullanarak:

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

Burada:

`-db` *filename*	CMS anahtar veri tabanının tam olarak nitelenmiş yol adıdır.
`-pw` *password*	CMS anahtar veri tabanının parolasıdır.
`-label` *label*	sertifikaya eklenen etikettir.
`-target` *filename*	hedef dosyanın adıdır.
`-format` *ascii*	sertifikının biçimidir. The value can be `ascii` for Base64-encoded ASCII or `binary` for Binary DER data. Varsayılan değer `ascii`' dir.
`-fips`	Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

ULW *Adding a CA certificate, or the public part of a self-signed certificate, into a key repository on UNIX, Linux, and Windows*

Bir sertifika kuruluşu (CA) sertifikası ya da kendinden imzalı sertifikana ilişkin genel kısmı anahtar havuzuna eklemek için bu yordamı izleyin.

Eklemek istediğiniz sertifika bir sertifika zincirinde varsa, zincirin üstünde olan tüm sertifikaları da eklemeniz gerekir. Sertifikaları kökten başlayarak kesinlikle alçalan düzende eklemeniz gerekir; ardından, CA sertifikası zincirin hemen altında, vb. olarak da aşağıdan başlayarak, sertifika eklemelisiniz.

Aşağıdaki yönergelerin bir CA sertifikasına başvurduğu durumlarda, bu sertifikalar kendi kendine imzalanmış bir sertifikana ilişkin genel kısım için de geçerlidir.

Not: Sertifikenin ASCII (UTF-8) ya da ikili (DER) kodlamalarında olduğundan emin olmalısınız; IBM Global Secure Toolkit (GSKit), diğer kodlama türleriyle sertifikaları desteklememektedir.

Kullanılan `strmqikm`

TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** , FIPS uyumlu bir seçenek sunmaz.

CA sertifikasını eklemek istediğiniz makine üzerinde aşağıdaki adımları gerçekleştirin:

1. Start the GUI using the **strmqikm** command (on UNIX, Linux and Windows systems).
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı eklemek istediğiniz anahtar veritabanı dosyasını seçin (örneğin, `key.kdb`).
6. **Tamam** düğmesini tıklatın. Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. **Anahtar veritabanı içeriği** alanında **İmzalayıcı Sertifikaları**öğesini seçin.
9. **Ekle**düğmesini tıklatın. Bir Dosyadan CA Sertifikası Ekle penceresi açılır.
10. Sertifika dosyası adını ve sertifikenin saklandığı yeri yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
11. **Tamam** düğmesini tıklatın. Bir Etiket Girin penceresi açılır.
12. Enter a Label (Etiket Gir) penceresinde sertifikenin adını yazın.
13. **Tamam** düğmesini tıklatın. Sertifika, anahtar veritabanına eklenir.

Komut satırını kullanma

Anahtar veri tabanına bir CA sertifikası eklemek için aşağıdaki komutlardan birini kullanın:

- **runmqckm**komutunu kullanma:

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

- **runmqakm**komutunu kullanma:

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

Burada:

-db *kütükadı*
CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirtir.

-pw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

-label *etiket*
Sertifikaya ekli olan etiketi belirtir.

-file *kütükadı*
Sertifikayı içeren dosyanın adını belirtir.

-format *ascii*
Sertifikana ilişkin biçimi belirler. The value can be `ascii` for Base64-encoded ASCII or `binary` for Binary DER data. Varsayılan değer `ascii`' dir.

-fips.
Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

ULW *Kişisel bir sertifikayı UNIX, Linux, and Windowsüzerindeki bir anahtar havuzundan dışa aktarma*

Kişisel bir sertifikayı dışa aktarmak için bu yordamı izleyin.

Kullanılan `strmqikm`

TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** (iKeyman) FIPS uyumlu bir seçenek sunmaz.

Kişisel sertifikayı dışa aktarmak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. Start the GUI using the **strmqikm** command (on Windows UNIX and Linux).
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı dışa aktarmak istediğiniz anahtar veritabanı dosyasını seçin (örneğin, `key.kdb`).
6. **Aç**düğmesini tıklatın. Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. **Anahtar veritabanı içeriği** alanında, **Kişisel Sertifikalar** ' ı seçin ve dışa aktarmak istediğiniz sertifikayı seçin.
9. **Dışa Aktar/İçe Aktar**' ı tıklatın. Dışa Aktar/İçe Aktar tuşu penceresi açılır.
10. **Anahtarı Dışa Aktar**seçeneğini belirleyin.
11. Dışa aktarmak istediğiniz sertifikana ilişkin **Anahtar dosyası tipi** değerini seçin; örneğin, **PKCS12**.
12. Sertifikayı dışa aktarmak istediğiniz dosya adını ve yeri yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
13. **Tamam** düğmesini tıklatın. Parola İstemi penceresi açılır. Bir sertifikayı dışa aktardığınızda (çıkarmak yerine) sertifikana ilişkin genel ve özel bölümlerin de içerileceğini unutmayın. Bu, dışa aktarılan dosyanın parolayla korunmasının nedeni. Bir sertifikayı çıkardığınızda, sertifikana yalnızca genel bir kısmı dahil edilir, bu nedenle bir parola gerekmez.
14. **Parola** alanına bir parola yazın ve **Parolayı Onayla** alanına parolayı yeniden yazın.
15. **Tamam** düğmesini tıklatın. Sertifika, belirttiğiniz kütükaya aktarılır.

Komut satırını kullanma

Use the following commands to export a personal certificate using **runmqckm**:

- UNIX, Linux, and Windows'ta:

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

Burada:

`-db filename`	CMS anahtar veri tabanının tam olarak nitelenmiş yol adıdır.
`-fips`	Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.
`-pw password`	CMS anahtar veri tabanının parolasıdır.
`-label label`	sertifikaya eklenen etikettir.
`-type cms`	Veritabanı tipidir.

`-target` *filename*	hedef dosyanın tam olarak nitelenmiş yol adıdır.
`-target_pw` *password*	Sertifikayı şifrelemek için kullanılan paroladır.
`-target_type` *pkcs12*	Sertifikenin tipidir.

ULW *Kişisel bir sertifikin UNIX, Linux, and Windowsüzerindeki bir anahtar havuzuna aktarılması*

Kişisel bir sertifikayı içe aktarmak için bu yordamı izleyin

Kişisel bir sertifikayı PKCS #12 biçiminde anahtar veritabanı dosyasına aktarmadan önce, anahtar veritabanı dosyasına (bkz. “Adding a CA certificate, or the public part of a self-signed certificate, into a key repository on UNIX, Linux, and Windows” sayfa 291) izin veren CA sertifikalarının tam olarak geçerli bir zincirini eklemelisiniz.

PKCS #12 dosyaları, kullanıldıktan sonra geçici olarak dikkate alınmalı ve silinmelidir.

Kullanılan `strmqikm`

TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın. **strmqikm** , FIPS uyumlu bir seçenek sunmaz.

Kişisel sertifikayı içe aktarmak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. **strmqikm** komutunu kullanarak GUI ' yi başlatın.
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi görüntülenir.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı eklemek istediğiniz anahtar veritabanı dosyasını seçin (örneğin, key . kdb).
6. **Aç**'ı tıklatın. Parola İstemi penceresi görüntülenir.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. **Anahtar veritabanı içeriği** alanında **Kişisel Sertifikalar**öğesini seçin.
9. Kişisel Sertifikalar görünümünde sertifikalar varsa, aşağıdaki adımları izleyin:
   a. **Dışa Aktar/İçe Aktar**' ı tıklatın. Dışa Aktar/İçe Aktar tuşu penceresi görüntülenir.
   b. **Anahtarı İçe Aktar**seçeneğini belirleyin.
10. Kişisel Sertifikalar görünümünde sertifika yoksa, **İçe Aktar**düğmesini tıklatın.
11. İçe aktarmak istediğiniz sertifikana ilişkin **Anahtar dosya tipi** ' ne (örneğin PKCS12) seçin.
12. Sertifika dosyası adını ve sertifikenin saklandığı yeri yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
13. **Tamam**'ı tıklatın. Parola İstemi penceresi görüntülenir.
14. **Parola** alanına, sertifika dışa aktarıldığında kullanılan parolayı yazın.
15. **Tamam**'ı tıklatın. Etiketleri Değiştir penceresi görüntülenir. İçe aktarılmakta olan sertifikaların etiketlerini değiştirebilirsiniz (örneğin, hedef anahtar veritabanında aynı etikete sahip bir sertifika zaten var). Sertifika etiketlerinin değiştirilmesi, sertifika zinciri doğrulaması üzerinde bir etki göstermez. To associate the certificate with a particular queue manager or IBM MQ MQI client, IBM MQ uses either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or IBM MQ MQI client user logon ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.
16. Bir etiketi değiştirmek için, **Değiştirmek için bir etiket seçin** listesinden gerekli etiketi seçin. Etiket, **Yeni bir etiket girin** giriş alanına kopyalanır. Etiket metnini yeni etiketle değiştirin ve **Uygula**' yı tıklatın.

17. **Yeni bir etiket girin** giriş alanındaki metin, özgün olarak seçilen etiketin yerine **Değiştirmek için bir etiket seçin** alanına geri kopyalanır ve böylece ilgili sertifikayı yeniden aktarır.
18. Değiştirilmesi gereken tüm etiketleri değiştirdiğinizde **Tamam**düğmesini tıklatın. Etiketleri Değiştir penceresi kapanır ve özgün IBM Key Management penceresi **Kişisel Sertifikalar** ve **İmzalayıcı Sertifikalar** alanlarında doğru etiketlenmiş sertifikalarla birlikte yeniden görüntülenir.
19. Sertifika, hedef anahtar veritabanına içe aktarılır.

Komut satırını kullanma

Kişisel bir sertifikayı **runmqckm**komutunu kullanarak içe aktarmak için aşağıdaki komutu kullanın:

- UNIX, Linux, and Windows'ta:

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

Burada:

`-file filename`	PKCS #12 sertifikasını içeren dosyanın tam olarak nitelenmiş dosya adıdır.
`-pw password`	PKCS #12 sertifikasının parolasıdır.
`-type pkcs12`	Dosyanın tipidir.
`-target filename`	hedef CMS anahtar veri tabanının adıdır.
`-target_pw password`	CMS anahtar veri tabanının parolasıdır.
`-target_type cms`	`-target`tarafından belirtilen veritabanının tipidir
`-label label`	Kaynak anahtar veritabanından içe aktarılacak sertifikana ilişkin etikettir.
`-new_label label`	Sertifikanının hedef veritabanında atanacağı etikettir. `-new_label` seçeneğini çıkarırsanız, varsayılan değer `-label` seçeneğiyle aynı işlevi kullanmaktadır.
`-fips`	Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

runmqckm , sertifika etiketlerini doğrudan değiştirmek için bir komut sunmaz. Bir sertifika etiketini değiştirmek için aşağıdaki adımları kullanın:

1. Sertifikayı **-cert -export** komutunu kullanarak bir PKCS #12 dosyasına aktarın. `-label` seçeneği için var olan sertifika etiketini belirtin.
2. Remove the existing copy of the certificate from the original key database using the **-cert -delete** command.
3. **-cert -import** komutunu kullanarak, sertifikayı PKCS #12 kütüğünden içe aktarın. `-label` seçeneği için eski etiketi ve `-new_label` seçeneği için gereken yeni etiketi belirtin. Sertifika, gerekli etiketle birlikte anahtar veritabanına geri aktarılır.

ULW *Bir Microsoft.pfx dosyasından kişisel bir sertifikun içe aktarılması*

UNIX, Linux, and Windowsüzerindeki bir Microsoft.pfx dosyasından içe aktarmak için bu yordamı izleyin.

Bir .pfx dosyası, aynı anahtarla ilgili iki sertifika içerebilir. Biri kişisel ya da site sertifikasıdır (hem genel, hem de özel anahtar içerir). Diğeri, CA (imzalayıcı) sertifikasıdır (yalnızca bir genel anahtar içerir). Bu sertifikalar aynı CMS anahtar veritabanı dosyasında birlikte bulunamaz, bu nedenle yalnızca biri içe aktarılabilir. Ayrıca, "kullanımı kolay ad" ya da etiket yalnızca imzalayıcı sertifikasına eklenir.

Kişisel sertifika, sistem tarafından oluşturulan Benzersiz Kullanıcı Tanıtıcısı (UUID) ile tanımlanır. Bu bölümde, daha önce CA (signer) sertifikasına atanmış olan kullanımı kolay adla etiketlerken, bir pfx

dosyasından kişisel sertifikana ilişkin içe aktarma bilgileri gösterilir. Sertifika veren CA (signer) sertifikaları hedef anahtar veritabanına önceden eklenmelidir. PKCS#12 dosyalarının kullanıldıktan sonra geçici olarak kabul edilmesi ve silinmeleri gerektiğini unutmayın.

Kişisel bir sertifikayı kaynak pfx anahtar veritabanından içe aktarmak için aşağıdaki adımları izleyin:

1. **strmqikm** komutunu kullanarak GUI ' yi başlatın. IBM Key Management (Anahtar Yönetimi) penceresi görüntülenir.
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi görüntülenir.
3. **PKCS12**anahtar veritabanı tipi seçin.
4. **Bu adımı gerçekleştirmeden önce, pfx veritabanının yedeğini almak için önerildiniz.** İçe aktarmak istediğiniz pfx anahtar veri tabanını seçin. **Aç**düğmesini tıklatın. Password Prompt (Parola İstemi) penceresi görüntülenir.
5. Anahtar veritabanı parolasını girin ve **Tamam**düğmesini tıklatın. IBM Key Management (Anahtar Yönetimi) penceresi görüntülenir. Başlık çubuğu, dosyanın açık ve hazır olduğunu gösteren seçili pfx anahtar veritabanı dosyasının adını gösterir.
6. Listeden **İmzalayıcı Sertifikaları** öğesini seçin. Gerekli sertifikana ilişkin "kullanımı kolay ad", İmzalayıcı Sertifikaları panosunda bir etiket olarak görüntülenir.
7. Etiket girdisini seçin ve imzalayanın sertifikasını kaldırmak için **Sil** düğmesini tıklatın. Confirm (Doğrulama) penceresi görüntülenir.
8. **Evet**düğmesini tıklatın. Seçilen etiket artık İmzalayıcı Sertifikalar panosunda görüntülenmiyor.
9. İmzalayan tüm sertifikalar için 6, 7 ve 8 numaralı adımları yineleyin.
10. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi görüntülenir.
11. pfx dosyasının içe aktarılmakta olduğu hedef anahtar CMS veritabanını seçin. **Aç**düğmesini tıklatın. Password Prompt (Parola İstemi) penceresi görüntülenir.
12. Anahtar veritabanı parolasını girin ve **Tamam**düğmesini tıklatın. IBM Key Management (Anahtar Yönetimi) penceresi görüntülenir. Başlık çubuğu, dosyanın açık ve hazır olduğunu belirten, seçilen anahtar veritabanı dosyasının adını gösterir.
13. Listeden **Kişisel Sertifikalar** öğesini seçin.
14. Kişisel Sertifikalar görünümünde sertifikalar varsa, aşağıdaki adımları izleyin:
    a. **Dışa/İçe Aktar anahtarı**öğesini tıklatın. Dışa Aktar/İçe Aktar tuşu penceresi görüntülenir.
    b. İşlem Tipi Seç içinden **İçe Aktar** seçeneğini belirleyin.
15. Kişisel Sertifikalar görünümünde sertifika yoksa, **İçe Aktar**düğmesini tıklatın.
16. PKCS12 dosyasını seçin.
17. Pfx dosyasının adını Adım 4 'te kullanılan şekilde girin. **Tamam** düğmesini tıklatın. Password Prompt (Parola İstemi) penceresi görüntülenir.
18. İmzalayıcı sertifikasını sildiğinizde belirttiğiniz parolayı belirtin. **Tamam** düğmesini tıklatın.
19. Etiketleri Değiştir penceresi görüntülenir (içe aktarmak için yalnızca tek bir sertifika olması gerektikçe). The label of the certificate should be a UUID which has a format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.
20. To change the label select the UUID from the **Değiştirmek için bir etiket seçin:** panel. Etiket **Enter a new label:** (Yeni etiket girin:) alanına kopyalanır. Etiket metnini, Adım 7 'de silinen kullanımı kolay addan değiştirin ve **Uygula**' yı tıklatın. The friendly name must be either the value of the IBM MQ **CERTLABL** attribute, if it is set, or the default ibmwebspheremq with the name of the queue manager or IBM MQ MQI client user logon ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.
21. **Tamam** düğmesini tıklatın. Etiketleri Değiştir penceresi kaldırılır ve özgün IBM Anahtar Yönetimi penceresi Kişisel Sertifikalar ve İmzalayıcı Sertifikalar panolarıyla birlikte yeniden görüntülenir ve bu pencerelerle birlikte kişisel sertifika doğru olarak etiketlenir.

22. pfx kişisel sertifikası artık (hedef) veritabanına içe aktarılmaktadır.

Bir sertifika etiketinin **runmqckm** ya da **runmqakm**kullanılarak değiştirilmesi mümkün değildir.

Komut satırını kullanma

To import a personal certificate using **runmqckm** on UNIX, Linux, and Windows, use the following command:

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

Kişisel bir sertifikayı **runmqakm**komutunu kullanarak içe aktarmak için aşağıdaki komutu kullanın:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips -pfx
```

Burada:

`-file` *filename*	PKCS #12 sertifikasını içeren dosyanın tam olarak nitelenmiş dosya adıdır.
`-pw` *password*	PKCS #12 sertifikasının parolasıdır.
`-type` *pkcs12*	Dosyanın tipidir.
`-target` *filename*	hedef CMS anahtar veri tabanının adıdır.
`-target_pw` *password*	CMS anahtar veri tabanının parolasıdır.
`-target_type` *cms*	`-target`tarafından belirtilen veritabanının tipidir
`-label` *label*	Kaynak anahtar veritabanından içe aktarılacak sertifikana ilişkin etikettir.
`-new_label` *label*	Sertifikanının hedef veritabanında atanacağı etikettir. `-new_label` seçeneğini çıkarırsanız, varsayılan değer `-label` seçeneğiyle aynı işlevi kullanmaktadır.
`-fips`	Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.
`-pfx`	PFX dosya biçimini belirtir.

runmqckm , sertifika etiketlerini doğrudan değiştirmek için bir komut sunmaz. Bir sertifika etiketini değiştirmek için aşağıdaki adımları kullanın:

1. Sertifikayı **-cert -export** komutunu kullanarak bir PKCS #12 dosyasına aktarın. `-label` seçeneği için var olan sertifika etiketini belirtin.
2. Remove the existing copy of the certificate from the original key database using the **-cert -delete** command.
3. **-cert -import** komutunu kullanarak, sertifikayı PKCS #12 kütüğünden içe aktarın. `-label` seçeneği için eski etiketi ve `-new_label` seçeneği için gereken yeni etiketi belirtin. Sertifika, gerekli etiketle birlikte anahtar veritabanına geri aktarılır.

ULW *PKCS #7 dosyasından kişisel bir sertifikun içe aktarılması*

strmqikm (iKeyman) ve **runmqckm** (iKeycmd) araçları, PKCS #7 (`.p7b`) özelliğini desteklemez. Dosyalar. Use the **runmqckm** tool to import certificates from a PKCS #7 file on UNIX, Linux, and Windows.

Bir PKCS #7 kütüğünden bir CA sertifikası eklemek için aşağıdaki komutu kullanın:

```
runmqckm -cert -add -db filename -pw password -type cms -file filename
-label label
```

`-db` *filename*	CMS anahtar veri tabanının tam olarak nitelenmiş dosya adıdır.
`-pw` *password*	Anahtar veri tabanının parolasıdır.
`-type` *cms*	Anahtar veri tabanının tipidir.
`-file` *filename*	PKCS #7 dosyasının adıdır.
`-label` *label*	Sertifikanının hedef veritabanında atandığı etikettir. İlk sertifika verilen etiketi alır. Diğer tüm sertifikalar (varsa), konu adlarıyla etiketlenir.

Bir PKCS #7 kütüğünden kişisel bir sertifikayı içe aktarmak için aşağıdaki komutu kullanın:

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

`-db` *filename*	PKCS #7 sertifikasını içeren dosyanın tam olarak nitelenmiş dosya adıdır.
`-pw` *password*	PKCS #7 sertifikasının parolasıdır.
`-type` *pkcs7*	Dosyanın tipidir.
`-target` *filename*	hedef anahtar veri tabanının adıdır.
`-target_pw` *password*	Hedef anahtar veri tabanının parolasıdır.
`-target_type` *cms*	`-target`tarafından belirtilen veritabanının tipidir
`-label` *label*	İçe aktarılacak sertifikana ilişkin etikettir.
`-new_label` *label*	Sertifikanının hedef veritabanında atanacağı etikettir. `-new_label` seçeneğini çıkarırsanız, varsayılan değer, `-label` seçeneğiyle aynı işlevi kullanmaktadır.

ULW *UNIX, Linux, and Windowsüzerindeki bir anahtar havuzundan sertifika silme*

Kişisel ya da CA sertifikalarını kaldırmak için bu yordamı kullanın.

Kullanılan `strmqikm`

TLS sertifikalarını FIPS uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqakm** komutunu kullanın. **strmqikm** (iKeyman) FIPS uyumlu bir seçenek sunmaz.

1. Start the GUI using the **strmqikm** command (on UNIX, Linux, and Windows).
2. **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın. Open (Aç) penceresi açılır.
3. **Anahtar veritabanı tipi** seçeneğini tıklatın ve **CMS** (Sertifika Yönetimi Sistemi) seçeneğini belirleyin.
4. Anahtar veritabanı kütüklerini içeren dizine gitmek için **Göz At** düğmesini tıklatın.
5. Sertifikayı silmek istediğiniz anahtar veritabanı dosyasını seçin (örneğin, `key.kdb`).
6. **Aç**düğmesini tıklatın. Parola İstemi penceresi açılır.
7. Anahtar veri tabanını yaratırken ayarladığınız parolayı yazın ve **Tamam**düğmesini tıklatın. Anahtar veri tabanı dosyanızın adı, **Dosya Adı** alanında görüntülenir.
8. Açılan listeden **Kişisel Sertifikalar** ya da **İmzalayıcı Sertifikaları**öğesini seçin.
9. Silmek istediğiniz sertifikayı seçin.
10. Sertifikana ilişkin bir kopyaınız yoksa ve kaydetmek istiyorsanız, **Dışa Aktar/İçe Aktar** seçeneğini tıklatın ve dışa aktarın (bkz. “Kişisel bir sertifikayı UNIX, Linux, and Windowsüzerindeki bir anahtar havuzundan dışa aktarma” sayfa 293).
11. Sertifika seçilip **Sil**düğmesini tıklatın. Onayla penceresi açılır.
12. **Evet**düğmesini tıklatın. **Kişisel Sertifikalar** alanı artık sildiğiniz sertifikana ilişkin etiketi göstermiyor.

Komut satırını kullanma

runmqckmkullanarak bir sertifikayı silmek için aşağıdaki komutları kullanın:

- UNIX, Linux, and Windows'ta:

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

Burada:

-db *filename*	CMS anahtar veri tabanının tam olarak nitelenmiş dosya adıdır.
-pw *password*	CMS anahtar veri tabanının parolasıdır.
-label *label*	kişisel sertifikan ' a bağlı olan etikettir.
-fips	Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

ULW *UNIX, Linux, and Windowsüzerinde anahtar havuzu koruması için güçlü parolalar oluşturma*

Anahtar havuzu koruması için **runmqakm** (GSKCapiCmd) komutunu kullanarak güçlü parolalar oluşturabilirsiniz.

Güçlü bir parola oluşturmak için **runmqakm** komutunu aşağıdaki değiştirgelerle birlikte kullanabilirsiniz:

```
runmqakm -random -create -length 14 -strong -fips
```

Sonraki sertifika yönetimi komutlarının **-pw** parametresinde oluşturulan parolayı kullanırken, parolayı her zaman çift tırnak işareti içine alın. UNIX and Linux sistemlerinde, parola dizgisinde görüntülenmeleri durumunda, aşağıdaki karakterlerden kurtulmak için bir ters eğik çizgi karakteri de kullanmanız gerekir:

```
! \ " '
```

When entering the password in response to a prompt from **runmqckm**, **runmqakm** or the **strmqikm** GUI then it is not necessary to quote or escape the password. İşletim sistemi kabuğu bu vakalardaki veri girişini etkilmediği için bu gerekli değildir.

ULW *UNIX, Linux, and Windowsüzerinde şifreleme donanımı için yapılandırma*

Bir kuyruk yöneticisine ya da istemciye ilişkin şifreleme donanımını bir dizi şekilde yapılandırabilirsiniz.

Aşağıdaki yöntemlerden birini kullanarak UNIX, Linux, and Windows üzerinde bir kuyruk yöneticisi için şifreleme donanımını yapılandırabilirsiniz:

- Use the ALTER QMGR MQSC command with the SSLCRYP parameter, as described in ALTER QMGR.
- UNIX, Linux ya da Windows sisteminizdeki şifreleme donanımını yapılandırmak için IBM MQ Explorer 'ı kullanın. Ek bilgi için çevrimiçi yardıma bakın.

Aşağıdaki yöntemlerden birini kullanarak UNIX, Linux, and Windows üzerinde bir IBM MQ istemcisi için şifreleme donanımı yapılandırabilirsiniz:

- MQSSLCRYP ortam değişkenini ayarlayın. MQSSLCRYP için izin verilen değerler, ALTER QMGRiçinde açıklandığı gibi, SSLCRYP parametresiyle aynı olur.

  SSLCRYP parametresinin GSK_PKCS11 sürümünü kullanırsanız, PKCS #11 belirteci etiketi donanımınızı yapılandırdığınız etiketle eşleşmelidir.
- MQCONNX çağrısında SSL yapılanış seçenekleri yapısının (MQSCO) **CryptoHardware** alanını ayarlayın. Ek bilgi için bkz. Overview for MQSCO.

Bu yöntemlerden herhangi birini kullanarak PKCS #11 arabirimini kullanan şifreleme donanımını yapılandırdıysanız, kişisel sertifikayı yapılandırdığınız şifreleme simgesine ilişkin anahtar veri tabanı dosyasında bulunan kanallarınızda kullanmak üzere saklamanız gerekir. Bu, “PKCS #11 donanımlarındaki sertifikaları yönetme” sayfa 300içinde açıklanmaktadır.

PKCS #11 donanımlarındaki sertifikaları yönetme

PKCS #11 arabirimini destekleyen şifreleme donanımlarıyla ilgili dijital sertifikaları yönetebilirsiniz.

Bu görev hakkında

You must create a key database to prepare the IBM MQ environment, even if you do not intend to store certificate authority (CA) certificates in it, but will store all your certificates on your cryptographic hardware. Anahtar veritabanı, kuyruk yöneticisi için SSLKEYR alanına gönderme yapmak ya da istemci uygulamasının MQSSLKEYR ortam değişkenine gönderme yapmak için gereklidir. Bu anahtar veri tabanı, bir sertifika isteği yaratıyorsanız da gereklidir.

Anahtar veritabanını, komut satırını kullanarak ya da **strmqikm** (iKeyman) kullanıcı arabirimini kullanarak yaraladınız.

Yordam

Komut satırını kullanarak bir anahtar veritabanı yaratın.

1. Aşağıdaki komutlardan birini çalıştırın:
   - **runmqckm**komutunu kullanma:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - **runmqakm**komutunu kullanma:

     ```
     runmqakm -keydb -create -db filename -pw password -type cms
     -stash -fips -strong
     ```

   Burada:

   -db *kütükadı*
   Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirler ve `.kdb`dosya uzantısına sahip olmalıdır.

   -pw *parola*
   CMS anahtar veri tabanına ilişkin parolayı belirtir.

   -type *cms*
   Veri tabanının tipini belirtir. (IBM MQiçin, `cms`olmalıdır.)

   -stash
   Anahtar veritabanı parolasını bir dosyaya kaydeder.

   -fips.
   Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

   -Güçlü
   Girilen parolanın, parola güvenlik düzeyi için gereken minimum gereksinimleri karşıladığını denetler. Bir parolaya ilişkin minimum gereksinimler aşağıdaki gibidir:

   - Parola en az 14 karakter uzunluğunda olmalıdır.
   - Parola, en az bir küçük harf, bir büyük harf ve bir rakam ya da özel karakter içermelidir. Özel karakterler, yıldız işareti (*), dolar işareti ($), sayı işareti (#) ve yüzde işareti (%) içerir. Boşluk, özel karakter olarak sınıflandırılır.
   - Her karakter, bir parolada en çok üç kez oluşabilir.

- Parolada art arda en çok iki karakter aynı olabilir.
- Tüm karakterler standart ASCII yazdırılabilir karakter takımında, 0x20 - 0x7Earalığında yer alıyor.

Diğer bir seçenek olarak, **strmqikm** (iKeyman) kullanıcı arabirimini kullanarak bir anahtar veritabanı yaratın.

2. UNIX and Linux sistemlerinde, kök kullanıcı olarak oturum açın. Windows sistemlerinde, Yönetici olarak ya da MQM grubunun bir üyesi olarak oturum açın.
3. Java güvenlik özellikleri dosyasını (`java.security`) açın.
   - UNIX and Linux sistemlerinde, Java güvenlik özellikleri dosyası, IBM MQ kuruluş dizininin `java/jre64/jre/lib/security` alt dizininde bulunur.
   - Windows sistemlerinde, Java güvenlik özellikleri dosyası, IBM MQ kuruluş dizininin `java\jre\lib\security` alt dizininde bulunur.

   Dosyada önceden mevcut değilse, IBMPKCS11Impl güvenlik sağlayıcısını ekleyin. Örneğin, aşağıdaki satırı ekleyin:

   ```
   security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
   ```
4. **strmqikm** komutunu çalıştırarak kullanıcı arabirimini başlatın.
5. **Anahtar Veritabanı Dosyası** > **Aç**öğelerini tıklatın.
6. **Anahtar veritabanı tipi** öğesini tıklatın ve **PKCS11Direct**öğesini seçin.
7. **File Name** (Dosya Adı) alanına, şifreleme donanımınızı yönetmek için modülün adını yazın; örneğin, `PKCS11_API.so`.

   PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.
8. **Konum** alanına yolu girin:
   - UNIX and Linux sistemlerinde bu `/usr/lib/pksc11`olabilir, örneğin.
   - Windows sistemlerinde, kitaplık adını yazabilirsiniz; örneğin, `cryptoki`.

   Tamam'ı tıklatın. Açık Şifreleme Simgesi penceresi açılır.
9. Sertifikaları saklamak için kullanmak istediğiniz şifreleme aygıtı belirteci etiketini seçin.
10. **Cryptographic Token Password** (Şifreleme Aygıtı Parolası) alanında, şifreleme donanımını yapılandırdığınızda ayarladığınız parolayı yazın.
11. Şifreleme donanımınızda kişisel bir sertifikayı almak ya da içe aktarmak için gerekli imzalayıcı sertifikalarını tutma kapasitesi varsa, hem ikincil anahtar veritabanı onay kutularını temizleyin, hem de “15” sayfa 302adımından devam edin.

    İmzalayıcı sertifikalarını tutmak için ikincil bir CMS anahtar veritabanı gerekiyorsa, **Var olan ikincil anahtar veritabanı dosyasını aç** ya da **Yeni ikincil anahtar veritabanı dosyası yarat**seçeneğini belirleyin.
12. **File Name** (Dosya Adı) alanına bir dosya adı yazın. Bu alan `key.kdb`metnini zaten içeriyor. Kök adınız `key`ise, bu alanı değiştirmeden bırakın. Farklı bir kök adı belirtdiyseniz, `key` yerine kök adınızı koyun. `.kdb` sonekini değiştirmemelisiniz.
13. **Konum** alanına yolu yazın, örneğin:
    - Kuyruk yöneticisi için: `/var/mqm/qmgrs/QM1/ssl`
    - IBM MQ MQI clientiçin: `/var/mqm/ssl`

    Tamam'ı tıklatın. Parola İstemi penceresi açılır.
14. Bir parola girin.

"11" sayfa 301adımında **Var olan ikincil anahtar veritabanı dosyasını aç** seçeneğini belirlediyseniz, **Parola** alanına bir parola yazın.

"11" sayfa 301adımında **Yeni ikincil anahtar veritabanı dosyası yarat** seçeneğini belirlediyseniz, aşağıdaki alt adımları tamamlayın:

a) **Parola** alanına bir parola yazın ve **Parolayı Onayla** alanına parolayı yeniden yazın.

b) **Parola bir dosyaya göre stash**seçeneğini belirleyin. Parolayı saklamadıysanız, anahtar veritabanı dosyasına erişmek için gereken parolayı elde edemedikleri için TLS kanallarını başlatma girişimleri başarısız olur.

c) **Tamam**'ı tıklatın. Parolanın `key.sth` dosyasında olduğunu onaylayan bir pencere açılır (farklı bir kök adı belirtmediyseniz).

15. **Tamam**'ı tıklatın. Key veritabanı içerik çerçevesi görüntülenir.

ULW *PKCS #11 donanımınıza ilişkin kişisel bir sertifika istenmesi*

Şifreleme donanımınıza ilişkin kişisel bir sertifika istemek için kuyruk yöneticisi ya da IBM MQ MQI client için bu yordamı kullanın.

Bu görev hakkında

Bu görev, kişisel bir sertifika istemek için **strmqikm** kullanıcı arabirimini nasıl kullandığınızı açıklar. Komut satırı arabirimini kullanıyorsanız, bkz. "Komut satırını kullanma" sayfa 285.

Not: IBM MQ , SHA-3 ya da SHA-5 algoritmalarını desteklemez. You can use the digital signature algorithm names SHA384WithRSA and SHA512WithRSA because both algorithms are members of the SHA-2 family.

The digital signature algorithm names SHA3WithRSA and SHA5WithRSA are deprecated because they are an abbreviated form of SHA384WithRSA and SHA512WithRSA respectively.

Yordam

To request a personal certificate from the **strmqikm** (iKeyman) user interface, complete the following steps:

1. Şifreleme donanımınızla çalışmaya ilişkin adımları tamamlayın. Bkz. "PKCS #11 donanımlarındaki sertifikaları yönetme" sayfa 300.
2. **Yarat** menüsünden **Yeni Sertifika İsteği**öğesini tıklatın.

   Yeni Anahtar Yarat ve Sertifika İsteği Oluştur penceresi açılır.
3. **Key Label** (Anahtar Etiketi) alanına sertifika etiketini girin.

   The label is either the value of the **CERTLABL** attribute, if it is set, or the default `ibmwebspheremq` with the name of the queue manager or IBM MQ MQI client logon user ID appended, all in lowercase. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.
4. Gereksinim duyduğunuz **Anahtar Boyutu** ve **İmza Algoritması** ' ı seçin.
5. **Common Name** (Ortak Ad) ve **Organization**(Kuruluş) değerlerini girin ve bir **Country**(Ülke) seçin. Kalan isteğe bağlı alanlar için, varsayılan değerleri kabul edin ya da yeni değerleri yazın ya da seçin.

   Kuruluş Birimi alanında yalnızca bir ad sağlayabileceğiniz dikkat edin. Bu alanlarla ilgili daha fazla bilgi için bkz. "Belirleyici Adlar" sayfa 11.
6. **Sertifika isteği saklanacak bir dosyanın adını girin** alanında, varsayılan `certreq.arm`değerini kabul edin ya da tam yolu olan yeni bir değer yazın.
7. **Tamam**'ı tıklatın.

   Bir doğrulama penceresi açılır.
8. **Tamam**'ı tıklatın.

   Kişisel Sertifika İstekleri listesinde, yarattığınız yeni kişisel sertifika isteğinin etiketi gösterilir. Sertifika isteği, "6" sayfa 302adımında seçtiğiniz dosyada saklanır.

9. Yeni kişisel sertifikayı, dosyayı sertifika yetkilisine (CA) göndererek ya da dosyayı CA için web sitesindeki istek formuna kopyalayarak isteyin.

ULW *PKCShardwaredonanımınıza kişisel bir sertifika alma*

Şifreleme donanımınıza kişisel bir sertifika almak için kuyruk yöneticisi ya da IBM MQ MQI client için bu yordamı kullanın.

Başlamadan önce

Kişisel sertifikayı imzalayan CA ' nın sertifika kuruluşu (CA) sertifikasını ekleyin. Bunu şifreleme donanımını ya da ikincil CMS anahtar veri tabanına ekleyin. Bu işlemi, imzalanmış sertifikayı şifreleme donanımına almadan önce yapın. Bir anahtar halkasına CA sertifikası eklemek için, “Adding a CA certificate, or the public part of a self-signed certificate, into a key repository on UNIX, Linux, and Windows” sayfa 291içindeki yordamı izleyin.

Yordam

- To receive a personal certificate using the **strmqikm** (iKeyman) user interface, complete the following steps:
  a) Şifreleme donanımınızla çalışmaya ilişkin adımları tamamlayın. Bkz. “PKCS #11 donanımlarındaki sertifikaları yönetme” sayfa 300.
  b) **Al**düğmesini tıklatın. Bir Dosya penceresindeki Sertifika Al penceresi açılır.
  c) Yeni kişisel sertifikana ilişkin sertifika dosyası adını ve yerini yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
  d) **Tamam**'ı tıklatın. Anahtar veritabanınızda zaten kişisel bir sertifikanız varsa, bir pencere açılır ve eklemediğiniz anahtarı, veritabanında varsayılan anahtar olarak ayarlamak isteyip istemediğiniz sorularak görüntülenir.
  e) **Evet** ya da **Hayır**' ı tıklatın. Bir Etiket Girin penceresi açılır.
  f) **Tamam**'ı tıklatın. **Kişisel Sertifikalar** listesi, eklediğiniz yeni kişisel sertifikana ilişkin etiketi gösterir. Bu etiket, belirttiğiniz etiketten önce şifreleme belirteci etiketi eklenerek oluşturulur.
- To receive a personal certificate using the **runmqakm** (GSKCapiCmd) command, complete the following steps:
  a) Ortamınız için yapılandırılmış bir komut penceresi açın.
  b) Kişisel sertifikayı **runmqakm** (GSKCapiCmd) komutunu kullanarak alın:

```
runmqakm -cert -receive -file filename -crypto module_name
         -tokenlabel hardware_token -pw hardware_password
         -format cert_format -fips
         -secondaryDB filename -secondaryDBpw password
```

  Burada:

  -file *kütükadı*
  Kişisel sertifikayı içeren dosyanın tam olarak nitelenmiş dosya adını belirtir.

  -crypto *module_name*
  Şifreleme donanımıyla birlikte sağlanan PKCS #11 kitaplığının tam olarak nitelenmiş adını belirtir.

  -tokenlabel *hardware_belirteci*
  PKCScryptographicşifreleme aygıtı belirteci etiketini belirtir.

  -pw *parola_parolası*
  Şifreleme donanıma erişmek için kullanılacak parolayı belirtir.

  -format *cert_format*
  Sertifikana ilişkin biçimi belirler. The value can be `ascii` for Base64-encoded ASCII or `ikili` for binary DER data. Varsayılan değer ASCII 'dir.

-fips.
Komutun FIPS kipinde çalıştırıldığını belirtir. FIPS kipindeki ICC bileşeni, FIPS 140-2 olarak doğrulanan algoritmaları kullanır. ICC bileşeni FIPS kipinde kullanıma hazırlanmazsa, **runmqakm** komutu başarısız olur.

-secondaryDB *dosyaadı*
CMS anahtar veri tabanının tam olarak nitelenmiş dosya adını belirtir.

-secondaryDBpw *parola*
CMS anahtar veri tabanına ilişkin parolayı belirtir.

MQ Appliance IBM MQ Applianceüzerinde SSL/TLS ile çalışma

IBM MQ Appliance , Transport Layer Security (TLS) desteğine sahiptir.

IBM MQ Appliance , sertifikaları yönetmek için ayrı komutlara sahiptir. Sertifika yönetimiyle ilgili ayrıntılı bilgi için IBM MQ Appliance belgelerine, TLS sertifika yönetiminebakın.

z/OS z/OSüzerinde SSL/TLS ile çalışma

This information describes how you set up and work with Transport Layer Security (TLS) on z/OS.

Her konu, her bir görevi RACFkullanarak gerçekleştirmeye ilişkin örnekleri içerir. Diğer dış güvenlik yöneticilerini kullanarak benzer görevleri gerçekleştirebilirsiniz.

z/OS'ta, her kuyruk yöneticisinin TLS çağrılarını işlemek için kullandığı sunucu alt görevlerinin sayısını “z/OSüzerinde SSLASKS parametresinin ayarlanması” sayfa 305' da açıklandığı şekilde ayarlamanız gerekir.

z/OS TLS desteği, işletim sisteminin ayrılmaz bir parçasıdır ve *Sistem SSL*olarak bilinir. System SSL is part of the Cryptographic Services Base element of z/OS. Cryptographic Services Base üyeleri *pdsname*' a kurulur. SIEALNKE bölümlenmiş veri kümesi (PDS). Sistem SSL 'i kurduğunuzda, gereksinim duyduğunuz CipherSpecs ' i sağlamak için uygun seçenekleri seçmeye dikkat edin.

z/OS *z/OSüzerinde TLS için ek kullanıcı kimliği gereksinimleri*

This information describes the additional requirements your user ID needs to set up and work with TLS on z/OS.

Sisteminizde tüm uygun Yüksek Etki ya da Saldırgan (HIPER) güncellemelerinin tümüne sahip olduğundan emin olun.

Aşağıdaki önkoşulları ayarladığınızdan emin olun:

- *ssidCHIN* kullanıcı kimliği, RACFiçinde doğru olarak tanımlıdır ve *ssidCHIN* kullanıcı kimliğinin aşağıdaki tanıtımlara okuma erişimi vardır:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

  Bu değişkenler, RACF FACILITY Sınıfı 'nda tanımlanır.
- *ssidCHIN* kullanıcı kimliği, anahtar halkasının sahibidir.
- The personal certificate of the queue manager, if created by the RACDCERT command, is created with a certificate type user ID that is also the same as the *ssidCHIN* user ID.
- The channel initiator is recycled, or the command **REFRESH SECURITY TYPE(SSL)** is issued, to pick up any changes you make to the key ring.
- IBM MQ Channel Initiator yordamsa, bağlantı listesi, LPA ya da STEPLIB DD deyimi aracılığıyla sistem SSL çalıştırma zamanı kitaplığına *pdsname*.IEALNKE erişimine sahip olur. Bu kitaplığın APF yetkisi olması gerekir.
- Kanal başlatıcı yetkisine sahip olan kullanıcı kimliği, z/OS UNIX System Services Planning belgelerinde açıklandığı gibi, UNIX System Services (USS) olanağını kullanacak şekilde yapılandırılır.

  Kanal başlatıcısının guest/default UID ve OMVS kesimini kullanarak UNIX System Services olanağını başlatmasını istemeyen kullanıcılar, kanal başlatıcı için özel izin gerektirmediği için varsayılan kesime

dayalı olarak yeni bir OMVS kesiminin modeline gereksinim duyar ve ayrıcalıklı kullanıcı olarak UNIX içinde çalışmaz.

z/OS *z/OSüzerinde SSLASKS parametresinin ayarlanması*

TLS çağrılarının işlenmesine ilişkin sunucu alt görevi sayısını ayarlamak için ALTER QMGR komutunu kullanın.

TLS kanallarını kullanmak için, ALTER QMGR komutunu kullanarak SSLASKS parametresini ayarlayarak en az iki sunucu alt görevi olduğundan emin olun. Örneğin:

```
ALTER QMGR SSLTASKS(5)
```

Depolama ayırması ile ilgili sorunları önlemek için SSLTASKS özniteliğini, CRL (Certificate Revocation List; Sertifika İptal Listesi) denetiminin olmadığı bir ortamda sekizden daha büyük bir değere ayarlamayın.

CRL denetimi kullanılırsa, kanal tarafından denetmenin süresi boyunca bir SSLTASK tutulur. Her bir SSLTASK bir z/OS görev denetim bloğu olduğu için, ilgili LDAP sunucusu ile iletişim kurulabilirken bu, önemli bir geçen süre için olabilir.

SSLASKS özniteliğinin değerini değiştirirseniz, kanal başlatıcıyı yeniden başlatmanız gerekir.

z/OS *z/OSüzerinde bir anahtar havuzu ayarlanıyor*

Bağlantının her iki ucunda da bir anahtar havuzu ayarlayın. Her bir anahtar havuzunu kuyruk yöneticisiyle ilişkilendirin.

TLS bağlantısı, bağlantının her iki ucunda bir *anahtar havuzu* gerektirir. Her kuyruk yöneticisinin bir anahtar havuzuna erişimi olması gerekir. Bir anahtar havuzunu bir kuyruk yöneticisiyle ilişkilendirmek için ALTER QMGR komutundaki SSLKEYR parametresini kullanın. Ek bilgi için “SSL/TLS anahtarı havuzu” sayfa 23 başlıklı konuya bakın.

z/OSüzerinde, sayısal sertifikalar, Dış Güvenlik Yöneticiniz (ESM) tarafından yönetilen bir *anahtarlık* içinde saklanır. Bu sayısal sertifikalar, sertifikayı kuyruk yöneticisiyle ilişkilendiren etiketlere sahiptir. TLS, kimlik doğrulama amacıyla bu sertifikaları kullanır. All the examples that follow use RACF commands. Diğer ESM programları için eşdeğer komutlar vardır.

On z/OS, IBM MQ uses either the value of the **CERTLABL** attribute, if it is set, or the default `ibmWebSphereMQ` with the name of the queue manager appended. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

Kuyruk yöneticisine ilişkin anahtar havuzu adı, RACF veritabanınızdaki bir anahtarlık adıdır. Anahtarlık adını yaratmadan önce ya da sonra anahtar halkası yaratıldıktan sonra belirleyebilirsiniz.

Kuyruk yöneticisi için yeni bir anahtarlık yaratmak üzere aşağıdaki yordamı kullanın:

1. RACDCERT komutunu vermek için gereken yetkiye sahip olup olmadığınızı denetleyin (ayrıntılı bilgi için *SecureWay Security Server RACF Command Language Reference* adlı belgelere bakın).
2. Şu komutu verin:

   ```
   RACDCERT ID( userid1 ) ADDRING( ring-name )
   ```

   Burada:

   - *userid1* , kanal başlatıcı adres alanının kullanıcı kimliğidir ya da anahtarlık (anahtar halkası paylaşılıyorsa) kendisine ait olan kullanıcı kimliğine sahip olur.
   - *halka-adı* , anahtarlık anahtarınıza vermek istediğiniz addır. Bu adın uzunluğu 237 karaktere kadar çıkabilmektedir. Bu ad, büyük ve küçük harfe duyarlıdır. Sorunları önlemek için büyük harfli karakterler içinde *halka-adı* değerini belirtin.

z/OS *CA sertifikalarının z/OSüzerinde bir kuyruk yöneticisi tarafından kullanılabilmesini sağlar*

Anahtarınızı yarattıktan sonra, ilgili CA sertifikalarını buna bağlayın.

Bir veri kümesinde CA sertifikasına sahipseniz, aşağıdaki komutu kullanarak sertifikayı RACF veritabanına eklemeniz gerekir:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Daha sonra, My CA için bir CA sertifikasını anahtarlık anahtarınıza bağlamak için aşağıdaki komutu kullanın:

```
RACDCERT ID(userid1)
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

Burada *userid1* , kanal başlatıcı kullanıcı kimliği ya da paylaşılan anahtar halkasının sahibi olur.

CA sertifikalarıyla ilgili daha fazla bilgi için “dijital sertifikalar” sayfa 9' e bakın.

z/OS *z/OSüzerinde bir kuyruk yöneticisine ilişkin anahtar havuzunun bulunması*

Kuyruk yöneticinizin anahtar halkasının yerini almak için bu yordamı kullanın.

1. Aşağıdaki MQSC komutlarından birini kullanarak kuyruk yöneticinizin özniteliklerini görüntüleyin:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

2. Anahtar halkasının yeri için komut çıkışını inceleyin.

z/OS *z/OSüzerinde bir kuyruk yöneticisi için anahtar havuzu yerini belirtme*

Kuyruk yöneticinizin anahtar halkasının yerini belirtmek için, kuyruk yöneticinizin anahtar havuzu özniteliğini ayarlamak için ALTER QMGR MQSC komutunu kullanın.

Örneğin:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

anahtar halkası kanal başlatıcı adres alanına aitse, ya da:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

Paylaşılan anahtar halkaysa, burada *userid1* anahtar halkasının sahibi olan kullanıcı kimliğidir.

z/OS *Kanal başlatıcı, z/OSüzerinde doğru erişim haklarını veriyor*

Kanal başlatıcı (CHINIT), anahtar havuzu ve bazı güvenlik profillerine erişmeye gerek duyar.

Anahtar havuzu okumak için CHINIT erişimi verilmesi

Anahtar havuzu CHINIT kullanıcı kimliğine aitse, bu kullanıcı kimliğinin IRR.DIGTCERT.LISTRING tanıtımı ve tersi durumda erişimi güncelleyin. ERMIT komutunu ACCESS (UPDATE) ya da ACCESS (READ) ile uygun olarak kullanarak erişim verin:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
```

Burada *kullanıcı kimliği* , kanal başlatıcı adres alanının kullanıcı kimliğidir.

Uygun CSF* tanıtımlarına CHINIT okuma erişimi verilmesi

Kullanılacak Integrated Cryptographic Service Facility (ICSF) aracılığıyla sağlanan donanım desteği için, aşağıdaki komutu kullanarak, CHINIT kullanıcı kimliğinizin CSFSERV sınıfındaki uygun CSF* tanıtımlarına okuma erişimine sahip olduğunu doğrulayın:

```
PERMIT csf-resource CLASS(CSFSERV) ID( userid ) ACCESS(READ)
```

Burada *csf-resource* , CSF* profilinin adı ve *userid* , kanal başlatıcı adres alanının kullanıcı kimliğidir.

Aşağıdaki CSF* tanıtımlarının her biri için bu komutu yineleyin:

- CFDSG
- CFDSV
- CFPKT
- CFPKE
- CSFPKI

CHINIT kullanıcı kimliğinizin diğer CSF* tanıtımlarına okuma erişimi de gerekebilir. Örneğin, ECDHE_RSA_AES_256_GCM_SHA384 Cipher Spec kullanıyorsanız, CHINIT kullanıcı kimliğinizin aşağıdaki CSF* profillerine okuma erişimi de gerekir:

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC
- CSF1TRD

Ek bilgi için RACF CSFSERV kaynak gereksinmeleribaşlıklı konuya bakın.

Sertifika anahtarlarınız ICSF 'de saklanırsa ve kuruluşunuz, ICSF' de saklanan anahtarlar üzerinde erişim denetimi oluşturduysa, aşağıdaki komutu kullanarak, CHINIT kullanıcı kimliğinizin CSFKEYS sınıfındaki tanıtıma okuma erişimi olduğunu doğrulayın:

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

Burada *kullanıcı kimliği* , kanal başlatıcı adres alanının kullanıcı kimliğidir.

Integrated Cryptographic Service Facility (ICSF) olanağının kullanılması

Kanal başlatıcı, TLS kullanılmıyorsa, istemci kanallarının üzerinden akan parolaların karartılması için parola koruma algoritmasını görürken rasgele bir sayı oluşturmak için ICSF ' yi kullanabilir.

Daha fazla bilgi için bkz. “Integrated Cryptographic Service Facility (ICSF) olanağının kullanılması” sayfa 251

z/OS *Sertifikalar üzerindeki değişiklikler ya da anahtar havuzu z/OSüzerinde etkili olduğunda*

Kanal başlatıcı başlatıldığında ya da havuz yenilendiğinde değişiklikler etkili olur.

Özellikle, anahtar halkasındaki sertifikalarda ve anahtar havuzu özniteliğinin üzerinde yapılan değişiklikler aşağıdaki durumlarda yürürlüğe girer:

- Kanal başlatıcı başlatıldığında ya da yeniden başlatıldığında.
- Anahtar havuzunun içeriğini yenilemek için REFRESH SECURITY TYPE (SSL) komutu verildiğinde.

z/OS z/OSüzerinde kendinden onaylı bir kişisel sertifika oluşturma

Kendinden onaylı bir kişisel sertifika yaratmak için bu yordamı kullanın.

1. Aşağıdaki komutu kullanarak bir sertifika ve bir genel ve özel anahtar çifti oluşturun:

```
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. Aşağıdaki komutu kullanarak sertifikayı anahtarlık anahtarınıza bağlayın:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

Burada:

- *userid1* , kanal başlatıcı adres alanının ya da paylaşılan anahtar halkasının sahibinin kullanıcı kimliğidir.
- *userid2* , sertifikayla ilişkilendirilen kullanıcı kimliğidir ve kanal başlatıcı adres alanının kullanıcı kimliği olmalıdır.

  userid1 ve *userid2* aynı tanıtıcıya sahip olabilir.
- *halka-adı* , “z/OSüzerinde bir anahtar havuzu ayarlanıyor” sayfa 305' ta anahtar halkasına verdiğiniz addır.
- *etiket-adı* must be either the value of the IBM MQ **CERTLABL** attribute, if it is set, or the default `ibmWebSphereMQ` with the name of the queue manager appended. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

z/OS z/OSüzerinde kişisel sertifika isteme

RACFkullanarak kişisel bir sertifika için başvurun.

Kişisel bir sertifika başvurmak için, RACF seçeneğini aşağıdaki gibi kullanın:

1. “z/OSüzerinde kendinden onaylı bir kişisel sertifika oluşturma” sayfa 308' de olduğu gibi kendinden onaylı bir kişisel sertifika oluşturun. Bu sertifika, Ayırt Edici Ad için öznitelik değerleri ile istek sağlar.
2. Aşağıdaki komutu kullanarak bir veri kümesine yazılan bir PKCS #10 Base64-encoded sertifika isteği yaratın:

```
RACDCERT ID(userid2) GENREQ(LABEL(' label_name ')) DSN(' output_data_set_name ')
```

   burada:

   - *userid2* , sertifikayla ilişkilendirilen kullanıcı kimliğidir ve kanal başlatıcı adres alanının kullanıcı kimliği olmalıdır.
   - *label_name* , kendinden onaylı sertifika yaratılırken kullanılan etikettir.

   Ayrıntılar için bkz. “Dijital sertifika etiketleri, gereksinimleri anlama” sayfa 25.
3. Yeni bir kişisel sertifika istemek için, veri kümesini bir Sertifika Yetkilisi 'ne (CA) gönderin.
4. İmzalanmış sertifika Sertifika Yetkilisi tarafından size geri verildiğinde, sertifikayı özgün etiketi kullanarak RACF veritabanına geri ekleyin (“Kişisel sertifikaların z/OSüzerindeki bir anahtar havuzuna eklenmesi” sayfa 309içinde açıklandığı gibi).

z/OS RACF imzalı kişisel sertifika yaratılması

RACF , sertifika yetkilisi olarak işlev görebilirler ve kendi CA sertifikasını yayınlayabilir.

Bu bölüm, RACFtarafından yayınlanan bir CA sertifikasını göstermek için *imzalayıcı sertifikası* terimini kullanır.

Aşağıdaki yordamı gerçekleştirmeden önce imzalayıcı sertifikasının özel anahtarının RACF veritabanında olması gerekir:

1. Use the following command to generate a personal certificate signed by RACF, using the signer certificate contained in your RACF database:

```
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. Aşağıdaki komutu kullanarak sertifikayı anahtarlık anahtarınıza bağlayın:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

Burada:

- *userid1* , kanal başlatıcı adres alanının ya da paylaşılan anahtar halkasının sahibinin kullanıcı kimliğidir.
- *userid2* , sertifikayla ilişkilendirilen kullanıcı kimliğidir ve kanal başlatıcı adres alanının kullanıcı kimliği olmalıdır.

  userid1 ve *userid2* aynı tanıtıcıya sahip olabilir.
- *halka-adı* , “z/OSüzerinde bir anahtar havuzu ayarlanıyor” sayfa 305' ta anahtar halkasına verdiğiniz addır.
- *etiket-adı* must be either the value of the IBM MQ **CERTLABL** attribute, if it is set, or the default `ibmWebSphereMQ` with the name of the queue manager or queue sharing group appended. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.
- *signer-label* , kendi imzalayıcı sertifikanızı etiketlemektedir.

z/OS *Kişisel sertifikaların z/OSüzerindeki bir anahtar havuzuna eklenmesi*

Bir anahtar halkasına kişisel sertifika eklemek ya da bu sertifikayı içe aktarmak için bu yordamı kullanın.

Sertifika yetkilisi size yeni bir kişisel sertifika gönderdikten sonra, aşağıdaki yordamı kullanarak anahtarı anahtarlık 'a ekleyin:

1. Aşağıdaki komutu kullanarak sertifikayı RACF veritabanına ekleyin:

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. Aşağıdaki komutu kullanarak sertifikayı anahtarlık anahtarınıza bağlayın:

```
RACDCERT ID( userid1 )
CONNECT(ID( userid2 ) LABEL(' label-name ') RING( ring-name ) USAGE(PERSONAL))
```

Burada:

- *userid1* , kanal başlatıcı adres alanının ya da paylaşılan anahtar halkasının sahibinin kullanıcı kimliğidir.
- *userid2* , sertifikayla ilişkilendirilen kullanıcı kimliğidir ve kanal başlatıcı adres alanının kullanıcı kimliği olmalıdır.

- *halka-adı* , “z/OSüzerinde bir anahtar havuzu ayarlanıyor” sayfa 305' ta anahtar halkasına verdiğiniz addır.
- *input-data-set-name* , CA imzalanmış sertifikayı içeren veri kümesinin adıdır. Veri kümesi kataloğa alınmalı ve PDS ya da PDS üyesi olmamalıdır. RCDCERT tarafından beklenen kayıt biçimi (RECFM) VB ' dir. RCDCERT, veri kümesini dinamik olarak ayırır ve açar ve sertifikayı bu verileri ikili veri olarak okur.
- *etiket-adı* , özgün isteği yarattığınızda kullanılan etiket adıdır. Bu değer, IBM MQ **CERTLABL** özniteliğinin değeri, ayarlandıysa ya da kuyruk yöneticisi ya da kuyruk paylaşım grubu adının sonuna eklenen varsayılan `ibmWebSphereMQ` olmalıdır. Ayrıntılı bilgi için Dijital sertifika etiketleri başlıklı konuya bakın.

z/OS *Kişisel bir sertifikayı z/OSüzerindeki bir anahtar havuzundan dışa aktarma*

RACDCERT komutunu kullanarak sertifikayı dışa aktarın.

Sertifikayı dışa aktarmak istediğiniz sistemde şu komutu kullanın:

```
RACDCERT ID(userid2) EXPORT(LABEL('label-name'))
DSN(output-data-set-name) FORMAT(CERTB64)
```

Burada:

- *userid2* , sertifikana anahtar halkasına eklendiği kullanıcı kimliğidir.
- *label-name* , almak istediğiniz sertifikana ilişkin etikettir.
- *çıkış-veri-kümesi-adı* , sertifikanının yerleştirileceği veri kümesidir.
- CERTB64 , Base64 biçiminde olan bir DER kodlamalı X.509 sertifikasıdır. Alternatif bir biçim seçebilirsiniz, örneğin:

  CERTDER
  DER kodlamalı X.509 sertifikası ikili biçimde kodlandı

  PKCS12B64
  PKCS #12 sertifikası Base64 biçiminde

  PKCS12DER
  PKCS #12 sertifikası ikili biçimde

z/OS *Kişisel sertifikının z/OSüzerindeki bir anahtar havuzundan silinmesi*

RCDCERT komutunu kullanarak kişisel bir sertifikayı silin.

Kişisel bir sertifikayı silmeden önce, dosyanın bir kopyasını saklamak isteyebilirsiniz. Kişisel sertifikanızı, silmeden önce bir veri kümesine kopyalamak için, “Kişisel bir sertifikayı z/OSüzerindeki bir anahtar havuzundan dışa aktarma” sayfa 310içindeki yordamı izleyin. Daha sonra kişisel sertifikanızı silmek için aşağıdaki komutu kullanın:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

Burada:

- *userid2* , sertifikana anahtar halkasına eklendiği kullanıcı kimliğidir.
- *etiket-adı* , silmek istediğiniz sertifikana ilişkin addır.

z/OS *z/OSüzerindeki bir anahtar havuzundaki kişisel sertifikanının yeniden adlandırılması*

RACDCERT komutunu kullanarak bir sertifikayı yeniden adlandırın.

Belirli bir etiketin bulunduğu bir sertifika istemezseniz, ancak bunu silmek istemiyorsanız, aşağıdaki komutu kullanarak geçici olarak yeniden adlandırabilirsiniz:

```
RACDCERT ID( userid2 ) LABEL(' label-name ') NEWLABEL(' new-label-name ')
```

Burada:

- *userid2* , sertifikana anahtar halkasına eklendiği kullanıcı kimliğidir.
- *etiket-adı* , yeniden adlandırmak istediğiniz sertifikana ilişkin addır.
- *new-label-name* , sertifikenin yeni adıdır.

TLS istemcisi kimlik doğrulaması test edildiğinde bu yararlı olabilir.

z/OS *Associating a user ID with a digital certificate on z/OS*

IBM MQ , bir RACF sertifikasıyla ilişkili bir kullanıcı kimliğini, kanal kullanıcı kimliği olarak kullanabilir. Bir kullanıcı kimliğini, bu kullanıcı kimliğinin altına kurarak ya da bir Sertifika Adı Süzgeci kullanarak bir sertifikaya sahip olarak ilişkilendirin.

Bu konuda açıklanan yöntem, kullanıcı kimliğini, kanal doğrulama kayıtlarını kullanan bir sayısal sertifikayla ilişkilendirmek için platformdan bağımsız bir yönteme alternatif bir yöntemdir. Kanal kimlik doğrulama kayıtlarıyla ilgili daha fazla bilgi için bkz. “Kanal doğrulama kayıtları” sayfa 47.

When an entity at one end of a TLS channel receives a certificate from a remote connection, the entity asks RACF if there is a user ID associated with that certificate. Varlık, bu kullanıcı kimliğini kanal kullanıcı kimliği olarak kullanır. Sertifikayla ilişkilendirilmiş bir kullanıcı kimliği yoksa, varlık, kanal başlatıcısının altında çalıştığı kullanıcı kimliğini kullanır.

Bir kullanıcı kimliğini, aşağıdaki yöntemlerden birini kullanarak bir sertifikayla ilişkilendirin:

- Install that certificate into the RACF database under the user ID with which you want to associate it, as described in “Kişisel sertifikaların z/OSüzerindeki bir anahtar havuzuna eklenmesi” sayfa 309.
- Use a Certificate Name Filter (CNF) to map the Distinguished Name of the subject or issuer of the certificate to the user ID, as described in “z/OSüzerinde bir sertifika adı süzgecinin ayarlanması” sayfa 311.

z/OS *z/OSüzerinde bir sertifika adı süzgecinin ayarlanması*

Bir Ayırt Edici Adı bir kullanıcı kimliğiyle eşleyen bir sertifika adı süzgeci (CNF) tanımlamak için RACDCERT komutunu kullanın.

CNF oluşturmak için aşağıdaki adımları gerçekleştirin.

1. Aşağıdaki komutu kullanarak CNF işlevlerini etkinleştirin. Bu işlemi yapmak için, DIGTNMAP sınıfı üzerinde güncelleme yetkisine gerek duyarsınız.

   ```
   SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
   ```

2. CNF ' yi tanımlayın. Örneğin:

   ```
   RACDCERT ID(USER1) MAP WITHLABEL('filter1') TRUST
   SDNFILTER('O=IBM.C=UK') IDNFILTER('O=ExampleCA.L=Internet')
   ```

   Burada USER1 , aşağıdaki durumlarda kullanılacak kullanıcı kimliğidir:

   - Konunun ayırt edici adı (DN) `IBM` ve Country of UK(Ülke) adlı bir Kurulumuna sahiptir.
   - The DN of the issuer has an Organization of `ExampleCA` and a Locality of `Internet`.

3. CNF eşlemelerini yenileyin:

   ```
   SETROPTS RACLIST(DIGTNMAP) REFRESH
   ```

Not:

1. Gerçek sertifika RACF veritabanında saklandıysa, kurulu olduğu kullanıcı kimliği, herhangi bir CNF ile ilişkili kullanıcı kimliğine tercihte kullanılır. Sertifika RACF veritabanında saklanmazsa, en özel eşleşen CNF ile ilişkilendirilmiş kullanıcı kimliği kullanılır. Konu DN 'nin eşleşmeleri, sertifika veren DN' nin eşleşmelerinden daha özel olarak kabul edilir.

2. CNF ' lerde yapılan değişiklikler, CNF eşlemelerini yenilinceye kadar geçerli olmaz.
3. DN, yalnızca DN süzgeci, DN ' nin *en az önemli bölümü* ile aynı olduğunda, CNF içindeki DN süzgeciyle eşleşir. Ayırt edici adın en az önemli bölümü, genellikle ayırt edici adın en sonunda yer alan, ancak sertifikenin başında yer alan özniteliklerden oluşur.

   Örneğin, SDNFILTER `'O=IBM.C=UK''`ı göz önünde bulundurun. A subject DN of `'CN=QM1.O=IBM.C=UK'` matches that filter, but a subject DN of `'CN=QM1.O=IBM.L=Hursley.C=UK'` does not match that filter.

   Bazı sertifikaların en az önemli bölümü, DN süzgeciyle eşleşmeyen alanlar içerebilir. DEFINE CHANNEL komutundaki SSLPEER örüntüünde bir DN kalıbı belirleyerek bu sertifikaları dışlamayı göz önünde bulundurun.
4. CNF ile eşleşen en özel değer, RACF olarak NOTRUST olarak tanımlandıysa, varlık, kanal başlatıcının altında çalıştığı kullanıcı kimliğini kullanır.
5. RACF uses the `'.'` character as a separator. IBM MQ , virgül ya da noktalı virgül kullanır.

Varlığın kanal kullanıcı kimliğini varsayılan değere ayarlamamasını sağlamak için CNF ' leri tanımlayabilirsiniz; bu, kanal başlatıcının altında çalıştığı kullanıcı kimliğidir. Varlıkla ilişkili anahtar halkasındaki her CA sertifikası için, o CA sertifikasının konu DN ' siyle tam olarak eşleşen bir IDNFILTER ile bir CNF tanımlayın. Bu, varlığın kullanabileceği tüm sertifikaların bu CNF ' lerden en az biri ile eşleşmesini sağlar. Bunun nedeni, tüm bu sertifikaların varlıkla ilişkili anahtarlık anahtarına bağlanması ya da bir sertifikenin varlıkla ilişkili anahtarlık için bir CA tarafından verilmesi gerekir.

CNF ' leri işlemek için kullandığınız komutlarla ilgili ek bilgi için *SecureWay Security Server RACF Security Administrator's Guide* adlı yayına bakın.

z/OS *z/OSüzerindeki QMA ' da bir gönderen kanalı ve iletim kuyruğu tanımlama*

Gerekli nesneleri ayarlamak için **DEFINE CHANNEL** ve **DEFINE QLOCAL** komutlarını kullanın.

Yordam

QMA ' da, aşağıdaki örnek gibi komutlar verin:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Sender channel using TLS from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

Sonuçlar

Bir gönderen kanalı (TO.QMBve bir iletim kuyruğu (QMB) yaratılır.

z/OS *z/OSüzerinde QMB ' de bir alıcı kanalı tanımlama*

Gerekli nesneyi ayarlamak için **DEFINE CHANNEL** komutunu kullanın.

Yordam

QMB ' de aşağıdaki örnek gibi bir komut yayınlayın:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS to QMB')
```

Sonuçlar

Bir alıcı kanalı, TO.QMB, yaratılır.

z/OS *Starting the sender channel on QMA on z/OS*

Gerekiyorsa, bir dinleyici programı başlatın ve güvenliği yenileyin. Then start the channel using the **START CHANNEL** command.

Yordam

1. İsteğe bağlı: Henüz yapmadıysanız, QMB ' de bir dinleyici programı başlatın.

   Dinleyici programı gelen ağ isteklerini dinler ve gerektiğinde alıcı kanalını başlatır. Bir dinleyicinin nasıl başlatılacağı hakkında bilgi için Kanal dinleyicisi başlatmabaşlıklı konuya bakın.
2. İsteğe bağlı: Önceden herhangi bir SSL/TLS kanalı çalıştırıldıysa, `REFRESH SECURITY TYPE(SSL)` komutunu verin.

   Bu, anahtar havuzunda yapılan tüm değişikliklerin kullanılabilir olmasını sağlar.
3. Start the channel on QMA, using the command `START CHANNEL(TO.QMB)`.

Sonuçlar

Gönderen kanalı başlatıldı.

z/OS *z/OS' da kendinden imzalı sertifikalar alışverişi yapma*

Daha önce çıkardığınız sertifikaları değiştirin. FTP kullanıyorsanız, doğru biçimi kullanın.

Yordam

Transfer the CA part of the QM1 certificate to the QM2 system and vice versa, for example, by FTP.

FTP ' yi kullanarak sertifikaları aktarırsanız, doğru biçimde yapmanız gerekir.

Aşağıdaki sertifika tiplerini *ikili* biçimde aktarın:

- DER kodlanmış ikili X.509
- PKCS #7 (CA sertifikaları)
- PKCS #12 (kişisel sertifikalar)

Aşağıdaki sertifika tiplerini ASCII biçiminde aktarın:

- PEM (gizlilik-gelişmiş posta)
- Base64 kodlamalı X.509

z/OS *Defining a sender channel and transmission queue on QM1 on z/OS*

Gerekli nesneleri ayarlamak için **DEFINE CHANNEL** ve **DEFINE QLOCAL** komutlarını kullanın.

Yordam

QM1üzerinde, aşağıdaki örnek gibi komut verin:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using TLS from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

Kanalın her bir ucundaki CipherSpecs (şifreleme Belirtimleri) aynı olmalıdır.

Kanalınızın TLS ' yi kullanmasını istiyorsanız, yalnızca SSLCIPH parametresi zorunludur. SSLCIPH parametresine ilişkin izin verilen değerler hakkında bilgi için bkz. “IBM MQiçindeCipherSpecs ve CipherSuites” sayfa 38 .

Sonuçlar

Gönderen kanalı, QM1.TO.QM2ve bir iletim kuyruğu (QM2) yaratılır.

z/OS *z/OSüzerinde QM2 üzerinde bir alıcı kanalı tanımlama*

Gerekli nesneyi ayarlamak için **DEFINE CHANNEL** komutunu kullanın.

Yordam

QM2üzerinde aşağıdaki örnek gibi bir komut yayınlayın:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS from QM1 to QM2')
```

Kanal, “Defining a sender channel and transmission queue on QM1 on z/OS” sayfa 313içinde tanımladığınız gönderici kanalıyla aynı ada sahip olmalıdır ve aynı CipherSpec' i kullanmalıdır.

z/OS *Starting the sender channel on QM1 on z/OS*

Gerekiyorsa, bir dinleyici programı başlatın ve güvenliği yenileyin. Then start the channel using the **START CHANNEL** command.

Yordam

1. İsteğe bağlı: Henüz yapmadıysanız, QM2' de bir dinleyici programı başlatın.

   Dinleyici programı gelen ağ isteklerini dinler ve gerektiğinde alıcı kanalını başlatır. Bir dinleyicinin nasıl başlatılacağı hakkında bilgi için Kanal dinleyicisi başlatmabaşlıklı konuya bakın.
2. İsteğe bağlı: Önceden çalıştırılan bir SSL/TLS kanalı varsa, REFRESH SECURITY TYPE (SSL) komutunu verin.

   Bu, anahtar havuzunda yapılan tüm değişikliklerin kullanılabilir olmasını sağlar.
3. On QM1, start the channel, using the command `START CHANNEL(QM1.TO.QM2)`.

Sonuçlar

Gönderen kanalı başlatıldı.

z/OS *Refreshing the SSL or TLS environment on z/OS*

REFRESH SECURITY komutunu kullanarak kuyruk yöneticisi QMA üzerinde TLS ortamını yenileyin.

Yordam

QMA ' da aşağıdaki komutu girin:

```
REFRESH SECURITY TYPE(SSL)
```

Bu, anahtar havuzunda yapılan tüm değişikliklerin kullanılabilir olmasını sağlar.

z/OS *z/OSüzerindeki bir alıcı kanalına anonim bağlantılara izin verme*

SSL ya da TLS istemcisi kimlik doğrulamasını isteğe bağlı yapmak için **ALTER CHANNEL** komutunu kullanın.

Yordam

QMB ' de aşağıdaki komutu girin:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS *Starting the sender channel on QM1 on z/OS*

Gerekiyorsa, kanal başlatıcıyı başlatın, bir dinleyici programı başlatın ve güvenliği yenileyin. Then start the channel using the **START CHANNEL** command.

Yordam

1. İsteğe bağlı: daha önce yapmadıysanız, kanal başlatıcıyı başlatın.
2. İsteğe bağlı: Henüz yapmadıysanız, QM2' de bir dinleyici programı başlatın.

   Dinleyici programı gelen ağ isteklerini dinler ve gerektiğinde alıcı kanalını başlatır. Bir dinleyicinin nasıl başlatılacağı hakkında bilgi için Kanal dinleyicisi başlatmabaşlıklı konuya bakın.
3. İsteğe bağlı: Kanal başlatıcı zaten çalışıyorsa ya da daha önce SSL/TLS kanalları çalıştırıldıysa, REFRESH SECURITY TYPE (SSL) komutunu verin.

   Bu, anahtar havuzunda yapılan tüm değişikliklerin kullanılabilir olmasını sağlar.
4. On QM1, start the channel, using the command `START CHANNEL(QM1.TO.QM2)`.

Sonuçlar

Gönderen kanalı başlatıldı.

z/OS *Starting the sender channel on QMA on z/OS*

Gerekiyorsa, kanal başlatıcıyı başlatın, bir dinleyici programı başlatın ve güvenliği yenileyin. Then start the channel using the **START CHANNEL** command.

Yordam

1. İsteğe bağlı: Henüz yapmadıysanız, kanal başlatıcıyı başlatın.
2. İsteğe bağlı: Henüz yapmadıysanız, QMB ' de bir dinleyici programı başlatın.

   Dinleyici programı gelen ağ isteklerini dinler ve gerektiğinde alıcı kanalını başlatır. Bir dinleyicinin nasıl başlatılacağı hakkında bilgi için Kanal dinleyicisi başlatmabaşlıklı konuya bakın.
3. İsteğe bağlı: Kanal başlatıcısı zaten çalışıyorsa ya da önceden çalıştırılan bir SSL/TLS kanalı varsa, `REFRESH SECURITY TYPE(SSL)` komutunu verin.

   Bu, anahtar havuzunda yapılan tüm değişikliklerin kullanılabilir olmasını sağlar.
4. Start the channel on QMA, using the command `START CHANNEL(TO.QMB)`.

Sonuçlar

Gönderen kanalı başlatıldı.

z/OS *z/OSüzerinde eliptik eğri anahtar uzunluğunu değiştirme*

GSK_CLIENT_ECURVE_LIST ortam değişkenini nasıl değiştirdiğinizde, istemci tarafından belirlenen eliptik eğrilerin ya da desteklenen grupların listesini, bir ya da daha çok 4 karakterden oluşan bir dizgi olarak kullanılmak üzere ayarlamak için kullanılır.

Önemli: TLS 1.0, TLS 1.1 ve/ya da TLS 1.2 ile anlaşmalı bağlantılar kullanılırken, belirli eliptik eğrilerin işletim sistemi tarafından etkin hale getirilmesine izin vermek için düzeltmeyi z/OS APAR OA61783 içinde uygulamalısınız.

CEEOPTS DD deyimini kullanarak, kanal başlatıcı başlatma JCL ' de bu TLS ortam değişkenini ayarlayabilirsiniz:

```
CEEOPTS DD DSN=<dataset-name>,DISP=SHR
```

Yukarıda gönderme yapılan veri kümesinde, kullanmak istediğiniz listeyi belirtin, örneğin:

```
ENVAR("GSK_CLIENT_ECURVE_LIST=002300240025")
```

Önemli: Ortam değişkeninin bu deyimi kullanarak tüm TLS görevleri için ayarlanmasını önlediği için, bu CEEOPTS deyimini akış içi verilerle kullanmayın.

Bir SSLTASKS değeri birden büyük kullanıldığında bu işin çalışmasına izin vermek için, sıralı bir veri kümesine ya da bölümlenmiş bir veri kümesi üyeye başvuruda bulunduğunuzdan emin olun.

GS_SERVER_ALLOWED_KEX_ECURVES GSK_CLIENT_ECURVE_LIST sunucu analogue değerini de kullanabilirsiniz. Ek bilgi için Limiting tuşu değişimi eliptik eğrileri başlıklı konuya bakın.

Ayrıca, geçerli 4 karakterli eliptik eğri ve desteklenen gruplar belirtimlerinin bir listesi için Cipher suite definitions (Şifreleme takımı tanımlarında) başlıklı konuya bakın.

Varsayılan belirtim `00210023002400250019' dir. TLS V1.3 etkinleştirilmişse, 0029 (x25519)` varsayılan listenin sonuna eklenir.

Kullanıcıların tanımlanması ve kimlik doğrulaması

You can identify and authenticate users by using X.509 certificates, the MQCSP structure or in several types of user exit program.

X.509 sertifikalarını kullanma

You can identify and authenticate users by using x.509 certificates with the **CHLAUTH** command and **SSLPEER** parameter. **SSLPEER** parametresi, kanalın diğer ucundaki eşdüzey kuyruk yöneticisinden ya da istemciden gelen sertifikenin Konu Ayırt Edici Adı ile karşılaştırmak için kullanılacak bir süzgeci belirtir.

CHLAUTH komutunu ve **SSLPEER** parametresini kullanmaya ilişkin daha fazla bilgi için bkz. SET CHLAUTH.

MQCSP yapısını kullanma

MQCONNX çağrısında MQCSP bağlantı güvenliği değiştirgeleri yapısını belirtiyorsunuz; bu yapı bir kullanıcı kimliği ve parola içeriyor. Gerekiyorsa, bir güvenlik çıkışında MQCSP ' yi değiştirebilirsiniz.

Not: Nesne yetkilisi yöneticisi (OAM) parolayı kullanmaz. Ancak OAM, kullanıcı kimliği ile sınırlı bir çalışma yapar ve bu, kimlik doğrulama için önemsiz bir form olarak kabul edilebilir. Bu denetimler, uygulamalarınızdaki bu parametreleri kullanırsanız, başka bir kullanıcı kimliğini edinmenizi sağlar.

Uyarı: Bazı durumlarda, istemci uygulaması için bir MQCSP yapısındaki parola, düz metindeki bir ağ üzerinden gönderilir. İstemci uygulaması parolalarının uygun şekilde korunmasını sağlamak için bkz. “MQCSP parola koruması” sayfa 28.

Güvenlik çıkışlarında kimlik doğrulama ve kimlik doğrulama uygulanması

Bir güvenlik çıkığının birincil amacı, bir kanalın her bir ucundaki MCA ' yı iş ortağının kimliğini doğrulamaya olanak sağlamaktır. Bir ileti kanalının her iki ucunda ve bir MQI kanalının sunucu ucunda, MCA genellikle bağlı olduğu kuyruk yöneticisi adına hareket eder. Bir MQI kanalının istemci ucunda, MCA genellikle IBM MQ istemci uygulamasının kullanıcısı adına hareket eder. Bu durumda, karşılıklı kimlik doğrulaması aslında iki kuyruk yöneticisi arasında ya da bir kuyruk yöneticisi ile bir IBM MQ MQI client uygulamasının kullanıcısı arasında gerçekleşir.

The supplied security exit (the SSPI channel exit) illustrates how mutual authentication can be implemented by exchanging authentication tokens that are generated, and then checked, by a trusted authentication server such as Kerberos. Daha fazla ayrıntı için bkz. “Windows' da SSPI kanal çıkış programı” sayfa 145.

Ortak kimlik doğrulaması, Public Key Infrastructure (PKI) teknolojisi kullanılarak da uygulanabilir. Her güvenlik çıkışı, bazı rasgele veriler oluşturur, bu verileri kuyruk yöneticisinin ya da temsil ettiği kullanıcının özel anahtarını kullanarak işaretler ve imzalanmış verileri bir güvenlik iletisinde iş ortağına gönderir. İş ortağı güvenlik çıkışı, kuyruk yöneticisinin ya da kullanıcının genel anahtarı kullanılarak dijital imzayı denetleyerek kimlik doğrulamayı gerçekleştirir. Dijital imzalar alışverişi yapmadan önce, kullanmak üzere birden fazla algoritma kullanılabiliyorsa, güvenlik çıkışlarının ileti özeti oluşturma algoritmasını kabul etmesi gerekebilir.

Bir güvenlik çıkışı, imzalanmış verileri iş ortağına gönderdiğinde, kuyruk yöneticisinin ya da kullanıcının temsil ettiği kullanıcı tanımlamak için bazı araçlar da göndermesi gerekir. Bu bir Ayırt Edici Ad, hatta sayısal bir sertifika olabilir. Bir dijital sertifika gönderilirse, iş ortağı güvenlik çıkışı, sertifika zinciri aracılığıyla kök CA sertifikasına çalışarak sertifikana doğrulanabilir. Bu, dijital imzayı kontrol etmek için kullanılan genel anahtarın sahipliğini güvence altına alır.

İş ortağı güvenlik çıkışı, yalnızca sertifika zincirindeki geri kalan sertifikaları içeren bir anahtar havuzuna erişimi olması durumunda sayısal sertifikayı doğrulayabilir. Kuyruk yöneticisi ya da kullanıcısı için bir sayısal sertifika gönderilmediyse, iş ortağı güvenlik çıkışa erişiminin olduğu anahtar havuzunda bir sertifika kullanılabilir olmalıdır. İş ortağı güvenlik çıkışı, imzalayanın genel anahtarını bulmadığı sürece dijital imzayı denetleyemez.

TLS (Transport Layer Security; İletim Katmanı Güvenliği), yalnızca anlatılanlar gibi PKI tekniklerini kullanır. TLS ' nin kimlik doğrulamayı nasıl gerçekleştireceği hakkında daha fazla bilgi için bkz. “Transport Layer Security (TLS) kavramları” sayfa 14.

Güvenilir bir kimlik doğrulama sunucusu ya da PKI desteği yoksa, diğer teknikler kullanılabilir. Güvenlik çıkışlarında uygulanabilen ortak bir teknik, simetrik bir anahtar algoritması kullanır.

Güvenlik çıkışlarından biri, A çıkışı, rasgele bir sayı oluşturur ve bunu, iş ortağı güvenlik çıkışa bir güvenlik iletisinde gönderir, B ' den çıkar. B çıkışı, yalnızca iki güvenlik çıkışı tarafından bilinen bir anahtarın kopyasını kullanarak numaradan şifrelenir. Çıkış B 'den çıkış, çıkış B' den çıkış yapan ikinci bir rasgele sayı içeren bir güvenlik iletisinde bulunan şifrelenmiş sayıyı gönderir. Exit A, ilk rasgele sayının doğru şekilde şifrelendiğini, anahtarın kopyasını kullanarak ikinci rasgele sayıyı şifreler ve bir güvenlik iletisinde B ' den çıkmak için şifrelenmiş numarayı gönderir. B çıkışı, ikinci rasgele sayının doğru şekilde şifrelenip şifrelenmediğini doğrular. Bu değişim sırasında, herhangi bir güvenlik çıkışı diğerinden memnun değilse, MCA ' yı kanalı kapatmaya yönlendirebilir.

Bu tekniğin bir avantajı, değiş tokuş sırasında iletişim bağlantısı üzerinden hiçbir anahtar ya da parolanın gönderilmemesine yol göstermez. Bir dezavantaj, paylaşılan anahtarın güvenli bir şekilde nasıl dağıtılması sorununa çözüm sağlamaması olabilir. Bu soruna bir çözüm “Kullanıcı çıkış programlarında gizliliği uygulama” sayfa 430içinde açıklanmıştır. Benzer bir teknik, bir oturum oluşturmak üzere bağlandığında iki LU 'nun karşılıklı kimlik doğrulaması için SNA' da kullanılır. Teknik, “Oturum düzeyi kimlik doğrulaması” sayfa 111içinde açıklanmıştır.

Karşılıklı kimlik doğrulama için önceki tüm teknikler, tek yönlü kimlik doğrulaması sağlamak üzere uyarlanabilir.

İleti çıkışlarında kimlik doğrulama ve kimlik doğrulama uygulanması

Bir uygulama bir kuyruğa ileti koyduğunda, ileti tanımlayıcısındaki *UserIdentifier* alanında uygulamayla ilişkili bir kullanıcı kimliği bulunur. Ancak, kullanıcı kimliğinin kimliğini doğrulamak için kullanılabilecek herhangi bir veri yok. Bu veriler, bir kanalın gönderme bitişindeki bir ileti çıkışı tarafından eklenerek, kanalın alıcı ucundaki bir ileti çıkışı tarafından denetlenebilir. Kimlik doğrulama verileri, örneğin şifrelenmiş bir parola ya da dijital imza olabilir.

Bu hizmet, uygulama düzeyinde uygulansa daha etkili olabilir. Temel gereksinme, iletiyi gönderen ve iletiyi gönderen uygulamanın kimliğini doğrulayabilecek bir iletiyi alan uygulamanın kullanıcısı içindir. Bu nedenle, bu hizmeti uygulama düzeyinde uygulamayı göz önünde bulundurmanız doğaldır. Daha fazla bilgi için “API çıkışta ve API ' den geçiş çıkışındaki kimlik eşlemesi” sayfa 322 başlıklı konuya bakın.

API çıkışta ve API ' den geçiş çıkışındaki kimlik doğrulama ve kimlik doğrulaması

Tek bir ileti düzeyinde, tanımlama ve kimlik doğrulama iki kullanıcı, gönderici ve iletinin alıcısı içeren bir hizmettir. Temel gereksinme, iletiyi gönderen ve iletiyi gönderen uygulamanın kimliğini doğrulayabilecek bir iletiyi alan uygulamanın kullanıcısı içindir. Gereksinimin iki yönlü değil, bir şekilde kimlik doğrulaması olduğunu unutmayın.

Bu hizmetin nasıl uygulanına bağlı olarak, kullanıcılar ve uygulamalarının hizmetle etkileşim kurması ya da etkileşimde bulunması gerekebilir. Buna ek olarak, hizmetin ne zaman ve nasıl kullanılacağı, kullanıcıların ve uygulamalarının bulunduğu yere ve uygulamaların doğasına bağlı olabilir. Bu nedenle, hizmeti, bağlantı düzeyinde değil, uygulama düzeyinde uygulamayı göz önünde bulundurmanız doğaldır.

Bu hizmeti bağlantı düzeyinde uygulamayı göz önünde bulundurmanız durumunda, aşağıdakiler gibi sorunları çözümlemeniz gerekebilir:

- Bir ileti kanalında, hizmeti yalnızca gerektiren iletiler için nasıl uygulardınız?
- Bu bir gereksinim olduğunda, kullanıcıları ve uygulamalarını, hizmetle, arabirimle etkileşimli olarak nasıl etkinleştirebildiniz?
- Çok sekmeli bir durumda, bir iletinin varış noktasına giden yolda birden fazla ileti kanalı üzerinden gönderildiği durumlarda, hizmetin bileşenlerini nereden çağırdınız?

Tanıtım ve kimlik doğrulama hizmetinin uygulama düzeyinde nasıl uygulanabileceğinin bazı örnekleri burada bulunmaktadır. *API çıkışı* terimi, bir API çıkışı ya da bir API geçiş çıkışı anlamına gelir.

- Bir uygulama bir iletiyi kuyruğa yerleştirdiğinde, bir API çıkışı, Kerberosgibi güvenilir bir kimlik doğrulama sunucusundan bir kimlik doğrulama belirteci edinebilir. API çıkışı, bu simgeyi iletteki uygulama verilerine ekleyebilirler. İleti alan uygulama tarafından alındığında, ikinci bir API çıkışı, kimlik doğrulama sunucusunda, belirteci denetleyerek gönderenin kimliğini doğrulamasına izin verebilir.
- Bir uygulama bir iletiyi kuyruğa yerleştirdiğinde, bir API çıkışı aşağıdaki öğeleri iletteki uygulama verilerine ekleyebilirler:
  - Gönderenin sayısal sertifikası
  - Gönderenin dijital imzası

  Bir ileti özeti oluşturmak için kullanılabilecek farklı algoritmalar kullanılabiliyorsa, API çıkışı, kullandığı algoritmanın adını içerebilir.

  İleti alma uygulaması tarafından alındığında, ikinci bir API çıkışı aşağıdaki denetimleri gerçekleştirebilir:

  - API çıkışı, sertifika zinciri aracılığıyla kök CA sertifikasına çalışarak sayısal sertifikayı doğrulayabilir. Bunu yapmak için, API çıkısının, sertifika zincirindeki geri kalan sertifikaları içeren bir anahtar havuzuna erişimi olması gerekir. Bu denetim, Ayırt Edici Ad tarafından tanımlanan gönderenin, sertifikada yer alan genel anahtarın gerçek sahibi olduğunu garanti eder.
  - API çıkışı, sertifikada bulunan ortak anahtarı kullanarak dijital imzayı denetleyebilir. Bu denetim, gönderenin kimliğini doğrular.

  Gönderenin Ayırt Edici Adı, tüm dijital sertifika yerine gönderilebilir. Bu durumda, ikinci API çıkışı gönderenin genel anahtarını bulabilmesi için anahtar havuzunun gönderenin sertifikasını içermesi gerekir. Diğer bir olasılık da sertifika zincirindeki tüm sertifikaları göndermenin.
- Bir uygulama bir kuyruğa ileti koyduğunda, ileti tanımlayıcısındaki *UserIdentifier* alanında uygulamayla ilişkili bir kullanıcı kimliği bulunur. Kullanıcı kimliği, göndereni tanımlamak için kullanılabilir. Kimlik doğrulamayı etkinleştirmek için, bir API çıkışı, şifrelenmiş parola gibi bazı verileri iletteki uygulama verilerine ekleyebilirler. İleti alan uygulama tarafından alındığında, ikinci bir API çıkışı, iletiyle birlikte seyahat eden verileri kullanarak kullanıcı kimliğinin kimliğini doğrulayabilir.

  Bu teknik, denetimli ve güvenilir bir ortamda kaynaklanan iletiler için ve güvenilir bir kimlik doğrulama sunucusunun ya da PKI desteğinin kullanılamadığı durumlarda yeterli kabul edilebilir.

Eklenebilir Kimlik Doğrulama Yöntemi (PAM)

Linux UNIX

PAM artık UNIX and Linux platformlarında yaygındır ve hizmetlerden kullanıcı kimlik doğrulamasının ayrıntılarını gizleyen genel bir mekanizma sağlar.

Farklı hizmetler için farklı kimlik doğrulama kuralları kullanılabilir. Bu kurallar, hizmetlerin kendileri için gerekli herhangi bir değişiklik olmadan, kuralları yapılandırılarak kullanılabilir.

Ek bilgi için “Pluggable Authentication Method (PAM) olanağının kullanılması” sayfa 334 ' e bakın.

Ayrıcalıklı kullanıcılar

Ayrıcalıklı bir kullanıcı, IBM MQiçin tam yönetim yetkilerine sahip bir kullanıcıdır.

Aşağıdaki tabloda listelenen kullanıcılara ek olarak, kuyruk yöneticisinin bütünlüğünü ve güvenliğini sağlamak için erişim verilirken ek bakımın alınması gereken belirli nesneler ve yetkiler vardır. Aşağıdaki yetkilerden herhangi birine izin verilirken ek inceleme uygulanmalıdır:

- SYSTEM nesnelerine ilişkin tüm yetkiler
- Nesneleri oluşturmak, değiştirmek ve silmek için yönetim yetkileri.

  z/OS z/OS' da bu yetki, DEFINE, ALTER ve DELETE komutlarının yayınına ilişkin komut güvenliği ve komut kaynağı güvenlik yetkisine sahip olur.

  Multi Diğer tüm platformlarda bu yetkiler, `+crt`, `+chg` ve `+dlt`gibi yönetim yetkisleridir.
- Kuyrukları temizlemek için denetim yetkisi.

  z/OS z/OSüzerinde, bu yetki, CLEAR komutlarını vermek için komut güvenliği ve komut kaynağı güvenlik yetkisine sahip olur.

  Multi Diğer tüm platformlarda bu yetki `+clr`' dir.
- Kanalları durdurma, geri alma ya da kesinleştirme iletileri için denetim yetkileri.

  z/OS z/OS' ta, bu yetki, RESET CHANNEL, START CHANNEL ve STOP CHANNEL gibi komutları vermek için komut güvenliği ve komut kaynağı güvenlik yetkisine sahip olur.

  Multi Diğer tüm platformlarda bu yetkiler `+ctrl` ve `+ctrlx`' dir.
- Uygulamaların yetkilendirme denetimleri için ayrıcalıkları yükseltmesine olanak tanıyan diğer kullanıcı MQI yetkisi.

  z/OS z/OS' ta bu yetki, diğer kullanıcı güvenlik profillerine verilen herhangi bir yetkidir.

  Multi Diğer tüm platformlarda bu yetki `+altusr`' dir.
- Uygulamaların, iletilerin güvenlik bağlamını değiştirmesine izin veren bağlam yetkileri.

  z/OS z/OS' ta bu yetki, bağlam güvenliği profillerine verilen herhangi bir yetkidir.

  Multi Diğer tüm platformlarda bu yetkiler `+setall` ve `+setid`' dir.

Genel bir birincil kullanıcı olarak, ileti alışverişi uygulamalarının yalnızca gereken kuyruklara ya da konulara ilişkin temel MQI yetkileri verilmelidir. Ayrıcalıklı olmayan bir MCAUSER ve diğer bazı özel tip uygulamalar altında çalışan MCA kanalları, örneğin, ölü harf kuyruk işleyicileri gibi, uygulamaların düzgün bir şekilde çalışması için normalde ek yetkiler edinilmesini gerektirebilirler.

Çizelge 67. Altyapıya göre ayrıcalıklı kullanıcılar

Platform	**Ayrıcalıklı kullanıcılar**
Windows sistemleri	• SYSTEM • mqm grubunun üyeleri • Administrators (Yöneticiler) grubunun üyeleri
UNIX and Linux sistemleri	• mqm grubunun üyeleri
IBM i IBM i IBM i sistemleri	• qmqm ve qmqmadm tanıtımlar • qmqmadm grubunun tüm üyeleri • *ALLOBJ ayarına sahip kullanıcı tanımlı

Çizelge 67. Altyapıya göre ayrıcalıklı kullanıcılar (devamı var)	
Platform	**Ayrıcalıklı kullanıcılar**
z/OS	Kanal başlatıcı, kuyruk yöneticisi ve gelişmiş ileti güvenliği adres alanlarının altında çalıştığı kullanıcı kimliği. Bu kullanıcı kimlikleri IBM MQiçin otomatik olarak tam yönetim yetkilerine sahip değildir; ancak, bu kullanıcı kimliklerine genellikle verilen erişim düzeyi nedeniyle ayrıcalıklı kabul edilir.

MQCSP yapısını kullanarak kullanıcıların belirlenmesi ve doğrulanmaları

MQCONNX çağrısında MQCSP bağlantı güvenliği değiştirgeleri yapısını belirtebilirsiniz.

MQCSP bağlantı güvenliği parametreleri yapısı, yetkilendirme hizmetinin kullanıcıyı tanımlamak ve doğrulamak için kullanabileceği bir kullanıcı kimliği ve parola içeriyor.

Bir güvenlik çıkışında MQCSP ' yi değiştirebilirsiniz.

Uyarı: Bazı durumlarda, bir istemci uygulamasına ilişkin MQCSP yapısındaki parola ağ üzerinden düz metin olarak gönderilir. İstemci uygulama parolalarının uygun şekilde korunduğundan emin olmak için bkz. “MQCSP parola koruması” sayfa 28.

MQCSP ile AdoptCTX ayarları arasındaki ilişki

IBM MQ , bağlantı kimlik doğrulama özelliği etkinleştirilmemişse, MQCSP yapısından geçirilen kimlik bilgilerini her zaman doğrular. Kimlik bilgileri başarıyla doğrulandıktan sonra, ADOPTCTX etkinleştirilmemişse, IBM MQ ileride yapılacak yetkilendirme denetimleri için kullanıcı kimliğini benimseme girişiminde bulunur.

IBM MQ yetki denetimi için kullanıcı kimliğine ilişkin kullanıcı kimliğine ilişkin bir sınır vardır. Bu sınırlar “Kullanıcı Kimlikleri” sayfa 79konusunda ayrıntılı olarak açıklanmıştır. MQCSP yapısından geçirilen bir kullanıcı kimliği benimsenirken IBM MQ , diğer yapılandırma seçeneklerine bağlı olarak farklı davranır:

- LDAP bağlantısı kimlik doğrulamasını kullanırken IBM MQ , kullanıcının LDAP kaydından SHORTUSR içinde ayarlanan alanın değerini alır ve o kullanıcı kimliğini kullanır.

  Örneğin, SHORTUSR `'CN'` olarak ayarlanırsa ve LDAP kaydı bir kullanıcıyı `'CN=Test,SN=MQ,O=IBM,C=UK'`olarak listelerse, `Test` kullanıcı kimliği kullanılır.
- İşletim sistemi bağlantısı kimlik doğrulaması ya da PAM kimlik doğrulaması kullanılırken ADOPTCTX YES ise, MQCSP yapısından geçirilen kullanıcı kimliği, bağlantı bağlamı olarak benimsendiğinde 12 karakterlik IBM MQ kullanıcı kimliği sınırını karşılamak için kesilir.

  ChlAuthEarlyAdopt etkinleştirilirse, kullanıcı kimlik bilgileri doğrulandıktan sonra kesme gerçekleşir.

  ChlAuthEarlyAdopt etkinleştirilmezse, kısaltma benimsemeden önce gerçekleşir. Windows' da, kullanıcı `user@domain`biçiminde sağlanırsa, bu, kullanıcı 12 karakterden kısa olduğunda geçerli olmayan bir etki alanı belirtimine neden olabilir anlamına gelir.

  Örneğin, bir kullanıcı `` `ibmmq@windowsdomain` `` MQCSP aracılığıyla sağlanırsa, bu kullanıcı bu senaryoda `` `ibmmq@window` `` olarak kesilir. Bu, aşağıdaki hatayla sonuçlanır:

  ```
  AMQ8074W: 'SID' varlığı 'ibmmq@window' ile eşleşmediğinden yetkilendirme başarısız oldu
  ```

  Bu temelde, Windows formdaki etki alanı kullanıcı kimliği `user@domain`gibi 12 karakterden uzun bir kullanıcı kimliğini MQCSP aracılığıyla geçirirseniz, bu hatayı önlemek için qm.ini dosyasındaki **ChlAuthEarlyAdopt**=*Y* değerini yapılandırmanız gerekir.

  Alternatif olarak, CONNAUTH AUTHINFO yapılandırmasında ADOPTCTX (NO) kullanın ve kanala ilişkin kullanıcı kimliğini ayarlamak için CHLAUTH USERMAP kuralı, güvenlik çıkışı ya da kanal nesnesi MCAUSER ayarı gibi alternatif bir yaklaşım kullanın.

Güvenlik çıkışlarında kimlik doğrulama ve kimlik doğrulama uygulanması

Tek yönlü ya da karşılıklı kimlik doğrulaması uygulamak için bir güvenlik çıkışı kullanabilirsiniz.

Bir güvenlik çıkığının birincil amacı, bir kanalın her bir ucundaki MCA ' yı iş ortağının kimliğini doğrulamaya olanak sağlamaktır. Bir ileti kanalının her iki ucunda ve bir MQI kanalının sunucu ucunda, MCA genellikle bağlı olduğu kuyruk yöneticisi adına hareket eder. Bir MQI kanalının istemci ucunda, MCA genellikle IBM MQ MQI client uygulamasının kullanıcısı adına hareket eder. Bu durumda, karşılıklı kimlik doğrulaması aslında iki kuyruk yöneticisi arasında ya da bir kuyruk yöneticisi ile bir IBM MQ MQI client uygulamasının kullanıcısı arasında gerçekleşir.

The supplied security exit (the SSPI channel exit) illustrates how mutual authentication can be implemented by exchanging authentication tokens that are generated, and then checked, by a trusted authentication server such as Kerberos. Daha fazla ayrıntı için bkz. “Windows' da SSPI kanal çıkış programı” sayfa 145.

Ortak kimlik doğrulaması, Public Key Infrastructure (PKI) teknolojisi kullanılarak da uygulanabilir. Her güvenlik çıkışı, bazı rasgele veriler oluşturur, bu verileri kuyruk yöneticisinin ya da temsil ettiği kullanıcının özel anahtarını kullanarak işaretler ve imzalanmış verileri bir güvenlik iletisinde iş ortağına gönderir. İş ortağı güvenlik çıkışı, kuyruk yöneticisinin ya da kullanıcının genel anahtarı kullanılarak dijital imzayı denetleyerek kimlik doğrulamayı gerçekleştirir. Dijital imzalar alışverişi yapmadan önce, kullanmak üzere birden fazla algoritma kullanılabiliyorsa, güvenlik çıkışlarının ileti özeti oluşturma algoritmasını kabul etmesi gerekebilir.

Bir güvenlik çıkışı, imzalanmış verileri iş ortağına gönderdiğinde, kuyruk yöneticisinin ya da kullanıcının temsil ettiği kullanıcı tanımlamak için bazı araçlar da göndermesi gerekir. Bu bir Ayırt Edici Ad, hatta sayısal bir sertifika olabilir. Bir dijital sertifika gönderilirse, iş ortağı güvenlik çıkışı, sertifika zinciri aracılığıyla kök CA sertifikasına çalışarak sertifikana doğrulanabilir. Bu, dijital imzayı kontrol etmek için kullanılan genel anahtarın sahipliğini güvence altına alır.

İş ortağı güvenlik çıkışı, yalnızca sertifika zincirindeki geri kalan sertifikaları içeren bir anahtar havuzuna erişimi olması durumunda sayısal sertifikayı doğrulayabilir. Kuyruk yöneticisi ya da kullanıcısı için bir sayısal sertifika gönderilmediyse, iş ortağı güvenlik çıkışa erişiminin olduğu anahtar havuzunda bir sertifika kullanılabilir olmalıdır. İş ortağı güvenlik çıkışı, imzalayanın genel anahtarını bulmadığı sürece dijital imzayı denetleyemez.

TLS (Transport Layer Security; İletim Katmanı Güvenliği), yalnızca anlatılanlar gibi PKI tekniklerini kullanır. Güvenli Yuva Katmanının nasıl kimlik doğrulaması gerçekleştireceği hakkında daha fazla bilgi için bkz. “Transport Layer Security (TLS) kavramları” sayfa 14.

Güvenilir bir kimlik doğrulama sunucusu ya da PKI desteği yoksa, diğer teknikler kullanılabilir. Güvenlik çıkışlarında uygulanabilen ortak bir teknik, simetrik bir anahtar algoritması kullanır.

Güvenlik çıkışlarından biri, A çıkışı, rasgele bir sayı oluşturur ve bunu, iş ortağı güvenlik çıkışa bir güvenlik iletisinde gönderir, B ' den çıkar. B çıkışı, yalnızca iki güvenlik çıkışı tarafından bilinen bir anahtarın kopyasını kullanarak numaradan şifrelenir. Çıkış B 'den çıkış, çıkış B' den çıkış yapan ikinci bir rasgele sayı içeren bir güvenlik iletisinde bulunan şifrelenmiş sayıyı gönderir. Exit A, ilk rasgele sayının doğru şekilde şifrelendiğini, anahtarın kopyasını kullanarak ikinci rasgele sayıyı şifreler ve bir güvenlik iletisinde B ' den çıkmak için şifrelenmiş numarayı gönderir. B çıkışı, ikinci rasgele sayının doğru şekilde şifrelenip şifrelenmediğini doğrular. Bu değişim sırasında, herhangi bir güvenlik çıkışı diğerinden memnun değilse, MCA ' yı kanalı kapatmaya yönlendirebilir.

Bu tekniğin bir avantajı, değiş tokuş sırasında iletişim bağlantısı üzerinden hiçbir anahtar ya da parolanın gönderilmemesine yol göstermez. Bir dezavantaj, paylaşılan anahtarın güvenli bir şekilde nasıl dağıtılması sorununa çözüm sağlamaması olabilir. Bu soruna bir çözüm “Kullanıcı çıkış programlarında gizliliği uygulama” sayfa 430içinde açıklanmıştır. Benzer bir teknik, bir oturum oluşturmak üzere bağlandığında iki LU 'nun karşılıklı kimlik doğrulaması için SNA' da kullanılır. Teknik, “Oturum düzeyi kimlik doğrulaması” sayfa 111içinde açıklanmıştır.

Karşılıklı kimlik doğrulama için önceki tüm teknikler, tek yönlü kimlik doğrulaması sağlamak üzere uyarlanabilir.

İleti çıkışlarında kimlik eşlemesi

Bir kullanıcı kimliğini doğrulamak için gereken bilgileri işlemek için ileti çıkışlarını kullanabilirsiniz; ancak, kimlik doğrulamayı uygulama düzeyinde uygulamak daha iyi olabilir.

Bir uygulama bir kuyruğa ileti koyduğunda, ileti tanımlayıcısındaki *UserIdentifier* alanında uygulamayla ilişkili bir kullanıcı kimliği bulunur. Ancak, kullanıcı kimliğinin kimliğini doğrulamak için kullanılabilecek herhangi bir veri yok. Bu veriler, bir kanalın gönderme bitişindeki bir ileti çıkışı tarafından eklenerek, kanalın alıcı ucundaki bir ileti çıkışı tarafından denetlenebilir. Kimlik doğrulama verileri, örneğin şifrelenmiş bir parola ya da dijital imza olabilir.

Bu hizmet, uygulama düzeyinde uygulansa daha etkili olabilir. Temel gereksinme, iletiyi gönderen ve iletiyi gönderen uygulamanın kimliğini doğrulayabilecek bir iletiyi alan uygulamanın kullanıcısı içindir. Bu nedenle, bu hizmeti uygulama düzeyinde uygulamayı göz önünde bulundurmanız doğaldır. Daha fazla bilgi için “API çıkışta ve API ' den geçiş çıkışındaki kimlik eşlemesi” sayfa 322 başlıklı konuya bakın.

API çıkışta ve API ' den geçiş çıkışındaki kimlik eşlemesi

İletiyi alan bir uygulama, iletiyi gönderen uygulamanın kullanıcısının kimliğini belirleyebilmeli ve doğrulayabilmelidir. Bu hizmet genellikle uygulama düzeyinde en iyi şekilde uygulanmaktadır. API çıkışları, hizmeti çeşitli şekillerde uygulayabilir.

Tek bir ileti düzeyinde, tanımlama ve kimlik doğrulama iki kullanıcı, gönderici ve iletinin alıcısı içeren bir hizmettir. Temel gereksinme, iletiyi gönderen ve iletiyi gönderen uygulamanın kimliğini doğrulayabilecek bir iletiyi alan uygulamanın kullanıcısı içindir. Gereksinimin iki yönlü değil, bir şekilde kimlik doğrulaması olduğunu unutmayın.

Bu hizmetin nasıl uygulanına bağlı olarak, kullanıcılar ve uygulamalarının hizmetle etkileşim kurması ya da etkileşimde bulunması gerekebilir. Buna ek olarak, hizmetin ne zaman ve nasıl kullanılacağı, kullanıcıların ve uygulamalarının bulunduğu yere ve uygulamaların doğasına bağlı olabilir. Bu nedenle, hizmeti, bağlantı düzeyinde değil, uygulama düzeyinde uygulamayı göz önünde bulundurmanız doğaldır.

Bu hizmeti bağlantı düzeyinde uygulamayı göz önünde bulundurmanız durumunda, aşağıdakiler gibi sorunları çözümlemeniz gerekebilir:

- Bir ileti kanalında, hizmeti yalnızca gerektiren iletiler için nasıl uygulardınız?
- Bu bir gereksinim olduğunda, kullanıcıları ve uygulamalarını, hizmetle, arabirimle etkileşimli olarak nasıl etkinleştirebildiniz?
- Çok sekmeli bir durumda, bir iletinin varış noktasına giden yolda birden fazla ileti kanalı üzerinden gönderildiği durumlarda, hizmetin bileşenlerini nereden çağırdınız?

Tanıtım ve kimlik doğrulama hizmetinin uygulama düzeyinde nasıl uygulanabileceğinin bazı örnekleri burada bulunmaktadır. *API çıkışı* terimi, bir API çıkışı ya da bir API geçiş çıkışı anlamına gelir.

- Bir uygulama bir iletiyi kuyruğa yerleştirdiğinde, bir API çıkışı, Kerberosgibi güvenilir bir kimlik doğrulama sunucusundan bir kimlik doğrulama belirteci edinebilir. API çıkışı, bu simgeyi iletteki uygulama verilerine ekleyebilirler. İleti alan uygulama tarafından alındığında, ikinci bir API çıkışı, kimlik doğrulama sunucusunda, belirteci denetleyerek gönderenin kimliğini doğrulamasına izin verebilir.
- Bir uygulama bir iletiyi kuyruğa yerleştirdiğinde, bir API çıkışı aşağıdaki öğeleri iletteki uygulama verilerine ekleyebilirler:
  - Gönderenin sayısal sertifikası
  - Gönderenin dijital imzası

  Bir ileti özeti oluşturmak için kullanılabilecek farklı algoritmalar kullanılabiliyorsa, API çıkışı, kullandığı algoritmanın adını içerebilir.

  İleti alma uygulaması tarafından alındığında, ikinci bir API çıkışı aşağıdaki denetimleri gerçekleştirebilir:

  - API çıkışı, sertifika zinciri aracılığıyla kök CA sertifikasına çalışarak sayısal sertifikayı doğrulayabilir. Bunu yapmak için, API çıkısının, sertifika zincirindeki geri kalan sertifikaları içeren bir anahtar havuzuna erişimi olması gerekir. Bu denetim, Ayırt Edici Ad tarafından tanımlanan gönderenin, sertifikada yer alan genel anahtarın gerçek sahibi olduğunu garanti eder.

– API çıkışı, sertifikada bulunan ortak anahtarı kullanarak dijital imzayı denetleyebilir. Bu denetim, gönderenin kimliğini doğrular.

Gönderenin Ayırt Edici Adı, tüm dijital sertifika yerine gönderilebilir. Bu durumda, ikinci API çıkışı gönderenin genel anahtarını bulabilmesi için anahtar havuzunun gönderenin sertifikasını içermesi gerekir. Diğer bir olasılık da sertifika zincirindeki tüm sertifikaları göndermenin.

- Bir uygulama bir kuyruğa ileti koyduğunda, ileti tanımlayıcısındaki *UserIdentifier* alanında uygulamayla ilişkili bir kullanıcı kimliği bulunur. Kullanıcı kimliği, göndereni tanımlamak için kullanılabilir. Kimlik doğrulamayı etkinleştirmek için, bir API çıkışı, şifrelenmiş parola gibi bazı verileri iletteki uygulama verilerine ekleyebilirler. İleti alan uygulama tarafından alındığında, ikinci bir API çıkışı, iletiyle birlikte seyahat eden verileri kullanarak kullanıcı kimliğinin kimliğini doğrulayabilir.

  Bu teknik, denetimli ve güvenilir bir ortamda kaynaklanan iletiler için ve güvenilir bir kimlik doğrulama sunucusunun ya da PKI desteğinin kullanılamadığı durumlarda yeterli kabul edilebilir.

İptal edilen sertifikalarla çalışma

Sayısal sertifikalar Sertifika Yetkilileri tarafından iptal edilebilir. Platforma bağlı olarak, OCSP ya da LDAP sunucularındaki CRL ' leri kullanarak sertifikaların iptal durumunu denetleyebilirsiniz.

TLS el sıkışması sırasında, iletişim ortakları dijital sertifikalar ile birbirlerinin kimliklerini doğrulalar. Kimlik doğrulaması, alınan sertifikana güvenilebilecek bir onay kutusunu içerebilir. Sertifika Yetkilileri (CA ' lar), aşağıdakiler de dahil olmak üzere çeşitli nedenlerle sertifikaları iptal eder:

- Sahip farklı bir kuruluşa taşındı
- Özel anahtar artık gizli değil.

CAs yayın, iptal edilen kişisel sertifikaları bir Sertifika İptal Listesi 'nde (CRL) iptal eder. İptal edilen CA sertifikaları, bir Yetki İptal Listesi (ARL) içinde yayınlanmıştır.

Aşağıdaki altyapılarda, IBM MQ SSL desteği, OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü) ya da LDAP (Lightweight Directory Access Protocol; Temel Dizin Erişimi Protokolü) sunucularında CRL 'ler ve ARL' leri kullanarak geri alınmış sertifikaları denetler. OCSP, tercih edilen yöntemdir.

- Linux
- UNIX
- Windows

IBM MQ classes for Java ve IBM MQ classes for JMS , bir istemci kanal tanımlama çizelgesi dosyasında OCSP bilgilerini kullanamaz. Ancak, OCSP ' yi Using Online Certificate Protocol(Çevrimiçi Sertifika İletişim Kuralı) altında açıklandığı gibi yapılandırabilirsiniz.

Aşağıdaki altyapılarda ve IBM MQ SSL desteği, yalnızca LDAP sunucularında CRL ve ARL ' leri kullanarak geri alınmış sertifikaları denetler:

- IBM i
- z/OS

Sertifika Yetkilileri hakkında daha fazla bilgi için bkz. “dijital sertifikalar” sayfa 9.

OCSP/CRL denetimi

Uzak gelen sertifikalar için Online Certificate Status Protocol (OCSP) /Certificate Revocation List (CRL) denetimi gerçekleştirilir. İşlem, uzak sistemin kişisel sertifikasından kök sertifikasına kadar olan tüm zinciri denetler.

OCSP doğrulamasını doğrulamak için openSSL ' nin kullanılması

Kuruluşunuz OCSP ' yi doğrulamak için openSSL kullanıyorsa ve daha sonra GSKit TLS bağlantısı kullanmayı denerseniz, UNKNOWN durum uyarısı alırsınız.

Bunun nedeni, zincirdeki tüm sertifikaların kök dışındaki tüm sertifikalar, iptal durumu için GSKit tarafından denetlenmesinden kaynaklanır. GSKit işlemi RFC 5280 'e uygun ve bu, GSKit Güven İlkesi 'nde açıklanmaktadır. GSKit algoritması, RFC 5280 ve GSKit Trust Policy ile açıklandığı gibi, kullanılabilir tüm geri alma bilgileri için kullanılabilir tüm kaynakları dener.

OCSP/CRL denetimi IBM MQ' ta nasıl çalışıyor?

IBM MQ , sertifika uzantısında ya da AUTHINFO nesnelerinde tanımlandığı şekilde, adı belirtilen OCSP ya da CRL uç noktalarına ilişkin sertifikalar denetlenirken davranışı denetlemek için iki mekanizmayı destekler:

- qm.ini dosyasının SSL kısmı' in **OCSPCheckExtensions**, **CDPCheckExtensions**ve **OCSPAuthentication** özniteliklerinin ve
- Kuyruk yöneticisinin ve AUTHINFO OCSP ve CRLLDAP yapılanışlarının SSLCRLNL parametresinin kullanılması. Ek bilgi için ALTER AUTHINFO ve ALTER QMGR başlıklı konuya bakın.

Uyarı:

AUTHTYPE(OCSP) ile ALTER AUTHINFO komutu, IBM i ya da z/OS kuyruk yöneticilerindeki kullanım için geçerli değildir. Ancak, istemci kullanımı için istemci kanal tanımlama çizelgesine (CCDT) kopyalanmak üzere bu altyapılarda belirlenebilir.

OCSPCheckExtensions ve **CDPCheckExtensions** SSL stanza öznitelikleri, IBM MQ ' in sertifikanın AIA uzantısı içinde ayrıntılı olarak OCSP ya da CRL sunucusuna ilişkin bir sertifikayı doğrulayıp doğrulamayacağını denetler.

Etkinleştirilmezse, sertifika uzantısındaki OCSP ya da CRL sunucusu ile iletişim kurulmaz.

OCSP ya da CRL sunucuları AUTHINFO nesnelerine göre ayrıntılı bir şekilde kullanılıyorsa ve SSLCRLNL **QMGR** özniteliği kullanılarak başvurulsa, sertifika iptal işlemi sırasında IBM MQ bu sunucularla bağlantı kurma girişiminde bulunur.

Önemli: SSLCRLNL ad listesinde yalnızca bir OCSP AUTHINFO nesnesi tanımlanabilir.

Eğer:

OCSPCheckExtensions= NO ve **CDPCheckExtensions**=*NO* değeri ayarlanır ve AUTHINFO nesnelerinde OCSP ya da CRL sunucusu tanımlanmadı

Sertifika iptal denetimi gerçekleştirilmez.

When verifying a certificate for its revocation status, IBM MQ contacts the OCSP or CRL servers named in the following order, if enabled:

1. OCSP Sunucusu bir **AUTHTYPE(OCSP)** nesnesinde ayrıntılı olarak ve SSLCRLNL **QMGR** özniteisinde başvuruda bulunandır.
2. OCSP servers detailed in the AIA extension of the certificates, if **OCSPCheckExtensions**=*EVET*.
3. CRL servers detailed in the **CRLDistributionPoints** extension of the certificates, if **CDPCheckExtensions** =*EVET*.
4. **AUTHINFO(CRLLDAP)** nesnelerinde ayrıntılı olarak açıklanan ve SSLCRLNL **QMGR** özniteisinde başvurulan CRL sunucuları.

Bir sertifikayı doğrularken, OCSP ya da CRL sunucusundaki bir adım, sertifika için bir sorguya kesin bir REVOKED ya da VALID yanıtı döndürürse, başka bir denetim gerçekleştirilmez ve sertifikanın durumu, güvenilir olup olmadığını belirlemek için kullanılır.

Bir OCSP sunucusu ya da CRL sunucusu UNKNOWNsonucunu döndürürse, OCSP ya da CRL sunucusu kesin bir sonuç döndürünceye ya da tüm seçenekler tükeninceye kadar işleme devam eder.

Bir sertifikana ilişkin durum belirlenemezse, sertifikenin iptal edilip edilmeyeceği, OCSP ve CRL sunucuları için farklı bir davranışa yol gösterecektir:

- CRL sunucuları için, CRL sağlanmıyorsa, sertifika `NOT_REVOKED`olarak değerlendirilir.
- OCSP sunucuları için, herhangi bir iptal durumu OCSP sunucusundan alınamazsa, davranış, qm.ini dosyasının SSL Stanza 'sındaki **`OCSPAuthentication`** özniteliği aracılığıyla denetlenir.

  Bu özniteliği, bir bağlantıyı engelleyebilir, bir bağlantıya izin verebilir ya da bir uyarı iletisiyle bağlantıya izin verebilirsiniz için de yapılandırabilirsiniz.

Gerekiyorsa, OCSP denetimlerine ilişkin qm.ini ve mqclient.ini kütüklerinin SSL kısmında **`SSLHTTPProxyName`**=*dizgi* özniteliğini kullanabilirsiniz. Bu dizgi, GSKit for OCSP denetimlerini kullanarak kullanılacak HTTP yetkili sunucusunun anasistem adı ya da ağ adresidir.

From IBM MQ 9.1.5 you can set the **`OCSPTimeout`** value in the SSL stanza of the `qm.ini` or `mqclient.ini` files that sets the number of seconds to wait for an OCSP responder when performing a revocation check.

ULW İptal edilen sertifikalar ve OCSP

IBM MQ , hangi Online Certificate Status Protocol (OCSP) yanıtlayıcının kullanılacağını ve alınan yanıtı işleyeceğini belirler. OCSP yanıtlayıcıya erişilir kılmak için adımlar atmanız gerekebilir.

Not: Bu bilgiler yalnızca UNIX, Linux, and Windows sistemlerinde IBM MQ için geçerlidir.

OCSP kullanan bir sayısal sertifikana ilişkin iptal durumunu denetlemek için IBM MQ , hangi OCSP yanıtlayıcının iletişim kurabileceğini belirlemek için iki yöntem kullanabilir:

- Denetlenecek sertifikadaki AuthorityInfoAccess (AIA) sertifika uzantısını kullanarak.
- Bir kimlik doğrulama bilgileri nesnesinde belirtilen ya da bir istemci uygulaması tarafından belirtilen URL ' yi kullanarak.

Bir kimlik doğrulama bilgileri nesnesinde ya da bir istemci uygulaması tarafından belirtilen URL, AIA sertifika uzantısındaki bir URL ' nin üzerinde önceliğe sahip olur.

OCSP yanıtlayıcının URL 'si bir güvenlik duvarının arkasında yatar, güvenlik duvarını yeniden yapılandırın, böylece OCSP yanıtlayıcıya erişilebilir ya da bir OCSP yetkili sunucusu ayarlanabilirler. SSL stanzasında SSLHTTPProxyName değişkenini kullanarak yetkili sunucunun adını belirtin. İstemci sistemlerinde, MQSSLPROXY ortam değişkenini kullanarak, yetkili sunucunun adını da belirtebilirsiniz. Daha fazla ayrıntı için ilgili bilgilere bakın.

TLS sertifikalarının iptal edilip edilmediği konusunda endişe etmiyorsanız, bir test ortamında çalışmakta olduğunuz için, SSL stanza içinde OCSPCheckExtensions seçeneğini NO değerine ayarlayabilirsiniz. Bu değişkeni ayarlarsaniz, herhangi bir AIA sertifika uzantısı yoksayılır. Bu çözüm, büyük olasılıkla iptal edilen sertifikaları sunan kullanıcılardan erişime izin vermek istemediğiniz bir üretim ortamında kabul edilebilir bir şekilde kabul edilebilir bir şekilde değildir.

OCSP yanıtlayıcıya erişmek için yapılan arama aşağıdaki üç sonuçtan biriyle sonuçlanabilir:

İyi
Sertifika geçerli.

İptal Edildi
Sertifika iptal edildi.

Bilinmiyor
Bu sonuç üç nedenden biri için ortaya çıkabilir:

- IBM MQ , OCSP yanıtlayıcıya erişemiyor.
- OCSP yanıtlayıcısı bir yanıt gönderdi, ancak IBM MQ yanıtın dijital imzasını doğrulayamıyor.
- OCSP yanıtlayıcısı, sertifika için herhangi bir iptal verisi olmadığını belirten bir yanıt gönderdi.

IBM MQ , `Bilinmiyor`' un OCSP sonucunu alırsa, davranışı OCSPAuthentication özniteliğinin ayarına bağlıdır. Kuyruk yöneticileri için bu öznitelik aşağıdaki konumlardan birinde tutulur:

- Linux UNIX UNIX and Linuxüzerindeki `qm.ini` dosyasının SSL kısmına bakın.
- Windows Windows kayıt defterinde.

Bu öznitelik, IBM MQ Explorerkullanılarak ayarlanabilir. İstemciler için, öznitelik istemci konfigürasyon dosyasının SSL kısmında tutulur.

`Bilinmiyor` değeri alındıysa ve OCSPAuthentication REQUIRECTION (varsayılan değer) olarak ayarlandıysa, IBM MQ bağlantıyı reddeder ve AMQ9716tipinde bir hata iletisi yayınlar. Kuyruk yöneticisi SSL olay iletileri etkinleştirilirse, MQRC_CHANNEL_SSL_ERROR tipinde bir SSL olay iletisi ReasonQualifier ile MQRQ_SSL_HANDSHAKE_ERROR değerine sahip bir SSL olay iletisi üretilir.

`Bilinmiyor` değeri alındıysa ve OCSPAuthentication isteğe bağlı olarak ayarlandıysa, IBM MQ , SSL kanalının başlatılmasına izin verir ve uyarı ya da SSL olay iletileri oluşturulmadı.

`Bilinmiyor` değeri alınırsa ve OCSPAuthentication WARN olarak ayarlanmışsa, SSL kanalı başlatılır, ancak IBM MQ hata günlüğünde AMQ9717 tipinde bir uyarı iletisi yayınlar. Kuyruk yöneticisi SSL olay iletileri etkinleştirilirse, MQRC_CHANNEL_SSL_UYARY tipinde bir SSL olay iletisi ReasonQualifier ile MQRQ_SSL_UNKNOWN_REVOCATION değerine ayarlanır.

OCSP yanıtlarının dijital imzalanması

OCSP yanıtlayıcısı, yanıtlarını üç yöntemden biriyle imzalayabilir. Yanıtlayıcınız hangi yöntemin kullanıldığını size bildirecektir.

- OCSP yanıtı, denetleymekte olduğunuz sertifikayı veren CA sertifikası kullanılarak dijital olarak imzalanabilir. Bu durumda, ek sertifika kurmanız gerekmez; TLS bağlanırlığı oluşturmak için önceden attığınız adımlar, OCSP yanıtını doğrulamak için yeterlidir.
- OCSP yanıtı, denetleymekte olduğunuz sertifikayı veren aynı sertifika kuruluşu (CA) tarafından imzalanmış başka bir sertifika kullanılarak dijital olarak imzalanabilir. İmzalama sertifikası, bu durumda OCSP yanıtı ile birlikte gönderilir. OCSP yanıtlayıcısı tarafından aktarılan sertifikanda, bu amaç için güvenilebilmesi için bir Genişletilmiş Anahtar Kullanım Uzantısı `id-kp-OCSPSigning` değerine ayarlanmış olmalıdır. OCSP yanıtı, sertifikayı imzalayan sertifikayla birlikte gönderilir (ve bu sertifika, önceden TLS bağlanırlığı için güvenilen bir sertifika kuruluşu tarafından imzalanır), ek sertifika kuruluşuna gerek yoktur.
- OCSP yanıtı, denetleymekte olduğunuz sertifikayla doğrudan ilişkili olmayan başka bir sertifika kullanılarak dijital olarak imzalanabilir. Bu durumda, OCSP yanıtı OCSP yanıtlayıcısı tarafından verilen bir sertifika tarafından imzalanır. OCSP yanıtlayıcı sertifikasının bir kopyasını istemci ya da kuyruk yöneticisinin anahtar veritabanına eklemelisiniz; bu da OCSP denetimini gerçekleştiren ; bkz. “Adding a CA certificate, or the public part of a self-signed certificate, into a key repository on UNIX, Linux, and Windows” sayfa 291 . Bir CA sertifikası eklendiğinde, varsayılan olarak, bu bağlamda gerekli ayar olan güvenilen bir kök olarak eklenir. If this certificate is not added, IBM MQ cannot verify the digital signature on the OCSP response and the OCSP check results in an Unknown outcome, which might cause IBM MQ to close the channel, depending on the value of OCSPAuthentication.

Online Certificate Status Protocol (OCSP) in Java and JMS client applications

Due to a limitation of the Java API, IBM MQ can use Online Certificate Status Protocol (OCSP) certificate revocation checking for TLS secure sockets only when OCSP is enabled for the entire Java virtual machine (JVM) process. OCSP 'yi JVM' deki tüm güvenli yuvalar için etkinleştirmenin iki yolu vardır:

- Tablo 1 'de gösterilen OCSP yapılandırma ayarlarını dahil etmek için JRE java.security dosyasını düzenleyin ve uygulamayı yeniden başlatın.
- java.security.Security.setProperty() Herhangi bir Java Security Manager ilkesine tabi olan API, API.

Alt sınır olarak, ocsp.enable ve ocsp.responderURL değerlerinden birini belirtmelisiniz.

Özellik Adı	Tanım
ocsp.enable	Bu özelliğin değeri `true` ya da `false`değeridir. `true`ise, sertifika iptal denetimi yaparken OCSP denetimi etkinleştirilir; `false` ise ya da ayarlanmazsa, OCSP denetimi devre dışı bırakılır.
ocsp.responderURL	Bu özelliğin değeri, OCSP yanıtlayıcıya ait konumu tanımlayan bir URL 'dir. Burada bir örnek vardır; `ocsp.responderURL=http://ocsp.example.net:80`. Varsayılan olarak, OCSP yanıtlayıcının yeri, doğrulanmakta olan sertifikadan örtük olarak belirlenir. Bu özellik, Yetki Bilgileri (Authority Information Access) uzantısı (RFC 3280 'de tanımlı) sertifikadan eksik olduğunda ya da geçersiz kılma işlemi gerektirdiğinde kullanılır.
ocsp.responderCertSubjectName	Bu özelliğin değeri, OCSP yanıtlayıcısı sertifikasının konu adıdır. Burada bir örnek vardır; `ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"`. Varsayılan olarak, OCSP yanıtlayıcısının sertifikası, doğrulanmakta olan sertifikayı veren kullanıcının sertifikasına sahip olur. Bu özellik, varsayılan değer uygulanmadığında OCSP yanıtlayıcıya ilişkin sertifikayı tanıtır. Bu değer, RFC 2253 'de tanımlanan, sertifika kümesindeki bir sertifikayı tanıtan ayırt edici ad (RFC 2253) ile tanımlanır. Yalnızca konu adının sertifikayı benzersiz bir şekilde tanımlamak için yeterli olmadığı durumlarda, bunun yerine hem ocsp.responderCertIssuerName hem de ocsp.responderCertSerialNumber özelliklerinin kullanılması gerekir. Bu özellik ayarlandığında, ocsp.responderCertIssuerName ve ocsp.responderCertSerialNumber özellikleri yoksayılır.
ocsp.responderCertIssuerName	Bu özelliğin değeri, OCSP yanıtlayıcısının sertifikasının sertifika veren adıdır. Burada bir örnek vardır; `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Varsayılan olarak, OCSP yanıtlayıcısının sertifikası, doğrulanmakta olan sertifikayı veren kullanıcının sertifikasına sahip olur. Bu özellik, varsayılan değer uygulanmadığında OCSP yanıtlayıcıya ilişkin sertifikayı tanıtır. Bu değer, RFC 2253 'de tanımlanan, sertifika kümesindeki bir sertifikayı tanıtan ayırt edici ad (RFC 2253) ile tanımlanır. Bu özellik ayarlandığında, ocsp.responderCertSerialNumber özelliğinin de ayarlanması gerekir. ocsp.responderCertSubjectName özelliği ayarlandığında bu özellik yok sayılır.
ocsp.responderCertSerialNumber	Bu özelliğin değeri, OCSP yanıtlayıcının sertifikasının seri numarasıdır. Burada bir örnek vardır; `ocsp.responderCertSerialNumber=2A:FF:00`. Varsayılan olarak, OCSP yanıtlayıcısının sertifikası, doğrulanmakta olan sertifikayı veren kullanıcının sertifikasına sahip olur. Bu özellik, varsayılan değer uygulanmadığında OCSP yanıtlayıcıya ilişkin sertifikayı tanıtır. Bu değer, cert yolu geçerlilik denetimi sırasında sağlanan sertifikalar kümesindeki bir sertifikayı tanıtan onaltılı sayılardan oluşan bir dizilimdir (iki nokta ya da boşluk ayırıcısı olabilir). Bu özellik ayarlandığında, ocsp.responderCertIssuerName özelliğinin de ayarlanması gerekir. ocsp.responderCertSubjectName özelliği ayarlandığında bu özellik yok sayılır.

OCSP ' yi bu şekilde etkinleştirmeden önce, dikkat edilmesi gereken noktalar vardır:

- OCSP yapılanışının ayarlanması, JVM işlemindeki tüm güvenli yuvaları etkiler. Bazı durumlarda, JVM TLS güvenli yuvalarını kullanan diğer uygulama kodlarıyla paylaşıldığında bu yapılandırmanın istenmeyen

yan etkileri olabilir. Seçilen OCSP yapılandırmasının, aynı JVM içinde çalışmakta olan tüm uygulamalar için uygun olduğundan emin olun.

- JRE ' nize bakım uygulanması, java.security dosyasının üzerine yazılabilir. java.security dosyasının üzerine yazılmasını önlemek için Java ara düzeltmelerini ve ürün bakımını uyguladığınızda dikkatli olun. Bakım uyguladıktan sonra java.security değişikliklerinizi yeniden uygulamak gerekebilir. Bu nedenle, bunun yerine java.security.Security.setProperty() API 'sini kullanarak OCSP yapılandırmasını ayarlamayı düşünebilirsiniz.
- OCSP denetiminin etkinleştirilmesi, yalnızca iptal denetimi de geçerli kılındığında bir etkiye sahiptir. Geri alma denetimi, `PKIXParameters.setRevocationEnabled()` yöntemi tarafından etkinleştirilir.
- Yerel algılayıcılarda OCSP denetlemesi etkinleştiriyoriçinde açıklanan AMS Java Interceptor olanağını kullanıyorsanız, anahtar deposu yapılanış kütüğündeki AMS OCSP yapılanışlarıyla çakışan bir java.security OCSP yapılanışını kullanmaktan kaçınmak için dikkatli olun.

Sertifika İptal Listeleri ve Yetki İptal Listeleriyle Çalışma

CRL ve ARL ' ler içinIBM MQ desteği platforma göre değişir.

Her platform için CRL ve ARL desteği aşağıdaki gibidir:

- z/OSüzerinde, System SSL, Tivoli Public Key Infrastructure ürünü tarafından LDAP sunucularında saklanan CRL 'leri ve ARL' leri destekler.
- Diğer platformlarda, CRL ve ARL desteği, PKIX X.509 V2 CRL profili önerileri ile uyumludur.

IBM MQ , önceki 12 saat içinde erişilen CRL ve ARL ' lerin önbelleğini tutar.

Bir kuyruk yöneticisi ya da IBM MQ MQI client bir sertifika aldığında, sertifikenin geçerli olduğunu onaylamak için CRL ' yi denetler. Önbellek varsa,IBM MQ önce önbellekteki ilk denetimleri yapar. CRL önbellekte değilse, IBM MQ , LDAP CRL sunucusu yerlerini *SSLCRLNL* özniteliğinde belirtilen kimlik doğrulama bilgileri nesnelerinin ad listesinde yer aldıklarında, IBM MQ kullanılabilir bir CRL buluncaya kadar sorgular. Ad listesi belirlenmezse ya da boş bir değerle belirtildiyse, CRL ' ler denetlenmez.

LDAP sunucularının ayarlanması

LDAP Dizin Bilgileri Ağaç yapısını, CU ' ların Ayırt Edici Adları sıradüzenini yansıtacak şekilde yapılandırın. Bunu, LDAP Veri Değişimi Biçimi dosyalarını kullanarak yapın.

Sertifikalar ve CRL 'ler veren CA' nın Ayırt Edici Adları 'na karşılık gelen hiyerarşiyi kullanmak için LDAP Dizin Bilgileri Ağacı (DIT) yapısını yapılandırın. DIT yapısını, LDAP Data Interchange Format (LDIF) kullanan bir dosyayla ayarlayabilirsiniz. Bir dizini güncellemek için LDIF dosyalarını da kullanabilirsiniz.

LDIF dosyaları, bir LDAP dizinindeki nesneleri tanımlamak için gereken bilgileri içeren ASCII metin dosyalarıdır. LDIF dosyaları, her biri bir Ayırt Edici Ad, en az bir nesne sınıfı tanımlaması ve isteğe bağlı olarak birden çok öznitelik tanımlaması oluşturan bir ya da daha fazla giriş içerir.

`certificateRevocationList;binary` özniteliği, iptal edilen kullanıcı sertifikalarının ikili biçiminde bir listesini içerir. `authorityRevocationList;binary` özniteliği, iptal edilen CA sertifikalarının ikili bir listesini içerir. IBM MQ TLS ile kullanım için, bu özniteliklere ilişkin ikili veri, DER (Definite Encoding Rules) biçimine uymalıdır. LDIF dosyalarıyla ilgili ek bilgi için, LDAP sunucunuzla birlikte sağlanan belgelere bakın.

Şekil 20 sayfa 329 shows a sample LDIF file that you might create as input to your LDAP server to load the CRLs and ARLs issued by CA1, which is an imaginary Certificate Authority with the Distinguished Name "CN=CA1, OU=Test, O=IBM, C=GB", set up by the Test organization within IBM.

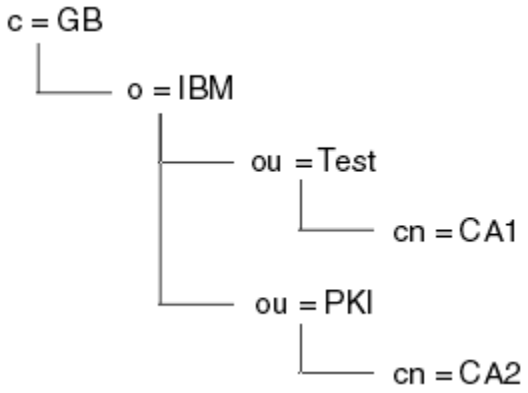
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

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)
```

Şekil 20. Bir Sertifika Yetkilisi için örnek LDIF dosyası. Bu, somutlamaya uygulanmasına kadar değişebilir.

Şekil 21 sayfa 329 , Şekil 20 sayfa 329 içinde gösterilen örnek LDIF dosyasını CA2ile birlikte gösterilen örnek LDIF dosyasını, PKI kuruluşu tarafından ayarlanan hayali bir Sertifika Yetkilisi (IBM) içinde deloadiçinde yüklediğinizde, LDAP sunucunuzun yarattığı DIT yapısını gösterir.



Şekil 21. LDAP Dizin Bilgileri Ağaç yapısı örneği

WebSphere MQ , hem CRL 'leri hem de ARL' leri denetler.

Not: LDAP sunucunuza ilişkin erişim denetimi listesinin, yetkili kullanıcıların CRL 'leri ve ARL' leri tutan girişleri okumasına, aramasına ve karşılaştırabilmelerine izin verdiğinden emin olun. WebSphere MQ , AUTHINFO nesnesinin LDAPUSER ve LDAPPWD özelliklerini kullanarak LDAP sunucusuna erişir.

LDAP sunucularının yapılandırılması ve güncellenmesi
LDAP sunucunuzu yapılandırmak ya da güncellemek için bu yordamı kullanın.

1. CRL 'leri ve ARL' leri Sertifika Yetkiliniz ya da Yetkililerden DER biçiminde edinin.
2. LDAP sunucunuzla birlikte sağlanan bir metin düzenleyicisini ya da aracı kullanarak, CA ' nın Ayırt Edici Adını ve gerekli nesne sınıfı tanımlarını içeren bir ya da daha çok LDIF dosyası yaratın. DER biçim verilerini LDIF dosyasına, CRL 'ler için `certificateRevocationList;binary` özniteliğinin değerleri, ARL' ler için `authorityRevocationList;binary` özniteliği ya da her ikisi olarak kopyalayın.
3. LDAP sunucunuzu başlatın.
4. Add the entries from the LDIF file or files you created at step “2” sayfa 329.

LDAP CRL sunucunuzu yapılandırdıktan sonra, doğru bir şekilde ayarlandığından emin olun. Önce, kanalda iptal edilmeyecek bir sertifika kullanmayı deneyin ve kanalın doğru olarak başlatılıp başlatılmadığına bakın. Daha sonra iptal edilen bir sertifikayı kullanın ve kanalın başlatılamadığını denetleyin.

Güncellenmiş CRL ' leri Sertifika Yetkilileri 'nden sık sık edinin. Bunu, her 12 saatte bir LDAP sunucularınızda yapmayı düşünün.

Bir kuyruk yöneticisiyle CRL 'ler ve ARL' lere erişme

Kuyruk yöneticisi, bir LDAP CRL sunucusunun adresini tutan bir ya da daha fazla kimlik doğrulama bilgisi nesnesiyle ilişkilendirildi. IBM i IBM i üzerindeIBM MQ , diğer platformlardan farklı şekilde davranır.

Bu bölümde, CRL ' ler (Sertifika İptal Listeleri) için Yetki İptal Listeleri (ARL) için de geçerli olduğunu unutmayın.

Kuyruk yöneticisine, her biri bir LDAP CRL sunucusunun adresini bulunduran kimlik doğrulama bilgileri nesneleriyle kuyruk yöneticisini sağlayarak CRL ' lere nasıl erişileceğini anlatıyorsunuz. Kimlik doğrulama bilgileri nesneleri, *SSLCRLNL* kuyruk yöneticisi öznitelemesinde belirtilen bir ad listesinde tutulur.

Aşağıdaki örnekte, değiştirgeleri belirtmek için MQSC kullanılır:

1. CRLLDAP olarak ayarlanmış AUTHTYPE parametresiyle DEFE AUTHINFO MQSC komutunu kullanarak kimlik doğrulama bilgileri nesnelerini tanımlayın. IBM i IBM iüzerinde, CRTMQMAUTI CL komutunu da kullanabilirsiniz.

   AUTHTYPE parametresine ilişkin CRLLDAP değeri, LDAP sunucularında CRL ' lerin erişildiğini gösterir. Yarattığınız her kimlik doğrulama bilgileri nesnesi, oluşturduğunuz bir LDAP sunucusunun adresini içerir. Birden çok kimlik doğrulama bilgisi nesnesiniz varsa, gösterdikleri LDAP sunucularının aynı bilgileri içermesi gerekir. Bu, bir ya da daha fazla LDAP sunucusunun başarısız olması durumunda hizmet sürekliliğini sağlar.

   z/OS Buna ek olarak, yalnızca z/OS üzerinde, tüm LDAP sunucularına aynı kullanıcı kimliği ve parola kullanılarak erişilmelidir. Kullanılan kullanıcı kimliği ve parola, ad listesindeki ilk AUTHINFO nesnesinde belirtilenlerdir.

   Tüm altyapılarda, kullanıcı kimliği ve parola LDAP sunucusuna şifrelenmemiş olarak gönderilir.
2. DEFINE NAMELIST MQSC komutunu kullanarak, kimlik doğrulama bilgileri nesnelerine ilişkin adlara ilişkin bir ad listesi tanımlayın. z/OS z/OSüzerinde, NLTYPE ad listesi özniteliğinin AUTHINFO olarak ayarlandığından emin olun.
3. ALTER QMGR MQSC komutunu kullanarak, ad listesini kuyruk yöneticisine belirtin. Örneğin:

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   Burada `sslcrlnlname` , kimlik doğrulama bilgileri nesnelerinin namelisten'inidir.

   Bu komut, *SSLCRLNL*adlı bir kuyruk yöneticisi özniteliğini ayarlar. Kuyruk yöneticisinin bu özniteliğe ilişkin ilk değeri boş.

IBM i IBM i' ta, kimlik doğrulama bilgileri nesnelerini belirtebilirsiniz, ancak kuyruk yöneticisi kimlik doğrulama bilgisi nesnelerini ya da kimlik doğrulama bilgileri nesneleri için bir ad listesi kullanır. Yalnızca, bir IBM i kuyruk yöneticisi tarafından oluşturulan istemci bağlantısı çizelgesini kullanan IBM MQ istemcileri, o IBM i kuyruk yöneticisi için belirtilen kimlik doğrulama bilgilerini kullanır. IBM i üzerindeki *SSLCRLNL* kuyruk yöneticisi özniteliği, bu istemcilerin hangi kimlik doğrulama bilgilerini kullanabileceğini belirler. Bir IBM i kuyruk yöneticisine CRL ' lere nasıl erişileceğini söylemeyle ilgili bilgi için bkz. “IBM i'ta CRL ve ARL' lere erişme” sayfa 330 .

Bir ya da daha fazla LDAP sunucusunun başarısız olması durumunda hizmet sürekliliğinin sağlanması için, ad listesine alternatif LDAP sunucularına en çok 10 bağlantı ekleyebilirsiniz. LDAP sunucularının aynı bilgileri içermesi gerektiğini unutmayın.

IBM i *IBM i'ta CRL ve ARL' lere erişme*

IBM i'ta CRL' ler ya da ARL ' lere erişmek için bu yordamı kullanın.

Bu bölümde, CRL ' ler (Sertifika İptal Listeleri) için Yetki İptal Listeleri (ARL) için de geçerli olduğunu unutmayın.

IBM i' ta belirli bir sertifika için bir CRL konumu ayarlamak üzere aşağıdaki adımları izleyin:

1. Access the DCM interface, as described in “DCM Olanağına Erişilmesi” sayfa 262.
2. Gezinme panosundaki **CRL konumlarını yönet** görev kategorisinde **CRL konumu ekle**seçeneğini tıklatın. Görev çerçevesinde CRL Konumlarını Yönet sayfası görüntülenir.
3. **CRL Konum Adı** alanına bir CRL konum adı yazın; örneğin, LDAP `Server #1`
4. **LDAP Server** (LDAP Sunucusu) alanında LDAP sunucusu adını yazın.
5. In the **SSL (Güvenli Yuva Arabirimi Katmanı) olanağını kullan** field, select **Evet** if you want to connect to the LDAP server using TLS. Tersi durumda **No**(Hayır) seçeneğini belirleyin.
6. **Port Number** (Kapı Numarası) alanına, LDAP sunucusu için bir kapı numarası yazın (örneğin, 389).
7. If your LDAP server does not allow anonymous users to query the directory, type a login distinguished name for the server in the **oturum açma belirleyici adı** field.
8. **Tamam** düğmesini tıklatın. DCM, CRL konumunu oluşturduğunu size bildirir.
9. Gezinme panosunda, **Select a Certificate Store**(Sertifika Deposu Seç) seçeneğini tıklatın. Bir Sertifika Deposu Seç sayfası, görev çerçevesinde görüntülenir.
10. **Diğer Sistem Sertifika Deposu** onay kutusunu seçin ve **Devam**düğmesini tıklatın. Sertifika Deposu ve Parola sayfası görüntülenir.
11. **Sertifika deposu yolu ve dosya adı** alanında, “IBM iüzerinde bir sertifika deposu oluşturma” sayfa 263olduğunda ayarladığınız IFS yolunu ve dosya adını yazın.
12. **Certificate Store Password** (Sertifika Deposu Parolası) alanına bir parola yazın. **Devam**düğmesini tıklatın. Geçerli Sertifika Deposu sayfası, görev çerçevesinde görüntülenir.
13. Gezinme panosundaki **Sertifikaları Yönet** görev kategorisinde **CRL konum atamasını güncelle**seçeneğini tıklatın. CRL Konumu Ataması sayfası görev çerçevesinde görüntülenir.
14. CRL konumunu atamak istediğiniz CA sertifikasına ilişkin radyo düğmesini seçin. **CRL Konumu Atamasını Güncelle**seçeneğini tıklatın. Görev çerçevesinde, CRL Konumu Ataması sayfasını Güncelle sayfası görüntülenir.
15. Sertifiya atamak istediğiniz CRL konumu için radyo düğmesini seçin. **Atamayı Güncelle**düğmesini tıklatın. DCM, atamayı güncellediğini size bildirir.

DCM ' nin, Sertifika Yetkilisi tarafından farklı bir LDAP sunucusu atamanıza izin verdiğini unutmayın.

Accessing CRLs and ARLs using IBM MQ Explorer
Bir kuyruk yöneticisine, CRL 'lere nasıl erişileceğini bir kuyruk yöneticisine anlatmak için IBM MQ Explorer ' u kullanabilirsiniz.

Bu bölümde, CRL ' ler (Sertifika İptal Listeleri) için Yetki İptal Listeleri (ARL) için de geçerli olduğunu unutmayın.

Bir CRL ' ye LDAP bağlantısı kurmak için aşağıdaki yordamı kullanın:

1. Kuyruk yöneticinizi başlattığınızdan emin olun.
2. **Kimlik Doğrulama Bilgileri** klasörünü sağ tıklatın ve **Yeni-> Kimlik Doğrulama Bilgileri**seçeneklerini belirleyin. Açılan özellik yaprağında:
   a. İlk sayfa **Kimlik Doğrulama Bilgileri Oluştur**sayfasında CRL (LDAP) nesnesi için bir ad girin.
   b. **Özellikleri Değiştir**' in **Genel** sayfasında bağlantı tipini seçin. İsteğe bağlı olarak bir tanım girebilirsiniz.
   c. **Change Properties**(Özellikleri Değiştir) sayfasının **CRL (LDAP)** (CRL) sayfasını seçin.
   d. LDAP sunucusu adını ağ adı ya da IP adresi olarak girin.
   e. Sunucu oturum açma ayrıntılarını gerektiriyorsa, bir kullanıcı kimliği ve gerekirse bir parola sağlayın.
   f. **Tamam**'ı tıklatın.

3. Namelists klasörünü farenin sağ düğmesiyle tıklatın ve **Yeni-> Ad listesi**öğelerini seçin. Açılan özellik yaprağında:
   a. Ad listesi için bir ad yazın.
   b. CRL (LDAP) nesnesinin adını (“2.a” sayfa 331 adımından) ekleyin. listeye girsin.
   c. **Tamam**'ı tıklatın.
4. Kuyruk yöneticisini sağ tıklatın, **Özellikler**' i seçin ve **SSL** sayfasını seçin:
   a. **Bu kuyruk yöneticisinin aldığı sertifikaları Onay Listelerine göre denetle** onay kutusunu seçin.
   b. Type the name of the namelist (from step “3.a” sayfa 332) in the **CRL Ad Listesi** field.

Accessing CRLs and ARLs with an IBM MQ MQI client

Bir IBM MQ MQI clienttarafından kontrol etmek üzere CRL ' leri tutan LDAP sunucularını belirlemek için üç seçeneğiniz vardır.

Bu bölümde, CRL ' ler (Sertifika İptal Listeleri) için Yetki İptal Listeleri (ARL) için de geçerli olduğunu unutmayın.

LDAP sunucularını belirlemenin üç yolu aşağıdaki gibidir:

- Kanal tanımlama çizelgesinin kullanılması
- MQCONNX çağrısında SSL yapılandırma seçenekleri yapısının kullanılması, MQSCO
- Active Directory (Active Directory desteğiyle Windows sistemlerinde) kullanılması

Daha fazla ayrıntı için, ilgili bilgilere bakın.

Bir ya da daha fazla LDAP sunucusunun başarısız olması durumunda hizmetin sürekliliğini sağlamak için alternatif LDAP sunucularına en fazla 10 bağlantı ekleyebilirsiniz. LDAP sunucularının aynı bilgileri içermesi gerektiğini unutmayın.

You cannot access LDAP CRLs from an IBM MQ MQI client channel running on Linux (zSeries platform).

Bir OCSP yanıtlayıcıya ve CRL ' leri tutan LDAP sunucularının konumu

Bir IBM MQ MQI client sisteminde, sertifika iptal listelerini (CRL ' ler) tutan bir OCSP yanıtlayıcısı ve LDAP (Lightweight Directory Access Protocol; Temel Dizin Erişimi Protokolü) sunucularının konumunu belirleyebilirsiniz.

Bu konumları, burada açıklanan üç şekilde, azalan öncelik sırasına göre belirleyebilirsiniz.

IBM i IBM iiçin bkz. IBM i'ta CRL ve ARL' lere erişme.

Bir IBM MQ MQI client uygulaması bir MQCONNX çağrısı yayınladığında

MQCONNX çağrısında bir OCSP yanıtlayıcısı ya da bir LDAP sunucusu tutan CRL ' leri belirtebilirsiniz.

Bir **MQCONNX** çağrısında, bağlantı seçenekleri yapısı, MQCNO, SSL yapılandırma seçenekleri yapısına gönderme yapabilir, MQSCO. Buna karşılık, MQSCO yapısı bir ya da daha fazla kimlik doğrulama bilgisi kaydı yapılarına (MQAIR) gönderme yapabilir. Each MQAIR structure contains all the information an IBM MQ MQI client requires to access an OCSP responder or an LDAP server holding CRLs. Örneğin, bir MQAIR yapısındaki alanlardan biri, yanıt verenin iletişim kurabileceği URL 'dir. MQAIR yapısı hakkında daha fazla bilgi için bkz. MQAIR-Authentication information record.

OCSP yanıtlayıcıya ya da LDAP sunucularına erişmek için istemci kanal tanımlama çizelgesi (ccdt) kullanılması

IBM MQ MQI client , CRL ' leri tutan bir OCSP yanıtlayıcıya ya da LDAP sunucularına erişebilmesi için, bir istemci kanalı tanımlama çizelgesindeki bir ya da daha çok kimlik doğrulama bilgisi nesnesinin özniteliklerini içerir.

Bir sunucu kuyruk yöneticisininde, bir ya da daha fazla kimlik doğrulama bilgisi nesnesi tanımlayabilirsiniz. Bir kimlik doğrulama nesnesinin öznitelikleri, bir OCSP yanıtlayıcıya (OCSP 'nin desteklendiği altyapılarda)

ya da CRL' leri tutan bir LDAP sunucusuna erişmek için gereken tüm bilgileri içerir. Öznitelikler den biri, OCSP yanıtlayıcı URL 'sini, başka bir kullanıcının anasistem adresini ya da LDAP sunucusunun çalıştığı bir sistemin IP adresini belirtir.

z/OS IBM i AUTHTYPE (OCSP) olan bir kimlik doğrulama bilgileri nesnesi, IBM i ya da z/OS kuyruk yöneticilerindeki kullanım için geçerli değildir; ancak, istemci kullanımı için istemci kanal tanımlama çizelgesine (CCDT) kopyalanmak üzere bu altyapılarda belirtilebilir.

IBM MQ MQI client 'in CRL' leri tutan bir OCSP yanıtlayıcıya ya da LDAP sunucularına erişmesini sağlamak için, bir ya da daha fazla kimlik doğrulama bilgisi nesnesinin öznitelikleri bir istemci kanal tanımlama çizelgesine eklenebilir. Bu tür öznitelikleri aşağıdaki yollardan biriyle ekleyebilirsiniz:

Multi

Sunucu platformlarında AIX, Linux, IBM i, Solarisve Windows

Bir ya da daha fazla kimlik doğrulama bilgisi nesnesinin adlarını içeren bir ad listesi tanımlayabilirsiniz. Daha sonra, kuyruk yöneticisi özniteliğini **SSLCRLNL**adını bu ad listesinin adıyla ayarlayabilirsiniz.

CRL ' ler kullanıyorsanız, daha yüksek kullanılabilirlik sağlamak üzere birden çok LDAP sunucusu yapılandırılabilir. Amaç, her LDAP sunucusunun aynı CRL ' leri tutması. Bir LDAP sunucusu gerekliyse, bir LDAP sunucusu kullanılamıyorsa, IBM MQ MQI client başka bir sunucuya erişmeyi deneyebilir.

Ad listesi tarafından tanımlanan kimlik doğrulama bilgileri nesnelerinin öznitelikleri burada toplu olarak *sertifika iptal konumu*olarak anılır. Kuyruk yöneticisi özniteliğini (**SSLCRLNL**), ad listesinin adına ayarladığınızda, sertifika iptal konumu, kuyruk yöneticisiyle ilişkilendirilmiş istemci kanalı tanımlama çizelgesine kopyalanır. CCDT 'ye bir istemci sisteminden paylaşılan bir dosya olarak erişilebilmesi ya da CCDT' nin istemci sistemine kopyalanması durumunda, bu sistemdeki IBM MQ MQI client , CRL 'leri tutan bir OCSP yanıtlayıcıya ya da LDAP sunucularına erişmek için CCDT' deki sertifika iptal konumunu kullanabilir.

Kuyruk yöneticisinin sertifika iptal konumu daha sonra değiştirilirse, değişiklik kuyruk yöneticisiyle ilişkili CCDT ' ye yansıtılır. Kuyruk yöneticisi özniteliği **SSLCRLNL**boş olarak ayarlandıysa, sertifika iptal konumu CCDT ' den kaldırılır. Bu değişiklikler, bir istemci sistemindeki çizelgenin herhangi bir kopyasına yansıtılmaz.

Bir MQI kanalının istemci ve sunucu uçlarında sertifika iptal konumunun farklı olmasını istiyorsanız ve sunucu kuyruk yöneticisi, sertifika iptal konumunu yaratmak için kullanılan sunucu kuyruk yöneticisiyse, bunu aşağıdaki gibi yapabilirsiniz:

1. Sunucu kuyruk yöneticisininde, istemci sisteminde kullanılmak üzere sertifika iptal konumunu yaratın.
2. Sertifika iptali konumunu içeren CCDT ' yi istemci sistemine kopyalayın.
3. Sunucu kuyruk yöneticisinde, sertifika iptal konumunu, MQI kanalının sunucu ucunda gerekli olan bir yere değiştirin.
4. On the client machine, you can use the **runmqsc** command with the **-n** parameter.

Multi

İstemci altyapılarında AIX, Linux, IBM i , Solarisve Windows

You can build a CCDT on the client machine by using the runmqsc command with the **-n** parameter and **DEFINE AUTHINFO** objects in the CCDT file. Nesnelerin tanımlı olduğu sıra, bunların dosyada kullanılanlarla sıralanır. Bir **DEFINE AUTHINFO** nesnesinde kullanabileceğiniz herhangi bir ad dosyada tutulmaz. Bir CCDT dosyasındaki **AUTHINFO** nesnelerini **DISPLAY** yaparken, yalnızca konumsal sayılar kullanılır.

Not: -n parametresini belirtirseniz, başka bir parametre belirtmemeniz gerekir.

Windowsüzerinde Active Directory ' in kullanılması

Windows

Windows sistemlerinde, geçerli CRL bilgilerini Active Directory' de yayınlamak için **setmqcrl** denetim komutunu kullanabilirsiniz.

setmqcrl komutu OCSP bilgilerini yayınlamıyor.

Bu komutla ve sözdizimiyle ilgili bilgi için bkz. setmqcrl.

Accessing CRLs and ARLs with IBM MQ classes for Java and IBM MQ classes for JMS

IBM MQ classes for Java ve IBM MQ classes for JMS erişim CRL ' leri diğer platformlardan farklı olarak erişim sağlar.

For information about working with CRLs and ARLs with IBM MQ classes for Java, see Sertifika iptal listelerini kullanma

For information about working with CRLs and ARLs with IBM MQ classes for JMS, see SSLCERTSTORS nesne özelliği

Kimlik Doğrulama Bilgileri Nesnelerinin Kullanılması

Kimlik doğrulama bilgileri nesnelerini MQSC ya da PCF komutlarını ya da IBM MQ Explorerkomutunu kullanarak değiştirebilirsiniz.

Aşağıdaki MQSC komutları kimlik doğrulama bilgileri nesneleri üzerinde işlem sağlar:

- DEFINE YAZAR
- ALTER AUTHINFO
- YAZAR BILGILERINI SIL
- AUTHENTICAFO GÖRÜNTÜLE

Bu komutlara ilişkin eksiksiz açıklamalar için MQSC komutlarıbaşlıklı konuya bakın.

Aşağıdaki Programlanır Komut Biçimi (PCF) komutları, kimlik doğrulama bilgileri nesnelerine göre hareket eder:

- Kimlik Doğrulama Bilgileri Oluştur
- Kimlik Doğrulama Bilgilerini Kopyala
- Kimlik Doğrulama Bilgilerini Değiştir
- Kimlik Doğrulama Bilgilerini Sil
- Kimlik Doğrulama Bilgilerini Sorgula
- Kimlik Doğrulama Bilgileri Adları

Bu komutlara ilişkin eksiksiz açıklamalar için Programlanır Komut Biçimlerinin Tanımlamalarıbaşlıklı konuya bakın.

Kullanılabilir olduğu platformlarda, IBM MQ Explorer' u da kullanabilirsiniz.

Linux UNIX Pluggable Authentication Method (PAM) olanağının kullanılması

PAM olanağını yalnızca UNIX and Linux altyapılarında kullanabilirsiniz. Tipik bir UNIX sisteminin, geleneksel kimlik doğrulama mekanizmasını uygulayan PAM modülleri vardır; ancak, daha fazlası da olabilir. Parolaların doğrulanmasına ilişkin temel görevin yanı sıra, ek kurallar taşımak için PAM modülleri de çağrılabilir.

Yapılandırma dosyaları, her bir uygulama için hangi kimlik doğrulama yönteminin kullanılacağını tanımlar. Örnek uygulamalar standart uçbirim oturum açma, ftp ve telnet bilgilerini içerir.

PAM ' in avantajı, uygulamanın, kullanıcı kimliğinin gerçekte nasıl doğrulanmakta olduğunu bilmesi ya da önemsememesine gerek olmadığını göstermektedir. Uygulama, PAM ' ye doğru bir kimlik doğrulama verisi sağlayabildiği sürece, arkasındaki mekanizma şeffaf olur.

Kimlik doğrulama verileri biçimi, kullanılmakta olan sisteme bağlıdır. Örneğin, IBM MQ , değiştirgelerden (MQCONNX API çağrısında kullanılan MQCSP yapısı gibi) bir parola alır.

Önemli: You cannot set the **AUTHENMD** attribute until you install IBM MQ 8.0.0 Fix Pack 3, and then restart the queue manager, using a **-e CMDLEVEL=***düzey* of *802* (on the strmqm command) to set the command level you require.

Sisteminizin PAM ' yi kullanacak şekilde yapılandırılması

The service name used by IBM MQ, when invoking PAM, is *ibmq*.

Bir IBM MQ kuruluşunun, farklı işletim sistemleri için bilinen varsayılan değerlere dayalı olarak işletim sistemi kullanıcılarından bağlantılara izin veren bir varsayılan PAM yapılandırmasını sürdürmeye çalışacağına dikkat edin.

Ancak, sistem denetimciniz `/etc/pam.conf`ya da `/etc/pam.d/ibmmq`dosyasında tanımlı olan kuralları doğrulamalıdır, ancak dosyalar hala uygundur.

Nesnelere erişim yetkisi verme

Bu bölümde, nesnelere erişimi denetlemek için nesne yetkisi yöneticisi ve kanal çıkış programlarının kullanılmasına ilişkin bilgiler yer alır.

ULW UNIX, Linux, and Windows sistemlerinde. Nesne yetkisi yöneticisini (OAM) kullanarak nesnelere erişimi denetliyorsunuz. Bu konu grubunda, OAM için komut arabiriminin kullanılmasına ilişkin bilgiler yer alır.

Bu bölümde ayrıca, tüm platformlarda sisteminize güvenlik uygulamak için hangi görevlerin gerçekleştirileceğini belirlemek üzere kullanabileceğiniz bir denetim listesi ve kullanıcılara IBM MQ yönetme ve IBM MQ nesneleriyle çalışma yetkisi verilmesine ilişkin dikkat edilmesi gereken noktalar yer alır.

eğer sağlanan güvenlik mekanizmaları ihtiyaçlarınızı karşılamazsa, kendi kanal çıkış programlarınızı geliştirebilirsiniz.

Yetki için hangi kullanıcının kullanıldığının belirlenmesi

Kaynaklara erişim yetkisi, kullanıcının üyesi olduğu gruplara ya da belirli kiplerde, doğrudan bağlantıyla ilişkili kullanıcıya verilir. Bağlantı işlemi sırasında ve özellikle uzak (istemci) bağlantılar için, bu kimlik kuyruk yöneticisinin yapılandırması tarafından değiştirilebilir. Bu sayfa, IBM MQ ürününün farklı özelliklerini ve bu özelliklerin yapılandırma seçeneklerini listeler. Bu seçenekler, bağlantı kuran bir uygulamanın kimliğini ve bu özelliklerin yürürlüğe girdiği öncelik sırasını etkileyebilir.

Hangi kullanıcının benimsendiğini değiştirebilen özellikler

Hangi kullanıcının yetkilendirilmesi gerektiğini ayarlayabilecek farklı özellikler şunlardır:

Uygulama tarafından bildirilir kullanıcı
IBM MQtarafından bir uzak bağlantı başlatıldığında, işlemin çalıştığı işletim sistemi kullanıcısı, alan kuyruk yöneticisine gönderilir. Kullanıcıyı değiştiren başka bir yapılandırma yoksa, yetkilendirme denetimi için kullanılabilecek bir kullanıcı olduğundan emin olmak için bu kullanıcı gönderilir.

Bağlantıların herhangi bir sunucu tarafı doğrulaması olmadan kimliklerini belirtmesine izin verdiğinden, bu kullanıcının yetki temeli olarak kullanılması önerilmez. Bu, yönetimle görevli kullanıcıyı ('mqm ') da içerebilir.

Kanal MCAUSER ayarı
Ağ bağlamaları aracılığıyla bağlanan uygulamalar bunu bir IBM MQ kanal tanımı kullanılarak yapar. Kanal tanımları, bağlanan uygulamalar tarafından bildirilen kullanıcı yerine yetkilendirme için kullanılacak farklı bir kullanıcı belirtmek için kullanılabilecek **MCAUSER** özniteliğini destekler.

Bağlantı doğrulaması ADOPTCTX
Uygulamalar, kimlik doğrulama amacıyla bir kuyruk yöneticisine gönderilecek bir kullanıcı ve parola belirleyebilir. Bu kimlik bilgilerinin kimliği, Bağlantı Kimlik Doğrulaması özelliği için belirtilen yapılandırma kullanılarak doğrulanır. Bağlantı Kimlik Doğrulaması için **ADOPTCTX** seçeneği, bir kullanıcının başarıyla doğrulandıktan sonra yetkilendirme için kullanılıp kullanılmayacağını denetler. YES(EVET) olarak ayarlanırsa, kimlik doğrulaması için sağlanan kullanıcı yetkilendirme denetimleri için kullanılır.

Kanal kimlik doğrulama kaydı MCAUSER
Bağlantı işlenirken kuyruk yöneticisi, bağlantıyla eşleşen bir kanal kimlik doğrulama kaydı bulmaya çalışır. Bir kanal kimlik doğrulama kaydı eşleşirse ve **USERSRC** öznitelik değeri MAPolarak ayarlanırsa, IBM MQ yetkilendirmeler için kullanılan kullanıcıyı **MCAUSER** özniteliğinin değeriyle değiştirir.

Güvenlik çıkışları
Güvenlik çıkışları, IBM MQ güvenlik işlemesi sırasında yazılıp çağrılabilen özel işlevlerdir. İşlev çağrıldığında, yetki denetimi için kullanılacak bağlantı kullanıcısıyla ilgili birkaç alanı içeren MQCD yapısının bir kopyasıyla birlikte verilir. Güvenlik çıkışları, yetkilendirilecek kullanıcıyı değiştirmek için bu alanları değiştirebilir.

öncelik sırası

Aşağıdaki çizelgede, IBM MQ yetki vermek üzere bir kullanıcı seçtiğinde “Hangi kullanıcının benimsendiğini değiştirebilen özellikler” sayfa 335 içinde açıklanan her güvenlik özelliği için öncelik sırası gösterilmektedir. Sıralama, en düşükten en yükseğe doğru, yani ilk satırdaki bir güvenlik özelliği ayarı, diğer satırların herhangi biri tarafından geçersiz kılınır.

Çizelge 68. Güvenlik özellikleri için öncelik sırası

Sipariş	**Özellik**
1 (en düşük)	Uygulama Bildirildi Tanıtıcısı
2	Kanal tanımlaması **MCAUSER** özniteliği
3	**ADOPTCTX(YES)** ile bağlantı kimlik doğrulaması
4	**USERSRC(MAP)** ile kanal kimlik doğrulama kayıtları
5 (en yüksek)	Güvenlik Çıkışı

Erken evlat edinmenin etkileri

Bağlantı kimlik doğrulaması ve kanal kimlik doğrulama kayıtları, bağlantı kimlik doğrulaması kullanıcı benimsemesinin ne zaman gerçekleştirileceğini denetleyen bir yapılandırma seçeneği sağlar. Bu ayar, erken benimseme olarak adlandırılır. Erken benimseme etkinleştirilirse, kanal kimlik doğrulama kayıtları işlenmeden önce bağlantı kimlik doğrulamasını benimseme gerçekleşir (bu, kanal kimlik doğrulama kayıtlarının herhangi bir **CONNAUTH** benimsemesini geçersiz kıldığı anlamına gelir).

Devre dışı bırakılırsa, sipariş tersine çevrilir; başka bir değişle, kanal kimlik doğrulama kayıtları **CONNAUTH** benimsemeden önce işlenir. Bu durumda, bağlantı kimlik doğrulamasının benimsenmesi, kanal kimlik doğrulamasının kaydedilmesi için daha yüksek etkili bir önceliğe sahiptir.

Erken benimseme için varsayılan ayar `enabled`(etkin) değeridir.

ULW Controlling access to objects by using the OAM on UNIX, Linux, and Windows

Nesne yetkisi yöneticisi (OAM), IBM MQ nesnelerine yetki verilmesi ve yetkiyi iptal etmek için bir komut arabirimi sağlar.

“UNIX, Linux, and Windowsüzerinde IBM MQ yönetimi yetkisi” sayfa 386' ta açıklandığı gibi, bu komutları kullanmak için uygun yetkiye sahip olmanız gerekir. IBM MQ ' ı yönetme yetkisi olan kullanıcı kimliklerinin

kuyruk yöneticisi için *super user* yetkisi vardır; bu yetki, bu kullanıcılara MQI isteklerini ya da komutlarını verme iznini daha fazla izin vermemeniz anlamına gelir.

Linux UNIX OAM user-based permissions on UNIX and Linux

From IBM MQ 8.0, on UNIX and Linux systems, the object authority manager (OAM) can use user-based authorization as well as group-based authorization.

IBM MQ 8.0' dan önce, UNIX and Linux üzerindeki erişim denetleme listeleri (EDL) yalnızca gruplara dayalıdır. From IBM MQ 8.0, ACLs are based on both user IDs and groups and you can use either the user-based model or the group-based model for authorization by setting the **SecurityPolicy** attribute to the appropriate value as described in Kurulabilir hizmetlerin yapılandırılması and UNIX ve Linuxüzerinde yetkilendirme hizmeti dayanaklarının yapılandırılması.

IBM MQ 8.0 ve sonraki yayın düzeylerindeki değişiklikler

From IBM MQ 8.0, when running with the user-based policy, some commands return different information from earlier versions of the product:

- **dmpmqaut** ve **dmpmqcfg** komutları, PCF eşdeğeri işlemlerini yapmak için kullanıcı tabanlı kayıtları gösterir.
- The OAM plug-in for IBM MQ Explorer shows user-based records and allows user-based modifications.
- OAM **Inquire** işlevi, kullanıcının yetenekli olduğunu gösteren sonuçlar döndürür.

Using the **-p** attribute on the **setmqaut** command does not grant access to all users in the same primary group, when user-based authorizations are enabled in the `qm.ini` file as described in qm.ini dosyasının hizmet kısmı.

Kullanıcı tabanlı yetkilendirmeyi kullanmaya ve birçok kullanıcıya sahip olmaya başlarsa, büyük olasılıkla AUTH kuyruğunda, grup tabanlı modelden daha fazla kayıt olacak ve doğrulama işlemi, doğrulamak için daha fazla kayıt olduğu için daha uzun sürebilir. bu artışın önemli olması beklenmiyor. Gerekirse, kullanıcı ve grup izinlerinin bir karışımının kullanılmasını kullanabilirsiniz.

Geçiş konuları

Modeli var olan bir kuyruk yöneticisi için gruptan kullanıcıya değiştirirseniz, anında etki olmaz. Önceden yapılmış olan yetkiler geçerli olmaya devam eder. Kuyruk yöneticisine bağlanan herhangi bir kullanıcı, önceki gibi aynı ayrıcalıkları alır: Tanıtımlarının ait olduğu tüm grupların birleşimidir. Kullanıcı kimlikleri için yeni **setmqaut** komutları verildiğinde, bunlar anında etki eder.

Kullanıcı ilkesiyle yeni bir kuyruk yöneticisi yaratırsanız, bu kuyruk yöneticisinin izinleri yalnızca onu yaratan kullanıcı için (genellikle `mqm` kullanıcı kimliği değil, olağan bir şekilde) izin veren bir kullanıcı için izinleri vardır. Ayrıca, `mqm` grubuna otomatik olarak verilen izinler de vardır. Ancak, birincil grup olarak `mqm` mqm 'i yoksa, `mqm` grubu ilk yetki kümesine dahil değildir.

Bir kullanıcıdan grup ilkesini taşırsanız, kullanıcı tabanlı yetkilendirmeler otomatik olarak silinmez. Ancak, bunlar artık izinler denetimi sırasında kullanılmıyorlar. İlkeyi tersine çevirmeden önce geçerli yapılandırmayı kaydedin, ilkeyi değiştirin, kuyruk yöneticisini yeniden başlatın ve daha sonra, komut dosyasını yeniden yürütün. Artık grup tabanlı bir kuyruk yöneticisi olduğundan, bu etki, kullanıcı kimliği kurallarının birincil gruba dayalı olarak saklandığından.

İlgili kavramlar

Nesne yetkisi yöneticisi (OAM)

UNIX, Linux ve Windows üzerindeki birincil kullanıcılar ve gruplar

qm.ini dosyasının hizmet kısmı

İlgili başvurular

crtmqm (kuyruk yöneticisi yarat) komutu

ULW UNIX, Linux, and Windowsüzerinde bir IBM MQ nesnesine erişim verme

Kullanıcılara ve kullanıcı gruplarına IBM MQ nesnelerine erişim izni vermek için **setmqaut** denetim komutunu, **SET AUTHREC** MQSC komutunu ya da **MQCMD_SET_AUTH_REC** PCF komutunu kullanın. IBM MQ Appliance ' da yalnızca **SET AUTHREC** komutunu kullanabildiğinizi unutmayın.

setmqaut denetim komutunun ve sözdiziminin tam tanımlı bir tanımı için bkz. setmqaut.

SET AUTHREC MQSC komutunun ve sözdiziminin tam tanımı için SET AUTHRECbaşlıklı konuya bakın.

MQCMD_SET_AUTH_REC PCF komutunun tam tanımı ve sözdizimiyle ilgili olarak bkz. Set Authority Record(Yetki Kayını Ayarla).

Bu komutu kullanmak için kuyruk yöneticisinin çalışır durumda olması gerekir. Bir birincil kullanıcı için erişimi değiştirdiğinizde, değişiklikler hemen OAM tarafından yansıtılır.

Kullanıcılara bir nesne için erişim izni vermek için şunları belirtmeniz gerekir:

- Çalışmakta olduğunuz nesnelerin iyesi olan kuyruk yöneticisinin adı; kuyruk yöneticisinin adını belirtmezseniz, varsayılan kuyruk yöneticisi varsayılır.
- Nesnenin adı ve tipi (nesneyi benzersiz olarak tanımlamak için). Adı bir *tanıtım* olarak belirtiyorsunuz; Bu, nesnenin belirtik adı ya da genel arama karakterleri de içinde olmak üzere genel bir ad. Soysal tanıtımların ayrıntılı açıklamaları ve bunların içinde genel arama karakterlerinin kullanılması için bkz. “UNIX, Linux, and Windows üzerinde OAM genel profillerini kullanma” sayfa 339.
- Yetkinin uygulanacağı bir ya da daha fazla birincil kullanıcı ve grup adı.

  Bir kullanıcı kimliği boşluk içeriyorsa, bu komutu kullandığınızda bunu tırnak işareti içine alın. Windows sistemlerinde, bir etki alanı adıyla bir kullanıcı kimliği niteleyebilirsiniz. Gerçek kullanıcı kimliği bir at işareti (@) simgesi içeriyorsa, kullanıcı kimliği ile etki alanı adı arasındaki sınırlayıcıya değil, kullanıcı kimliğinin bir parçası olduğunu göstermek için bu simgeyi @ @ ile değiştirin.
- Yetkilerin listesi. Listedeki her öğe, o nesneye verilecek erişim tipini belirtir (ya da bu nesneye geri çevrilir). Listedeki her yetki bir anahtar sözcük olarak, önekli olarak artı işareti (+) ya da eksi işareti (-) olarak belirtilir. Belirtilen yetkiyi eklemek için artı işareti ve yetkiyi kaldırmak için eksi işareti kullanın. + ya da-işareti ile anahtar sözcük arasında boşluk olmaması gerekir.

  Tek bir komutta istediğiniz sayıda yetki belirleyebilirsiniz. Örneğin, bir kullanıcının ya da grubun bir kuyruğa ileti yerleştirmesine ve bunlara göz atmalarına izin vermek için gereken yetkilerin listesi, ancak ileti almak için erişimi iptal etmek için aşağıdaki yetkiler şunlardır:

```
+browse -get +put
```

setmqaut komutunu kullanma örnekleri

Aşağıdaki örneklerde, bir nesneyi kullanmak için izin vermek ve iptal etmek için setmqaut komutunun nasıl kullanılacağı gösterilmektedir:

```
setmqaut -m saturn.queue.manager -t queue -n RED.LOCAL.QUEUE
         -g groupa +browse -get +put
```

Bu örnekte:

- saturn.queue.manager , kuyruk yöneticisi adıdır.
- queue , nesne tipidir
- RED.LOCAL.QUEUE , nesne adıdır
- groupa , değişiklik için yetkilendirilmekte olan grubun tanıtıcısıdır
- +browse -get +put , belirtilen kuyruğa ilişkin yetki listesidir

- `+browse` , kuyruktaki iletilere göz atma yetkisi ekler (göz atma seçeneği ile **MQGET** komutunu vermek için)
- `-get` , kuyruktan (**MQGET**) ileti almak için yetkilendirmeyi kaldırır
- `+put` , kuyruğa ekleme (**MQPUT**) iletilerini kuyruğa ekleme yetkisi ekler

Aşağıdaki komut, birincil kullanıcı fvkullanıcısından ve groupa ve groupb gruplarından MyQueue kuyruğunda bulunan yetkiyi iptal eder. UNIX and Linux sistemlerinde bu komut, fvuser ile aynı birincil gruptaki tüm birincil kullanıcılar için de bu komutu iptal eder.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser
         -g groupa -g groupb -put
```

`setmqaut` komutunu farklı bir yetkilendirme hizmetiyle kullanma

OAM yerine kendi yetkilendirme hizmetinizi kullanıyorsanız, komutu bu hizmete yönlendirmek için **setmqaut** komutundaki bu hizmetin adını belirtebilirsiniz. Aynı anda birden çok kurulabilir bileşeniniz varsa, bu değiştirgeyi belirtmeniz gerekir; bunu yapmazsanız, güncelleme, yetkilendirme hizmeti için ilk kurulabilir bileşene yapılır. Varsayılan değer olarak, sağlanan OAM budur.

SET AUTHREC için kullanım notları

Eklenecek yetkiler listesi ve kaldırılacak yetkiler listesi örtüşmemelidir. Örneğin, görüntüleme yetkisi ekleyemez ve görüntüleme yetkisini aynı komutla kaldıramazsınız. Bu kural, yetkiler farklı seçenekler kullanılarak ifade edilse bile geçerlidir. Örneğin, DSP yetkisi ALLADM yetkisiyle çakıştığından aşağıdaki komut başarısız olur:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALLADM)
```

Bu örtüşme davranışının kural dışı durumu ALL yetkisidir. Aşağıdaki komut önce TÜM yetkileri ekler, daha sonra SETID yetkisini kaldırır:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(ALL) AUTHRMV(SETID)
```

Aşağıdaki komut önce TÜM yetkileri kaldırır, daha sonra DSP yetkisini ekler:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALL)
```

Komut sırasına bakılmaksızın, önce ALL işlenir.

ULW UNIX, Linux, and Windows üzerinde OAM genel profillerini kullanma

Tek bir işlemde, bir kullanıcının birçok nesne için ayrıcalıklarını ayarlamak için OAM soysal tanıtımlarını kullanın; yaratıldığında her bir nesne için ayrı **setmqaut** komutları ya da **SET AUTHREC** komutları yayınlamak yerine. IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabildiğinizi unutmayın.

setmqaut ya da SET AUTHREC komutlarındaki soysal tanıtımları kullanarak, o tanıtıma uyan tüm nesneler için soysal bir yetki belirlemenizi sağlar.

Bu konu derlemi, soysal tanıtımların daha ayrıntılı olarak kullanılmasını açıklar.

OAM profillerinde genel arama karakterlerini kullanma

Bir tanıtımı soysal yapan şey, tanıtım adında özel karakterlerin (genel arama karakterleri) kullanılmasıdır. Örneğin, soru işareti (?) genel arama karakteri, bir addaki herhangi bir tek karakterle eşleşir. Bu nedenle,

ABC.?EFdeğerini belirlerseniz, o tanıtıma ilişkin yetki ABC.DEF, ABC.CEF, ABC.BEFgibi adlara sahip nesneler için de geçerlidir.

Kullanılabilecek genel arama karakterleri şunlardır:

?

Herhangi bir tek karakter yerine soru işaretini (?) kullanın. Örneğin, AB.?D , AB.CD, AB.EDve AB.FDnesneleri için geçerlidir.

*****

Yıldız işaretini (*) aşağıdaki gibi kullanın:

- Bir profil adında, nesne adındaki herhangi bir niteleyiciyle eşleşecek *niteleyici* . Niteleyici, bir nokta ile sınırlanmış bir nesne adının parçasıdır. Örneğin, ABC.DEF.GHIiçinde niteleyiciler ABC, DEFve GHI' dir.

  Örneğin, ABC.*.JKL , ABC.DEF.JKLve ABC.GHI.JKLnesneleri için geçerlidir. (ABC.JKL için geçerli **olmadığını** unutmayın; * bu bağlamda kullanılan her zaman bir niteleyiciyi gösterir.)
- Bir profil adındaki niteleyici içindeki, bir nesne adındaki niteleyici içindeki sıfır ya da daha fazla karakterle eşleşecek karakter.

  Örneğin, ABC.DE*.JKL , ABC.DE.JKL, ABC.DEF.JKLve ABC.DEGH.JKLnesneleri için geçerlidir.

******

Profil adında çift yıldız işaretini (**) **bir kez** kullanın:

- Tüm nesne adlarıyla eşleşecek tüm profil adı. Örneğin, süreçleri tanımlamak için `-t prcs` , tanıtım adı olarak ** kullanırsanız, tüm süreçlere ilişkin yetkileri değiştirirsiniz.
- Bir tanıtım adında, nesne adında sıfır ya da daha fazla niteleyiciyle eşleşecek başlangıç, ikinci ya da bitiş niteleyicisi olarak. Örneğin, **.ABC son niteleyicisi ABC olan tüm nesneleri tanıtır.

Çift yıldız işaretini ** yalnızca tam niteleyici olarak kullanabilirsiniz:

```
**.DEF
  ABC.**
  A*.**
```

ancak bu şekilde değil

```
A**
```

Aksi takdirde AMQ7226E: `Profil adı geçersiz.`

Not: UNIX ve Linux sistemlerinde genel arama karakterlerini kullanırken, profil adını tek tırnak işareti içine almanız **gerekir** .

Profil öncelikleri

Soysal tanıtımlar kullanılırken anlaşılması gereken önemli bir nokta, yaratılmakta olan bir nesneye uygulanacak yetkiler belirlenirken tanıtımların verildiği önceliktir. Örneğin, şu komutları yayınladığınızı varsayalım:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

İlki, adları AB. * tanıtımıyla eşleşen birincil kullanıcı Fred için tüm kuyruklara koyma yetkisi verir; İkincisi, AB.C*.

Şimdi AB.CD. Joker karakter eşleştirmeye ilişkin kurallara göre, her iki setmqaut bu kuyruğa uygulanabilir. Yani, otoriteye sahip mi?

Yanıtı bulmak için, bir nesneye birden çok profil uygulanabildiğinde **yalnızca en özel profilin geçerli olduğu**kuralını uygulayabilirsiniz. Bu kuralı uygulama şekliniz, profil adlarını soldan sağa karşılaştırmaktır. Farklı oldukları her yerde, soysal olmayan bir karakter soysal bir karakterden daha belirlidir. Bu örnekte, kuyruk AB.CD ' nin **get** yetkisi (AB.C*, AB. * ' den daha özeldir).

Soysal karakterleri karşılaştırırken *özgüllük* sırası şöyledir:

1. ?
2. *
3. **

Profil ayarlarının dökümü yapılıyor

dmpmqaut denetim komutunun tam tanımlaması ve sözdizimi için bkz. dmpmqaut.

DISPLAY AUTHREC MQSC komutunun tam tanımlaması ve sözdizimi için DISPLAY AUTHRECbaşlıklı konuya bakın.

MQCMD_INQUIRE_AUTH_RECS PCF komutunun tam tanımı ve sözdizimi için Inquire Authority Recordsbaşlıklı konuya bakın.

Aşağıdaki örneklerde, soysal tanıtımlara ilişkin yetki kayıtlarının dökümünü almak için **dmpmqaut** denetim komutunun kullanımı gösterilmektedir:

1. Bu örnek, birincil kullanıcı user1için a.b.c kuyruğuyla eşleşen bir tanıtımla tüm yetki kayıtlarının dökümünü sağlar.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Ortaya çıkan çöplük şöyle bir şeye benziyor:

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

   Not: UNIX ve Linux üzerindeki kullanıcılar **dmpmqaut** komutu için `-p` seçeneğini kullanabilseler de, yetkileri tanımlarken `-g groupname` kullanmaları gerekir.
2. Bu örnek, a.b.ckuyruğuyla eşleşen bir tanıtımla tüm yetki kayıtlarının dökümünü sağlar.

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

   Ortaya çıkan çöplük şöyle bir şeye benziyor:

   ```
   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. Bu örnek, a.b. * profili için tüm yetki kayıtlarının dökümünü sağlar. kuyruk tipinde.

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

   Ortaya çıkan çöplük şöyle bir şeye benziyor:

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

4. Bu örnek, qmXkuyruk yöneticisine ilişkin tüm yetki kayıtlarının dökümünü oluşturur.

```
dmpmqaut -m qmX
```

Ortaya çıkan çöplük şöyle bir şeye benziyor:

```
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. Bu örnek, qmXkuyruk yöneticisi için tüm profil adlarının ve nesne tiplerinin dökümünü alır.

```
dmpmqaut -m qmX -l
```

Ortaya çıkan çöplük şöyle bir şeye benziyor:

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

Not: Yalnızca IBM MQ for Windows için, görüntülenen tüm birincil kullanıcılar etki alanı bilgilerini içerir; örneğin:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ULW *Using wildcard characters in OAM profiles on UNIX, Linux, and Windows*

Bir nesnenin birden çok nesne için geçerli olmasını sağlamak için, nesne yetkisi yöneticisi (OAM) tanıtım adında genel arama karakterlerini kullanın.

Bir profil soysal, profil adında özel karakterlerin (genel arama karakterleri) kullanılmasıdır. Örneğin, soru imi (?) genel arama karakteri, bir addaki tek bir karakterle eşleşir. Bu nedenle, `ABC.?EF`belirtirseniz, bu tanıtıma verdiğiniz yetki, `ABC.DEF`, `ABC.CEF`, `ABC.BEF`ve benzeri nesneler için geçerli olan nesneler için geçerlidir.

Kullanılabilir genel arama karakterleri şunlardır:

?

Herhangi bir tek karakter yerine soru işaretini (?) kullanın. For example, `AB.?D` applies to the objects `AB.CD`, `AB.ED`, and `AB.FD`.

*****

Yıldız işaretini (*) aşağıdaki gibi kullanın:

- Profil adındaki bir *niteleyici* , bir nesne adındaki herhangi bir niteleyiciye eşleştirmek için. Niteleyici, bir nokta ile sınırlanmış bir nesne adının parçasıdır. For example, in `ABC.DEF.GHI`, the qualifiers are `ABC`, `DEF`, and `GHI`.

  For example, `ABC.*.JKL` applies to the objects `ABC.DEF.JKL`, and `ABC.GHI.JKL`. (**değil** ' in `ABC.JKL` için geçerli olduğunu unutmayın; * bu bağlamda kullanılan her zaman tek bir niteleyici belirtir.)

- Bir nesne adındaki niteleyici içinde sıfır ya da daha fazla karakterle eşleşen bir niteleyici içindeki bir niteleyici.

  For example, `ABC.DE*.JKL` applies to the objects `ABC.DE.JKL`, `ABC.DEF.JKL`, and `ABC.DEGH.JKL`.

******

Use the double asterisk (**) **bir kez** in a profile name as:

- Tüm nesne adlarını eşleştirmek için tüm profil adı. Örneğin, süreçleri tanımlamak için `-t prcs` kullanıyorsanız, profil adı olarak ** kullanırsanız, tüm süreçlere ilişkin yetkileri değiştirebilirsiniz.
- Bir profil adındaki başlangıç, orta ya da bitiş niteleyicisini, bir nesne adındaki sıfır ya da daha çok niteleyiciyle eşleşecek şekilde eşleştirin. Örneğin, `**.ABC` , ABC final niteleyicisine sahip tüm nesneleri tanıtır.

Not: UNIX and Linux sistemlerinde genel arama karakterlerini kullanırken, profil adını tek tırnak içine almalısınız **gerekir** .

ULW *UNIX, Linux, and Windowsüzerindeki profil öncelikleri*

Tek bir nesne için birden çok genel tanıtım uygulanabilir. Bu durumda, en özel kural geçerli olur.

Soysal profilleri kullanırken anlamanın önemli bir noktası, oluşturulmakta olan bir nesneye hangi yetkilerin uygulanana karar verilirken profillerin verilme önceliğidir. Örneğin, komutları yayınladığınızı varsayalım:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

İlk olarak, AB. * ile eşleşen adlara sahip asıl fred 'e ilişkin tüm kuyruklara yetki verilir. the second gives get authority to the same types of queue that match the profile AB.C*.

Şimdi AB.CD. Genel arama karakteri eşleştirmesine ilişkin kurallara göre, setmqaut o kuyruğa başvur. Yani, otoriteyi ortaya koyması mı, yoksa yetki mi?

Yanıtı bulmak için, bir nesneye birden çok profil uygulandığında, **yalnızca en özel geçerli**olan kuralı uygulayabilirsiniz. Bu kuralı uyguladığınız yol, profil adlarını soldan sağa ile karşılaştırarak uygulanır. Farklı olan her yerde, soysal olmayan bir karakter daha özeldir ve genel bir karakter olur. So, in this example, the queue AB.CD has **alma** authority (AB.C* is more specific than AB.*).

Soysal karakterleri karşılaştırırken, *belirtimlilik* sırası şöyledir:

1. ?
2. *
3. **

Bu MQSC komutunu kullanırken eşdeğer bilgi için SET AUTHREC başlıklı konuya bakın.

ULW *Dumping profile settings on UNIX, Linux, and Windows*

Belirtilen bir tanıtımla ilişkili yetkilerin dökümünü almak için **dmpmqaut** denetim komutunu, **DISPLAY AUTHREC** MQSC komutunu ya da **MQCMD_INQUIRE_AUTH_RECS** PCF komutunu kullanın. IBM MQ Appliance ' da yalnızca **DISPLAY AUTHREC** komutunu kullanabildiğinizi unutmayın.

dmpmqaut denetim komutunun ve sözdiziminin tam tanımı için bkz. dmpmqaut.

DISPLAY AUTHREC MQSC komutunun tam tanımı ve sözdizimine ilişkin bilgi için DISPLAY AUTHRECbaşlıklı konuya bakın.

MQCMD_INQUIRE_AUTH_RECS PCF komutunun ve sözdiziminin tam tanımı için Authoring Authority Recordsbaşlıklı konuya bakın.

Aşağıdaki örneklerde, soysal tanıtımlara ilişkin yetki kayıtlarının dökümünü almak için **dmpmqaut** denetim komutunun kullanımı gösterilmektedir:

1. Bu örnek, tüm yetki kayıtlarını, birincil kullanıcı user1için a.b.c kuyrukla eşleşen bir tanıtımla dökümünü alır.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Sonuçta ortaya çıkan döküm, aşağıdaki örneğe benzer bir şekilde görünür:

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

   Not: UNIX and Linux kullanıcıları `-p` seçeneğini kullanamaz; bunun yerine `-g groupname` seçeneğini kullanmaları gerekir.

2. Bu örnek, tüm yetki kayıtlarını a.b.ckuyruğuyla eşleşen bir profille döküyor.

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

   Sonuçta ortaya çıkan döküm, aşağıdaki örneğe benzer bir şekilde görünür:

   ```
   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. Bu örnek, a.btanıtılmasına ilişkin tüm yetki kayıtlarını dökümünü alır. *, (kuyruk).

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

   Sonuçta ortaya çıkan döküm, aşağıdaki örneğe benzer bir şekilde görünür:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   ```

```
type:        principal
authority:   get, browse, put, inq
```

4. This example dumps all authority records for queue manager qmX.

```
dmpmqaut -m qmX
```

   Sonuçta ortaya çıkan döküm, aşağıdaki örneğe benzer bir şekilde görünür:

```
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. This example dumps all profile names and object types for queue manager qmX.

```
dmpmqaut -m qmX -l
```

   Sonuçta ortaya çıkan döküm, aşağıdaki örneğe benzer bir şekilde görünür:

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

Not: Yalnızca IBM MQ for Windows için, tüm birincil kullanıcılar etki alanı bilgilerini içerir; örneğin:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ULW UNIX, Linux, and Windowsüzerindeki erişim ayarlarının görüntülenmesi

Belirli bir birincil kullanıcının ya da grubun belirli bir nesne için sahip olduğu yetkileri görüntülemek için **dspmqaut** denetim komutunu, **DISPLAY AUTHREC** MQSC komutunu ya da **MQCMD_INQUIRE_ENTITY_AUTH** PCF komutunu kullanın. IBM MQ Appliance ' da yalnızca **DISPLAY AUTHREC** komutunu kullanabildiğinizi unutmayın.

Bu komutu kullanmak için kuyruk yöneticisinin çalışır durumda olması gerekir. Bir birincil kullanıcıya ilişkin erişimi değiştirdiğinizde, değişiklikler hemen OAM tarafından yansıtılır. Yetki, aynı anda yalnızca bir grup ya da birincil kullanıcı için görüntülenebilir.

dmpmqaut denetim komutunun ve sözdiziminin tam tanımı için bkz. dmpmqaut.

DISPLAY AUTHREC MQSC komutunun tam tanımı ve sözdizimine ilişkin bilgi için DISPLAY AUTHRECbaşlıklı konuya bakın.

MQCMD_INQUIRE_AUTH_RECS PCF komutunun ve sözdiziminin tam tanımı için Authoring Authority Recordsbaşlıklı konuya bakın.

The following example shows the use of the **dspmqaut** control command to display the authorizations that the group GpAdmin has to a process definition named Annuities that is on queue manager QueueMan1.

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

ULW UNIX, Linux, and Windowsüzerindeki bir IBM MQ nesnesine erişimin değiştirilmesi ve geri alınması

Bir kullanıcının ya da grubun bir nesneye ilişkin erişim düzeyini değiştirmek için, **setmqaut** denetim komutunu, **DELETE AUTHREC** MQSC komutunu ya da **MQCMD_DELETE_AUTH_REC** PCF komutunu kullanın. MQ Appliance IBM MQ Appliance ' da yalnızca **DELETE AUTHREC** komutunu kullanabildiğinizi not edin.

Kullanıcıyı bir gruptan kaldırma işlemi şu şekilde açıklanmaktadır:

- Windows “Creating and managing groups on Windows” sayfa 138
- AIX “Creating and managing groups on AIX” sayfa 136
- Solaris “Creating and managing groups on Solaris” sayfa 137
- Linux “Creating and managing groups on Linux” sayfa 136

.

Bir IBM MQ nesnesi yaratan kullanıcı kimliği, o nesneye tam denetim yetkilerine sahip olur. Bu kullanıcı kimliğini yerel mqm grubundan (ya da Windows sistemlerinde Administrators (Yöneticiler) grubundan) kaldırırsanız, bu yetkiler iptal edilmez. Use the **setmqaut** control command or the **MQCMD_DELETE_AUTH_REC** PCF command to revoke access to an object for the user ID that created it, after removing it from the mqm or Administrators group.

Setmqaut denetim komutuna ve sözdizimine ilişkin tam tanım için bkz. setmqaut.

DELETE AUTHREC MQSC komutunun ve sözdiziminin tam tanımı için DELETE AUTHRECbaşlıklı konuya bakın.

MQCMD_DELETE_AUTH_REC PCF komutunun tam tanımı ve sözdizimiyle ilgili olarak bkz. Yetki Kaydını Sil.

Windows On Windows, from IBM MQ 8.0, you can delete the OAM entries corresponding to a particular Windows user account at any time using the **-u** *SID* parameter of **setmqaut**.

IBM MQ 8.0öncesinde, kullanıcı profilini silmeden önce belirli bir Windows kullanıcı hesabına karşılık gelen OAM girdilerini silmeniz gerekir. Kullanıcı hesabı kaldırıldıktan sonra OAM girişlerinin kaldırılması olanaksızdı.

ULW UNIX, Linux, and Windows sistemlerinde güvenlik erişimi denetimlerinin önlenmesi

Tüm güvenlik denetimlerini kapatmak için nesne yetki yöneticisini (OAM) geçersiz kılabilirsiniz. Bu, bir test ortamı için uygun olabilir. OAM ' yi devre dışı bırakmış ya da kaldırmış olsanız da, var olan bir kuyruk yöneticisine OAM ekleyemezsiniz.

Güvenlik denetimlerini gerçekleştirmek istemediğinize karar verirseniz (örneğin, bir test ortamında), OAM ' yi iki yoldan biriyle devre dışı bırakabilirsiniz:

- Bir kuyruk yöneticisi yaratmadan önce, işletim sistemi ortam değişkenini MQSNOAUT olarak ayarlayın.

  MQSNOAUT değişkeninin ayarlanmasının sonuçları ve MQSNOAUT değişkeninin Windows ve UNIXüzerinde nasıl ayarlandığıyla ilgili bilgi için Ortam değişkenleri açıklamaları başlıklı konuya bakın.
- Kuyruk yöneticisi yapılanış dosyasını düzenleyerek hizmeti kaldırın.

OAM devre dışı bırakıldığında **setmqaut**ya da **dspmqaut** komutunu kullanırsanız, aşağıdaki noktalara dikkat edin:

- OAM, belirtilen birincil kullanıcının ya da grubun geçerliliğini denetlemez; bu, komutun geçersiz değerleri kabul edebileceği anlamına gelir.
- OAM, güvenlik denetimleri gerçekleştirmez ve tüm birincil kullanıcı ve grupların tüm geçerli nesne işlemlerini gerçekleştirme yetkisine sahip olduğunu gösterir.

Uyarı: Bir OAM kaldırıldığında, var olan bir kuyruk yöneticisine geri konamaz. Bunun nedeni, OAM ' nin nesne oluşturma zamanında masından etmesi belirtir ısonra. IBM MQ OAM kaldırıldıktan sonra yeniden kullanmak için kuyruk yöneticisini yeniden oluşturun.

İlgili kavramlar

UNIX, Linux ve Windows için kurulabilir hizmetler ve bileşenler

İlgili görevler

Kurulabilir hizmetlerin yapılandırılması

İlgili başvurular

Kurulabilir hizmetler için başvuru bilgileri

Kaynaklara gerekli erişim verilmesi

Use this topic to determine what tasks to perform to apply security to your IBM MQ system on UNIX, Linux, Windows, IBM iVe z/OS.

Bu görev hakkında

Bu görev sırasında, IBM MQ kurulumunuzun öğelerine uygun güvenlik düzeyini uygulamak için hangi işlemlerin gerekli olduğuna karar verirsiniz. Başvurmakta olduğunuz her bir görev, tüm platformlar için adım adım yönergeler verir.

Yordam

1. Kuyruk yöneticinizin erişimini belirli kullanıcılar için sınırlandırmak mı gerekiyor?
   a) Hayır: Başka bir işlem yapma.
   b) Evet: Bir sonraki soruya geçin.
2. Bu kullanıcıların, kuyruk yöneticisi kaynakları alt kümesinde kısmi denetim erişimine sahip olması gerekiyor mu?
   a) Hayır: Bir sonraki soruya geçin.
   b) Evet: Bkz. “Kuyruk yöneticisi kaynakları alt kümesi için kısmi denetim erişimi verilmesi” sayfa 348.
3. Bu kullanıcıların, kuyruk yöneticisi kaynakları alt kümesinde tam yönetici erişimine sahip olması gerekir mi?
   a) Hayır: Bir sonraki soruya geçin.
   b) Evet: Bkz. “Kuyruk yöneticisi kaynaklarının bir alt kümesi üzerinde tam denetim erişimi verilmesi” sayfa 357.
4. Bu kullanıcıların, tüm kuyruk yöneticisi kaynaklarına salt okuma erişimi olması gerekiyor mu?
   a) Hayır: Bir sonraki soruya geçin.
   b) Evet: Bkz. “Bir kuyruk yöneticindeki tüm kaynaklar için salt okunur erişim verilmesi” sayfa 364.
5. Bu kullanıcıların tüm kuyruk yöneticisi kaynaklarında tam yönetici erişimine sahip olması gerekiyor mu?

a) Hayır: Bir sonraki soruya geçin.

b) Evet: Bkz. “Bir kuyruk yöneticisindeki tüm kaynaklara tam denetimci erişimi verilmesi” sayfa 365.

6. Kuyruk yöneticinize bağlanmak için kullanıcı uygulamalarınız gerekiyor mu?

a) No: Disable connectivity, as described in “Kuyruk yöneticisine bağlanılırlığı kaldırma” sayfa 367

b) Evet: Bkz. “Kullanıcı uygulamalarının kuyruk yöneticinize bağlanmasına izin verme” sayfa 367.

z/OS Multi Kuyruk yöneticisi kaynakları alt kümesi için kısmi denetim erişimi verilmesi

Bazı kullanıcılara, kuyruk yöneticisi kaynaklarının bazıları değil, bazıları için kısmi yönetimle ilgili erişim yetkisi vermeniz gerekir. Alması gereken işlemleri belirlemek için bu tabloyu kullanın.

Çizelge 69. Kuyruk yöneticisi kaynaklarına ilişkin bir altkümeye kısmi denetim erişimi verilmesi

Kullanıcıların bu tipteki nesneleri denetlemeleri gerekir	**Bu işlemi gerçekleştir**
Kuyruklar	Grant partial administrative access to the required queues, as described in “Bazı kuyruklara sınırlı yönetim erişimi verilmesi” sayfa 348
Konular	Grant partial administrative access to the required topics, as described in “Bazı konulara sınırlı yönetim erişimi verilmesi” sayfa 350
Kanallar	Grant partial administrative access to the required channels, as described in “Bazı kanallara sınırlı yönetim erişimi verilmesi” sayfa 351
Kuyruk yöneticisi	Kuyruk yöneticisine kısmi denetim erişimi ver (“Kuyruk yöneticisine sınırlı yönetim erişimi verilmesi” sayfa 352içinde açıklandığı gibi)
Süreçler	Grant partial administrative access to the required processes, as described in “Bazı süreçlere sınırlı yönetim erişimi verilmesi” sayfa 353
Ad listeleri	Grant partial administrative access to the required namelists, as described in “Bazı ad listelerine sınırlı yönetim erişimi verilmesi” sayfa 355
Hizmetler	Grant partial administrative access to the required services, as described in “Bazı hizmetler için sınırlı yönetim erişimi verilmesi” sayfa 356

Bazı kuyruklara sınırlı yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı kuyruklara kısmi denetim erişimi verin.

Bu görev hakkında

Bazı işlemler için bazı kuyruklara sınırlı yönetim erişimi vermek üzere işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX

- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

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

- IBM i
  IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS z/OSiçin, belirtilen bir kuyruğa erişim izni vermek için aşağıdaki komutları verin:

```
RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Kullanıcının kuyruğunda hangi MQSC komutlarının gerçekleştirebileceğini belirtmek için, her MQSC komutu için aşağıdaki komutları verin:

```
RDEFINE MQCMDS QMgrName. ReqdAction. QType UACC(NONE)
PERMIT QMgrName. ReqdAction. QType CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

  Kullanıcının DISPLAY QUEUE komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

```
RDEFINE MQCMDS QMgrName.DISPLAY. QType UACC(NONE)
PERMIT QMgrName.DISPLAY. QType CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

  ReqdAction
  Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

  – ULW UNIX, Linux, and Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + dlt, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

  – IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.

  – z/OS On z/OS, one of the values ALTER, CLEAR, DELETE, or MOVE.

  Not: Kuyruklar için + crt verilmesi, kullanıcıyı dolaylı olarak yapar ya da bir yönetici grubunu gruplamadır. Bazı kuyruklara sınırlı yönetim erişimi vermek için + crt yetkinizin kullanılmaması gerekir.

QType

DISPLAY KOMUTU için, QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE ya da QCluster değerlerinden biri.

Diğer *ReqdAction*değerleri için, QLOCAL, QALIAS, QMODEL ya da QREMOTE değerlerinden birini kullanın.

Bazı konulara sınırlı yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı konulara kısmi yönetici erişimi verin.

Bu görev hakkında

Bazı eylemlere ilişkin bazı konulara sınırlı yönetim erişimi vermek için işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW

  UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

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

- IBM i

  IBM iiçin şu komutu verin:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS z/OSiçin aşağıdaki komutları verin:

  ```
  RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
  PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Bu komutlar, belirtilen konuya erişim sağlar. Kullanıcının konu üzerinde hangi MQSC komutlarının gerçekleştirebileceğini belirlemek için, her MQSC komutu için aşağıdaki komutları verin:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.TOPIC UACC(NONE)
  PERMIT QMgrName. ReqdAction.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Kullanıcının DISPLAY TOPIC komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.TOPIC UACC(NONE)
  PERMIT QMgrName.DISPLAY.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

ReqdAction
Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

- ULW UNIX, Linux, and Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. + ctrl. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.
- IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.
- z/OS On z/OS, one of the values ALTER, CLEAR, DEFINE, DELETE, or MOVE.

Bazı kanallara sınırlı yönetim erişimi verilmesi
İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı kanallara kısmi yönetici erişimi verin.

Bu görev hakkında
Bazı işlemler için bazı kanallara sınırlı yönetim erişimi vermek üzere işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam
- ULW
  UNIX, Linux, and Windows'ta:

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

- IBM i
  IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS z/OS'ta:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Bu komutlar, belirtilen kanala erişim sağlar. Kullanıcının kanal üzerinde hangi MQSC komutlarının gerçekleştirebileceğini belirlemek için, her MQSC komutu için aşağıdaki komutları verin:

```
RDEFINE MQCMDS QMgrName. ReqdAction.CHANNEL UACC(NONE)
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Kullanıcının DISPLAY CHANNEL komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

```
RDEFINE MQCMDS QMgrName.DISPLAY.CHANNEL UACC(NONE)
PERMIT QMgrName.DISPLAY.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

ReqdAction
Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

- ULW UNIX, Linux, and Windows' ta, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.
- IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLx. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.
- z/OS On z/OS, one of the values ALTER, CLEAR, DEFINE, DELETE, or MOVE.

Kuyruk yöneticisine sınırlı yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, bir kuyruk yöneticisine kısmi yönetici erişimi verin.

Bu görev hakkında

Kuyruk yöneticiyle ilgili bazı işlemleri gerçekleştirmek üzere sınırlı yönetim erişimi vermek için işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW

UNIX, Linux, and Windows'ta:

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

- IBM i

IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS

z/OS'ta:

Kuyruk yöneticinde gerçekleştirebileceğiniz MQSC komutlarını saptamak için, her MQSC komutu için aşağıdaki komutları çalıştırın:

```
RDEFINE MQCMDS QMgrName. ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName. ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Kullanıcının DISPLAY QMGR komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

```
RDEFINE MQCMDS QMgrName.DISPLAY.QMGR UACC(NONE)
PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

ReqdAction
Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

– ULW UNIX, Linux, and Windows' ta, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

+ kümesi bir MQI yetkisi olmasına rağmen, normalde yönetici olarak kabul edilmemekle birlikte, kuyruk yöneticisine + ayarının verilmesi dolaylı olarak tam yönetim yetkisine yol açabilir. Olağan kullanıcılara ve uygulamalara + ayarlanmaz.

– IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.

Bazı süreçlere sınırlı yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı süreçlere kısmi yönetici erişimi verin.

Bu görev hakkında

Bazı işlemler için bazı süreçlere sınırlı yönetim erişimi vermek üzere işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux

- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

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

- IBM i
  IBM i'ta:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS z/OS'ta:

  ```
  RDEFINE MQADMIN QMgrName.PROCESS. ObjectProfile UACC(NONE)
  PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Bu komutlar, belirtilen kanala erişim sağlar. Kullanıcının kanal üzerinde hangi MQSC komutlarının gerçekleştirebileceğini belirlemek için, her MQSC komutu için aşağıdaki komutları verin:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.PROCESS UACC(NONE)
  PERMIT QMgrName. ReqdAction.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Kullanıcının DISPLAY PROCESS komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.PROCESS UACC(NONE)
  PERMIT QMgrName.DISPLAY.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

  ReqdAction
  Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

  - ULW UNIX, Linux, and Windows' ta, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.
  - IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.
  - z/OS On z/OS, one of the values ALTER, CLEAR, DEFINE, DELETE, or MOVE.

Bazı ad listelerine sınırlı yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı ad listelerine kısmi yönetici erişimi verin.

Bu görev hakkında

Bazı eylemlere ilişkin bazı ad listelerine sınırlı yönetim erişimi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW

  UNIX, Linux, and Windows'ta:

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

- IBM i

  IBM i'ta:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS z/OS'ta:

  ```
  RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
  PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Bu komutlar, belirlenen ad listesine erişim sağlar. Kullanıcının ad listesinde hangi MQSC komutlarının gerçekleştirebileceğini belirlemek için, her MQSC komutu için aşağıdaki komutları verin:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.NAMELIST UACC(NONE)
  PERMIT QMgrName. ReqdAction.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Kullanıcının DISPLAY NAMELIST komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.NAMELIST UACC(NONE)
  PERMIT QMgrName.DISPLAY.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

ReqdAction
Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

- ULW UNIX, Linux, and Windows' ta, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.
- IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.
- z/OS On z/OS, one of the values ALTER, CLEAR, DEFINE, DELETE, or MOVE.

Bazı hizmetler için sınırlı yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı hizmetlere kısmi yönetici erişimi verin.

Bu görev hakkında

Bazı işlemler için bazı hizmetlere sınırlı yönetim erişimi vermek üzere işletim sisteminiz için uygun komutları kullanın. z/OS Hizmet nesnelerinin z/OSüzerinde bulunmadığına dikkat edin.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

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

- IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS z/OS'ta:

  Bu komutlar, belirtilen hizmete erişim sağlar. Kullanıcının hizmette hangi MQSC komutlarının gerçekleştirebileceğini belirlemek için, her MQSC komutu için aşağıdaki komutları verin:

```
RDEFINE MQCMDS QMgrName. ReqdAction.SERVICE UACC(NONE)
PERMIT QMgrName. ReqdAction.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

  Kullanıcının DISPLAY SERVICE komutunu kullanmasına izin vermek için aşağıdaki komutları yürütün:

```
RDEFINE MQCMDS QMgrName.DISPLAY.SERVICE UACC(NONE)
PERMIT QMgrName.DISPLAY.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

ReqdAction
Grubun aşağıdakileri üstlenmesine izin verdiğiniz eylem:

- ULW UNIX, Linux, and Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.
- IBM i IBM i' ta, aşağıdaki yetkilerin herhangi bir birleşimi: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. *ALLADM yetkisi, tüm bu bireysel yetkilerin eşdeğeridir.

Kuyruk yöneticisi kaynaklarının bir alt kümesi üzerinde tam denetim erişimi verilmesi

Bazı kullanıcılara, kuyruk yöneticisi kaynaklarının bazıları değil, bazıları için tam yönetici erişimi vermeniz gerekir. Alması gereken işlemleri belirlemek için bu tabloları kullanın.

Çizelge 70. Kuyruk yöneticisi kaynaklarına ilişkin bir altkümeye tam denetimci erişimi verilmesi

Kullanıcıların bu tipteki nesneleri denetlemeleri gerekir	**Bu işlemi gerçekleştir**
Kuyruklar	Grant full administrative access to the required queues, as described in “Bazı kuyruklara tam denetimci erişimi verilmesi” sayfa 358
Konular	Grant full administrative access to the required topics, as described in “Bazı konulara tam yönetici erişimi verilmesi” sayfa 358
Kanallar	Grant full administrative access to the required channels, as described in “Bazı kanallara tam yönetim erişimi verilmesi” sayfa 359
Kuyruk yöneticisi	Grant full administrative access to the queue manager, as described in “Kuyruk yöneticisine tam denetimci erişimi verilmesi” sayfa 360
Süreçler	Grant full administrative access to the required processes, as described in “Bazı süreçlere tam yönetim erişimi verilmesi” sayfa 361
Ad listeleri	Grant full administrative access to the required namelists, as described in “Bazı ad listelerine tam denetimci erişimi verilmesi” sayfa 362
Hizmetler	“Bazı hizmetlere tam yönetim erişimi verilmesi” sayfa 363' ta açıklandığı şekilde, gerekli hizmetlere tam yönetici erişim yetkisi verin.

Bazı kuyruklara tam denetimci erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı kuyruklara tam yönetici erişimi verin.

Bu görev hakkında

Bazı kuyruklara tam denetimci erişimi vermek için, işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW

  UNIX, Linux, and Windows'ta:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
  ```

- IBM i

  IBM i'ta:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName
  ')
  ```

- z/OS

  z/OS'ta:

  ```
  RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
  PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

Bazı konulara tam yönetici erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı konulara tam yönetici erişimi verin.

Bu görev hakkında

Bazı eylemlere ilişkin bazı konulara tam yönetici erişimi vermek için işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
  ```

- IBM i
  IBM i'ta:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM) MQMNAME('
  QMgrName ')
  ```

- z/OS
  z/OS'ta:

  ```
  RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
  PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

Bazı kanallara tam yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı kanallara tam yönetici erişimi verin.

Bu görev hakkında

Bazı kanallara tam yönetici erişimi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- IBM i
  IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  z/OS'ta:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

Kuyruk yöneticisine tam denetimci erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, bir kuyruk yöneticisine tam yönetici erişimi verin.

Bu görev hakkında

Kuyruk yöneticisine tam yönetici erişimi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- IBM i
  IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  z/OS'ta:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bazı süreçlere tam yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı süreçlere tam yönetici erişim yetkisi verin.

Bu görev hakkında

Bazı süreçlere tam yönetici erişimi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

- IBM i
  IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  z/OS'ta:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bazı ad listelerine tam denetimci erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı ad listelerine tam yönetici erişimi verin.

Bu görev hakkında

Bazı ad listelerine tam yönetici erişimi vermek için, işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- IBM i
  IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  z/OS'ta:

```
RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bazı hizmetlere tam yönetim erişimi verilmesi

İş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bazı hizmetlere tam yönetici erişim yetkisi verin.

Bu görev hakkında

Bazı hizmetlere tam yönetici erişimi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- IBM i
  IBM i'ta:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  z/OS'ta:

```
RDEFINE MQADMIN QMgrName.SERVICE. ObjectProfile UACC(NONE)
PERMIT QMgrName.SERVICE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

z/OSz/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bir kuyruk yöneticindeki tüm kaynaklar için salt okunur erişim verilmesi

Bir iş gereksinimi olan her kullanıcıya ya da kullanıcı grubuna, kuyruk yöneticisiyle ilgili tüm kaynaklara salt okunur erişim izni verin.

Bu görev hakkında

Rol Tabanlı Yetkiler Ekle sihirbazını ya da işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM iIBM i
- LinuxLinux
- UNIXUNIX
- IBM iWindows

Not: MQ ApplianceIBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Herhangi bir yetki ayrıntısını değiştirdikten sonra, REFRESH SECURITY komutunu kullanarak güvenlik yenilemesi gerçekleştirin.

Yordam

- Sihirbazın kullanılması:
  a) IBM MQ Explorer Navigator bölmesinde, kuyruk yöneticisini sağ tıklatın ve **Nesne Yetkilileri** > **Rol Tabanlı Yetkiler Ekle**öğelerini seçin.
  Rol Tabanlı Yetkiler Ekle sihirbazı açılır.
- WindowsUNIX
  UNIX ve Windows sistemleri için aşağıdaki komutları verin:

```
setmqaut -m QMgrName -n ** -t queue -g GroupName +browse +dsp
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get
+put
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp +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
```

  SYSTEM.ADMIN.COMMAND.QUEUE VE SYSTEM.MQEXPLORER.REPLY.MODEL (MODEL) yalnızca, IBM MQ Explorerkullanmak istiyorsanız gereklidir.
- IBM i
  IBM iiçin aşağıdaki komutları verin:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*Q) USER('GroupName') AUT(*ADMDSP *BROWSE) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*TOPIC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
```

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CHL) USER('GroupName') AUT(*ADMDSP *INQ) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CLTCN) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*AUTHINFO) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*LSR) USER('GroupName') AUT(*ADMDSP)MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*NMLIST) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*SVC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ('object-name') OBJTYPE(*MQM) USER('GroupName') AUT(*ADMDSP *CONNECT *INQ)
MQMNAME('QMgrName')
```

- z/OS
  z/OSiçin aşağıdaki komutları verin:

```
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)
```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

Bir kuyruk yöneticisindeki tüm kaynaklara tam denetimci erişimi verilmesi

Bir iş gereksinimi olan her bir kullanıcı ya da kullanıcı grubuna, kuyruk yöneticisiyle ilgili tüm kaynaklara tam yönetici erişim yetkisi verin.

Bu görev hakkında

Rol Tabanlı Yetkiler Ekle sihirbazını ya da işletim sisteminiz için uygun komutları kullanabilirsiniz.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Notlar: ULW

1. If you are using **runmqsc** to administer the queue manager instead of the IBM MQ Explorer, you must grant authority to inquire, get, and browse the SYSTEM.MQSC.REPLY.QUEUE, and you do not need to grant any authorities on the SYSTEM.MQEXPLORER.REPLY.MODEL queue.

2. Bir kuyruk yöneticindeki tüm kaynaklara kullanıcı erişimi verildiğinde, kullanıcının `qm.ini` dosyasına okuma erişimi yoksa, kullanıcının çalıştıramadığı bazı komutlar vardır. Bunun nedeni, `mqm` dışındaki kullanıcıların `qm.ini` dosyasını okuyabilmekte olduğu kısıtlamalardan kaynaklanır.

   Kullanıcı, qm.ini dosyasına okuma erişimi vermezseniz, aşağıdaki komutları yayınlayamaz:

   - TLS ' yi kullanmak üzere yapılandırılmış bir kanal tanımlama
   - `qm.ini`içinde tanımlanan otomatik yapılandırma ekleme değişkenlerini kullanarak bir kanal tanımlama

Yordam

- Sihirbazı kullanıyorsanız, IBM MQ Explorer Navigator bölmesinde kuyruk yöneticisini sağ tıklatın ve **Nesne Yetkilileri** > **Rol Tabanlı Yetkiler Ekle**öğelerini seçin.

  Rol Tabanlı Yetkiler Ekle sihirbazı açılır.

- Linux UNIX

  UNIX and Linux sistemleri için aşağıdaki komutları verin:

```
setmqaut -m QMgrName -n '**' -t queue -g GroupName +alladm +browse
setmqaut -m QMgrName -n @class -t queue -g GroupName +crt
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get +put
setmqaut -m QMgrName -n '**' -t topic -g GroupName +alladm
setmqaut -m QMgrName -n @class -t topic -g GroupName +crt
setmqaut -m QMgrName -n '**' -t channel -g GroupName +alladm
setmqaut -m QMgrName -n @class -t channel -g GroupName +crt
setmqaut -m QMgrName -n '**' -t clntconn -g GroupName +alladm
setmqaut -m QMgrName -n @class -t clntconn -g GroupName +crt
setmqaut -m QMgrName -n '**' -t authinfo -g GroupName +alladm
setmqaut -m QMgrName -n @class -t authinfo -g GroupName +crt
setmqaut -m QMgrName -n '**' -t listener -g GroupName +alladm
setmqaut -m QMgrName -n @class -t listener -g GroupName +crt
setmqaut -m QMgrName -n '**' -t namelist -g GroupName +alladm
setmqaut -m QMgrName -n @class -t namelist -g GroupName +crt
setmqaut -m QMgrName -n '**' -t process -g GroupName +alladm
setmqaut -m QMgrName -n @class -t process -g GroupName +crt
setmqaut -m QMgrName -n '**' -t service -g GroupName +alladm
setmqaut -m QMgrName -n @class -t service -g GroupName +crt
setmqaut -m QMgrName -t qmgr -g GroupName +alladm +connect
```

  `@class`ile ilgili daha fazla bilgi için bkz. **setmqaut**

- Windows

  Windows sistemleri için, UNIX and Linux sistemleri için aynı komutları verin, ancakprofileyerine @CLASS profil adını kullanın.

- IBM i

  IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- z/OS

  z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

Kuyruk yöneticisine bağlanılırlığı kaldırma

Kullanıcı uygulamalarının kuyruk yöneticinize bağlanmasını istemiyorsanız, bu uygulamaların bağlantı kurma yetkisini kaldırın.

Bu görev hakkında

İşletim sisteminiz için uygun komutu kullanarak, tüm kullanıcıların kuyruk yöneticisine bağlanmasını istediğiniz yetkiyi geri alın.

UNIX, Linux, Windows sistemleri ve IBM isistemlerinde, DELETE AUTHREC komutunu da kullanabilirsiniz.

Not: IBM MQ Appliance ' da yalnızca **DELETE AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW

  UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

  ```
  setmqaut -m QMgrName -t qmgr -g GroupName -connect
  ```

- IBM i

  IBM iiçin şu komutu verin:

  ```
  RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
  ```

- z/OS

  z/OSiçin aşağıdaki komutları verin:

  ```
  RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
  RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
  RDEFINE MQCONN QMgrName.CICS UACC(NONE)
  RDEFINE MQCONN QMgrName.IMS UACC(NONE)
  ```

  Herhangi bir PERMIT komutu yayınlamayın.

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı.

  z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  GroupName
  Erişimi reddedilecek grubun adı.

Kullanıcı uygulamalarının kuyruk yöneticinize bağlanmasına izin verme

Kullanıcı uygulamasının kuyruk yöneticinize bağlanmasına izin vermek istiyorsunuz. Hangi işlemlerin yapılması gerektiğini belirlemek için bu konudaki tabloları kullanın.

Önce, istemci uygulamalarının kuyruk yöneticinize bağlanıp bağlanmayacağını saptayın.

If none of the applications that will connect to your queue manager are client applications, disable remote access as described in “Kuyruk yöneticisine uzaktan erişimi devre dışı bırakma” sayfa 375.

If one or more of the applications that will connect to your queue manager are client applications, secure remote connectivity as described in “Kuyruk yöneticisine uzaktan bağlanılırlığın sağlanması” sayfa 368.

Her iki durumda da, bağlantı güvenliğini “Bağlantı güvenliğinin ayarlanması” sayfa 375içinde açıklandığı gibi ayarlayın.

Kuyruk yöneticisine bağlanan her kullanıcı için kaynaklara erişimi denetlemek istiyorsanız, aşağıdaki çizelgeye bakın. İlk kolondaki deyim true (doğru) ise, ikinci kolonda listelenen işlemi gerçekleştirin.

Bildirim	Bu işlemi gerçekleştirin
Kuyruktan kullanım yapan uygulamalariniz var	Bkz. “Kuyruklara kullanıcı erişiminin denetlenmesi” sayfa 376
Konu kullanımını oluşturan uygulamalariniz var	Bkz. “Konulara kullanıcı erişimini denetleme” sayfa 382.
Kuyruk yöneticisi nesnesini sorgulayan uygulamalariniz var	Bkz. “Kuyruk Yöneticisi üzerinde sorgulama için yetki verilmesi” sayfa 384.
Süreç nesnelerini kullanan uygulamalariniz var	Bkz. “Süreçlere erişim yetkisi verilmesi” sayfa 385
Ad listelerini kullanan uygulamalariniz var	Bkz. “Ad listelerine erişim yetkisi verilmesi” sayfa 385

Kuyruk yöneticisine uzaktan bağlanılırlığın sağlanması

TLS, bir güvenlik çıkışı, kanal doğrulama kayıtları ya da bu yöntemlerin bir bileşimini kullanarak kuyruk yöneticisine uzaktan bağlanılırlık güvenliğini sağlayabilirsiniz.

Bu görev hakkında

İstemci iş istasyonunda bir istemci-bağlantı kanalı ve sunucuda bir sunucu bağlantısı kanalı kullanarak, bir istemciyi kuyruk yöneticisine bağlırsınız. Bu tür bağlantıları aşağıdaki yollardan biriyle sabitleyin.

Yordam

1. Kanal kimlik doğrulama kayıtlarıyla TLS ' nin kullanılması:
   a) Tüm DN ' leri USERSRC (NOACCESS) ile eşlemek için bir SSLPEERMAP kanal kimlik doğrulaması kaydı kullanarak, ayırt edici adın (DN) bir kanalı açmasını engelleyin.
   b) Belirli DN 'lerin ya da DN' lerin bir kanalı açmak için bir SSLPEERMAP kanalı kimlik doğrulaması kaydını kullanarak bunları USERSRC (KANAL) ile eşleyin.
2. Güvenlik çıkışıyla TLS ' nin kullanılması:
   a) MCAUSER, ayrıcalıksız bir kullanıcı tanıtıcıyla sunucu bağlantısı kanalına ayarlanır.
   b) MQCD yapısındaki çıkışa aktarılan SSLPeerNamePtr ve SSLPeerNameLength alanlarında aldığı TLS DN değerine bağlı olarak bir MCAUSER değeri atamak için bir güvenlik çıkışı yazın.
3. Sabit kanal tanımlama değerleri ile TLS ' nin kullanılması:
   a) Sunucu bağlantısı kanalında SSLPEER ' i belirli bir değer ya da dar değer aralığıyla ayarlayın.
   b) MCAUSER sunucu bağlantı kanalını, kanalın çalıştırılacağı kullanıcı kimliği için ayarlayın.
4. TLS kullanmayan kanallarda kanal doğrulama kayıtlarının kullanılması:
   a) ADDRESS (*) ve USERSRC (NOACCESS) içeren bir adres eşleme kanalı kimlik doğrulama kaydı kullanarak, kanal açma kanallarından herhangi bir IP adresini engelleyin.
   b) USERSRC (KANAL) ile ilgili adresler için adres eşleme kanalı kimlik doğrulama kayıtlarını kullanarak, belirli IP adreslerine açık kanallara izin verin.
5. Güvenlik çıkışı kullanılması:
   a) Seçtiğiniz herhangi bir özelliğe dayalı olarak bağlantılara yetki vermek için bir güvenlik çıkışı yazın; örneğin, kaynak IP adresi.
6. ayrıca, kanal kimlik doğrulama kayıtlarını bir güvenlik çıkığı ile kullanmak ya da belirli şartlarınız gerektiriyorsa, tüm üç yöntemi kullanmak da mümkündür.

Belirli IP adreslerinin engellenmesi
Bir IP adresinden gelen bağlantıyı kabul eden belirli bir kanalı önleyebilir ya da bir kanal kimlik doğrulaması kaydı kullanarak, tüm kuyruk yöneticisinin bir IP adresinden erişime izin vermelerini önleyebilirsiniz.

Başlamadan önce

Aşağıdaki komutu çalıştırarak kanal doğrulama kayıtlarını etkinleştirin:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Bu görev hakkında

Belirli kanalların gelen bağlantıyı kabul etmelerine izin vermek ve bağlantıların yalnızca doğru kanal adı kullanılırken kabul edildiğinden emin olmak için IP adreslerini engellemek için tek bir kural tipi kullanılabilir. Bir IP adresi erişimine tüm kuyruk yöneticisine izin vermemek için, olağan durumda bu güvenlik duvarını kalıcı olarak engellemek için bir güvenlik duvarı kullanırdınız. Ancak, birkaç adresi geçici olarak engellemenize olanak sağlamak için başka bir kural tipi de kullanılabilir; örneğin, güvenlik duvarının güncellenmesini bekliyorsanız.

Yordam

- To block IP addresses from using a specific channel, set a channel authentication record by using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**.

```
SET CHLAUTH(generic-channel-name) TYPE(ADDRESSMAP) ADDRESS(generic-ip-address)
USERSRC(NOACCESS)
```

Komutta üç parça vardır:

SET CHLAUTH (*soysal-kanal-adı*)
Tüm kuyruk yöneticisi, tek kanal ya da kanal aralığı için bir bağlantıyı engellemek isteyip istemediğinizi denetlemek için bu komutun bu bölümünü kullanıyorsunuz. Buraya koydugunuz alanlar hangi alanlarinin kapsanabildii belirler

Örneğin:

- SET CHLAUTH('*') -kuyruk yöneticisindeki her kanalı, yani tüm kuyruk yöneticisini engeller.
- SET CHLAUTH ('SYSTEM. *')-SYSTEM ile başlayan her kanalı bloke eder.
- SET CHLAUTH ('SYSTEM.DEF.SVRCONN')-kanal SYSTEM.DEF.SVRCONN

CHLAUTH kuralı tipi
Komutun tipini belirlemek için bu komutun bu bölümünü kullanın ve tek bir adres mi, yoksa adres listesi mi sağlamak istediğinizi belirler.

Örneğin:

- TYPE(ADDRESSMAP) -Tek bir adres ya da genel arama adresi sağlamak istiyorsanız, ADDRESSMAP kullanın. Örneğin, ADDRESS('192.168.*'),192.168' ta başlayan bir IP adresinden gelen bağlantıları engeller.

  IP adreslerini kalıplarla süzmek hakkında daha fazla bilgi için bkz. Generic IP address.
- TYPE(BLOCKADDR) -Blok için bir adres listesi sağlamak istiyorsanız BLOCKADR değerini kullanın.

Ek parametreler
Bu parametreler, komutun ikinci kısmında kullandığınız kural tipine bağlıdır:

- TYPE(ADDRESSMAP) için ADDRESS kullanıyorsunuz
- TYPE(BLOCKADDR) için ADDRIST kullanıyorsunuz

İlgili başvurular
CHLAUTH KüMESI

Kuyruk yöneticisi çalışmıyorsa, belirli IP adreslerini geçici olarak engelle
Kuyruk yöneticisi çalışmadığında ve bu nedenle MQSC komutlarını veremezseniz, belirli IP adreslerini ya da adres aralıklarını bloke etmek isteyebilirsiniz. You can temporarily block IP addresses on an exceptional basis by modifying the `blockaddr.ini` file.

Bu görev hakkında

`blockaddr.ini` dosyası, kuyruk yöneticisi tarafından kullanılan BLOCKADDR tanımlamalarının bir kopyasını içerir. Dinleyici, kuyruk yöneticilikinden önce başlatıldıysa, bu dosya dinleyici tarafından okunur. Bu koşullarda dinleyici, `blockaddr.ini` dosyasına el ile eklediğiniz değerleri kullanır.

Ancak, kuyruk yöneticisi başlatıldığında, BLOCKADDR tanımlamalarının kümesini `blockaddr.ini` dosyasına yazar, el ile düzenlemeyi her türlü el ile düzenleme işlemi yapmış olabilirsiniz. Benzer şekilde, **SET CHLAUTH** komutunu kullanarak bir BLOCKADR tanımlaması eklediğinizde ya da silerseniz, `blockaddr.ini` dosyası güncellenir. You can therefore make permanent changes to the BLOCKADDR definitions only by using the **SET CHLAUTH** command when the queue manager is running.

Yordam

1. `blockaddr.ini` dosyasını bir metin düzenleyicide açın.
   Dosya, kuyruk yöneticisinin veri dizininde bulunur.
2. IP adreslerini basit anahtar sözcük çiftleri olarak ekleyin; burada anahtar sözcük `Addr`olur.
   IP adreslerini kalıplarla süzmek hakkında bilgi için bkz. Genel IP adresleri.
   Örneğin:

```
Addr = 192.0.2.0
Addr = 192.0.*
Addr = 192.0.2.1-8
```

İlgili görevler
"Belirli IP adreslerinin engellenmesi" sayfa 369
Bir IP adresinden gelen bağlantıyı kabul eden belirli bir kanalı önleyebilir ya da bir kanal kimlik doğrulaması kaydı kullanarak, tüm kuyruk yöneticisinin bir IP adresinden erişime izin vermelerini önleyebilirsiniz.

İlgili başvurular
CHLAUTH KüMESI

Belirli kullanıcı kimliklerini engelle
Belirli kullanıcıların bir kanalı kullanmasını önleyebilirsiniz. Bu durumda, kullanıcı kimlikleri belirtilirse, kanal sona ermesine neden olur. Bunu bir kanal kimlik doğrulama kaydı ayarlayarak yapın.

Başlamadan önce

Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Yordam

Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH(' generic-channel-name ') TYPE(BLOCKUSER) USERLIST(userID1, userID2)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.

TYPE(BLOCKUSER) üzerinde sağlanan kullanıcı listesi yalnızca SVRCONN kanallarına uygulanır ve kuyruk yöneticisi için kuyruk yöneticisi kanallarına gönderilmez.

userID1 ve *userID2* , kanalın kullanılmasının önleneceği her kullanıcının tanıtıcısıdır. Ayrıcalıklı yönetici kullanıcılara başvuruda bulunmak için *MQADMIN özel değerini de belirtebilirsiniz. Ayrıcalıklı kullanıcılar hakkında daha fazla bilgi için bkz. “Ayrıcalıklı kullanıcılar” sayfa 318. *MQADMINile ilgili ek bilgi için SET CHLAUTHbaşlıklı konuya bakın.

İlgili başvurular

CHLAUTH KüMESI

Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi

Kanalın bağlanacağı kuyruk yöneticisine göre, bir kanala ilişkin MCAUSER özniteliğini ayarlamak için kanal kimlik denetimi kaydını kullanabilirsiniz.

Başlamadan önce

Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Bu görev hakkında

İsteğe bağlı olarak, kuralın uygulanacağı IP adreslerini sınırlayabilirsiniz.

Bu tekniğin sunucu bağlantısı kanalları için geçerli olmadığını unutmayın. Aşağıdaki komutlarda sunucu bağlantısı kanalının adını belirlerseniz, bu bir etki gösteremez.

Yordam

- Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

  ```
  SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
  ) USERSRC(MAP) MCAUSER(user)
  ```

  soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.

  soysal-ortak-qmgr-adı , kuyruk yöneticisinin adı ya da kuyruk yöneticisi adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesi de içinde olmak üzere bir örüntü.

  user (kullanıcı), belirtilen kuyruk yöneticisinden tüm bağlantılar için kullanılacak kullanıcı kimliğidir.
- Bu komutu belirli IP adresleriyle sınırlamak için, **ADDRESS** parametresini aşağıdaki gibi ekleyin:

  ```
  SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
  ) USERSRC(MAP) MCAUSER(user) ADDRESS(
  generic-ip-address)
  ```

  soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.

  soysal-ip-adresi tek bir adrestir ya da genel arama karakteri olarak yıldız işareti (*) simgesini ya da bir aralığı belirtmek için tire (-) içeren bir kalıp, bu adresle eşleşir. Soysal IP adreslerine ilişkin ek bilgi için Soysal IP adresleribaşlıklı konuya bakın.

İlgili başvurular

CHLAUTH KüMESI

İstemci kullanıcı kimliğinin MCAUSER kullanıcı kimliğiyle eşlenmesi
Bir istemciden alınan kullanıcı kimliğine göre, bir sunucu bağlantısı kanalının MCAUSER özniteliğini değiştirmek için bir kanal kimlik doğrulaması kaydını kullanabilirsiniz.

Başlamadan önce
Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Bu görev hakkında
Bu tekniğin yalnızca sunucu-bağlantı kanalları için geçerli olduğunu unutmayın. Diğer kanal tipleri üzerinde bir etkisi yoktur.

Yordam
Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record** . Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH(' generic-channel-name ') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.
istemci-kullanıcı-adı , istemci bağlantısıyla ilişkili kullanıcı kimliğidir; bu değer istemci uygulaması tarafından değerlendirilebilir, erken evlat edinme ya da kanal çıkışı aracılığıyla ayarlanan bağlantı kimlik doğrulamasıyla değiştirilir.
user (kullanıcı), istemci kullanıcı adı yerine kullanılacak kullanıcı kimliğidir.

İlgili başvurular
CHLAUTH KüMESI
Kanalların öznitelikleri (ChlauthEarlyAdopt)

SSL ya da TLS Ayırt Edici Adının MCAUSER kullanıcı kimliğine eşlenmesi
Bir kanala ilişkin MCAUSER özniteliğini ayarlamak için, alınan Ayırt Edici Ad 'a (DN) göre bir kanal kimlik doğrulaması kaydı kullanabilirsiniz.

Başlamadan önce
Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Yordam
Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH('generic-channel-name') TYPE (SSLPEERMAP)
SSLPEER(generic-ssl-peer-name) SSLCERTI(generic-issuer-name)
USERSRC(MAP) MCAUSER(user)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.
soysal-ssl-eş-adı , SSLPEER değerleri için standart IBM MQ kurallarını izleyen bir dizgidir. Bkz. SSLPEER değerleri içinIBM MQ kuralları.

kullanıcı , belirtilen DN ' yi kullanan tüm bağlantılar için kullanılacak kullanıcı kimliğidir.
soysal-yayıncı-adı , eşleştirilecek sertifikanın Sertifika Veren DN ' ini belirtir. Bu parametre isteğe bağlıdır; ancak, birden çok sertifika yetkilisi kullanımdaysa, yanlış sertifikadan büyük bir şekilde eşleşmemesi için bunu kullanmanız gerekir.

İlgili başvurular
CHLAUTH KüMESI

Uzak kuyruk yöneticisinden erişimin engellenmesi
Uzak kuyruk yöneticisinin kanallardan başlatılmasını önlemek için kanal kimlik denetimi kaydını kullanabilirsiniz.

Başlamadan önce
Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Bu görev hakkında
Bu tekniğin sunucu bağlantısı kanalları için geçerli olmadığını unutmayın. Aşağıdaki komutta bir sunucu bağlantı kanalının adını belirtirseniz, bu bir etki gösteremez.

Yordam
Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH(' generic-channel-name ') TYPE(QMGRMAP) QMNAME(' generic-partner-qmgr-name ')
USERSRC(NOACCESS)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.
soysal-ortak-qmgr-adı , kuyruk yöneticisinin adı ya da kuyruk yöneticisi adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesi de içinde olmak üzere bir örüntü.

İlgili başvurular
CHLAUTH KüMESI

İstemci kullanıcı kimliği için erişimin engellenmesi
Bir istemci kullanıcı kimliğinin bir kanal bağlantısı kurmasını önlemek için kanal kimlik denetimi kaydını kullanabilirsiniz.

Başlamadan önce
Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Bu görev hakkında
Bu tekniğin yalnızca sunucu-bağlantı kanalları için geçerli olduğunu unutmayın. Diğer kanal tipleri üzerinde bir etkisi yoktur.

Yordam
Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH(' generic-channel-name ') TYPE(USERMAP) CLNTUSER(' client-user-name ')
USERSRC(NOACCESS)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.

istemci-kullanıcı-adı , istemci bağlantısıyla ilişkili kullanıcı kimliğidir; bu değer istemci uygulaması tarafından değerlendirilebilir, erken evlat edinme ya da kanal çıkışı aracılığıyla ayarlanan bağlantı kimlik doğrulamasıyla değiştirilir.

İlgili başvurular

CHLAUTH KüMESI

SSL ya da TLS Ayırt Edici Adı için erişimin engellenmesi

Başlangıç kanallarından TLS Ayırt Edici Adı 'nı (DN) önlemek için kanal kimlik doğrulaması kaydını kullanabilirsiniz.

Başlamadan önce

Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Yordam

Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH('generic-channel-name') TYPE(SSLPEERMAP)
SSLPEER('generic-ssl-peer-name') SSLCERTI(generic-issuer-name)
USERSRC(NOACCESS)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.

soysal-ssl-eş-adı , SSLPEER değerleri için standart IBM MQ kurallarını izleyen bir dizgidir. Bkz. SSLPEER değerleri içinIBM MQ kuralları.

soysal-yayıncı-adı , eşleştirilecek sertifikanın Sertifika Veren DN ' ini belirtir. Bu parametre isteğe bağlıdır; ancak, birden çok sertifika yetkilisi kullanımdaysa, yanlış sertifikadan büyük bir şekilde eşleşmemesi için bunu kullanmanız gerekir.

İlgili başvurular

CHLAUTH KüMESI

Bir IP adresinin MCAUSER kullanıcı kimliği ile eşlenmesi

Bir kanala ilişkin MCAUSER özniteliğini, bağlantının alındığı IP adresine göre ayarlamak için kanal kimlik denetimi kaydını kullanabilirsiniz.

Başlamadan önce

Kanal doğrulama kayıtlarının aşağıdaki gibi etkinleştirildiğinden emin olun:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Yordam

Set a channel authentication record using the MQSC command **SET CHLAUTH**, or the PCF command **Set Channel Authentication Record**. Örneğin, MQSC komutunu yayınlayabilirsiniz:

```
SET CHLAUTH(' generic-channel-name ') TYPE(ADDRESSMAP) ADDRESS(' generic-ip-address ')
USERSRC(MAP) MCAUSER(user)
```

soysal-kanal-adı , erişimi denetlemek istediğiniz bir kanalın adı ya da kanal adıyla eşleşen bir genel arama karakteri olarak yıldız (*) simgesini içeren bir örüntü.

kullanıcı , belirtilen DN ' yi kullanan tüm bağlantılar için kullanılacak kullanıcı kimliğidir.

soysal-ip-adresi , bağlantının yapıldığı adres ya da bir genel arama karakteri olarak yıldız işareti (*) ya da bir aralığı belirtmek için tire (-) içeren bir kalıp ya da adresle eşleşen bir kalıdır.

İlgili başvurular

CHLAUTH KüMESI

Kuyruk yöneticisine uzaktan erişimi devre dışı bırakma

İstemci uygulamalarının kuyruk yöneticinize bağlanmasını istemiyorsanız, uzak erişimi bu erişim için devre dışı bırakın.

Bu görev hakkında

Aşağıdaki yollardan biriyle istemci uygulamalarının kuyruk yöneticisine bağlanmasını önleyin:

Yordam

- **DELETE CHANNEL**MQSC komutunu kullanarak tüm sunucu bağlantısı kanallarını silin.
- Set the message channel agent user identifier (MCAUSER) of the channel to a user ID with no access rights, using the MQSC command **ALTER CHANNEL**.

Bağlantı güvenliğinin ayarlanması

Bir iş gereksinimi olan her kullanıcı ya da kullanıcı grubuna kuyruk yöneticisine bağlanma yetkisi verin.

Bu görev hakkında

Bağlantı güvenliğini ayarlamak için, işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW
  UNIX, Linux, and Windows'ta:

  ```
  setmqaut -m QMgrName -t qmgr -g GroupName +connect
  ```

- IBM i
  IBM i'ta:

  ```
  GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM) USER('GroupName') AUT(*CONNECT)
  ```

- z/OS

z/OS'ta:

```
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)
```

Bu komutlar, toplu iş, CICS, IMS ve kanal başlatıcı (CHIN) için bağlantı kurma yetkisi verir. Belirli bir bağlantı tipini kullanmazsanız, ilgili komutları atlayın.

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

İlgili kavramlar

“Kanal başlatıcısı için bağlantı güvenliği profilleri” sayfa 189
Kanal başlatıcısından gelen bağlantıları denetlemek için kullanılan tanıtımlar, kuyruk yöneticisi ya da kuyruk paylaşım grubu adından ve ardından *CHIN*sözcüğünün izlediği bir tanıtımdan oluşur. Kanal başlatıcı tarafından kullanılan kullanıcı kimliğine, bağlantı tanıtımına görev adresi alanı okuma erişimi başlatmasını sağlar.

Kuyruklara kullanıcı erişiminin denetlenmesi

Uygulama erişimini kuyruklara kontrol etmek istiyorsunuz. Hangi işlemlerin yapılması gerektiğini belirlemek için bu konuyu kullanın.

İlk kolondaki her doğru deyim için, ikinci kolonda belirtilen işlemi gerçekleştirin.

Bildirim	**İşlem**
Uygulama kuyruktan ileti alır	Bkz. “Kuyruklardan ileti almak için yetki verilmesi” sayfa 376
Uygulama kümeleri bağlamı	Bkz. “Bağlamı ayarlamak için yetki verilmesi” sayfa 377
Uygulama bağlamı geçiyor	Bkz. “Bağlam geçişi için yetki verilmesi” sayfa 378
Uygulama, iletileri kümelenmiş bir kuyruğa koyar.	Bkz. “Uzak küme kuyruklarına ileti koyma yetkisi” sayfa 441
Uygulama, iletileri yerel bir kuyruğa koyar	Bkz. “İletileri yerel bir kuyruğa koyma yetkisi verilmesi” sayfa 379
Uygulama, iletileri bir model kuyruğuna koyar.	Bkz. “Bir model kuyruğuna ileti koymak için yetki verilmesi” sayfa 380
Uygulama, iletileri uzak bir kuyruğa koyar.	Bkz. “İletileri uzak bir küme kuyruğuna koyma yetkisi verilmesi” sayfa 381

Kuyruklardan ileti almak için yetki verilmesi
Bir kuyruktan ya da kuyruk kümesinden, iş gereksinimi olan her kullanıcı grubuna ileti alma yetkisi verin.

Bu görev hakkında

Bazı kuyruklardan ileti alma yetkisi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bağlamı ayarlamak için yetki verilmesi
Bir iş gereksinimi olan her bir kullanıcı grubuna, konmakta olan bir ileti üzerinde bağlam belirleme yetkisi verin.

Bu görev hakkında

Bazı kuyruklarda bağlam belirleme yetkisi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutlardan birini çalıştırın:
  - Yalnızca kimlik bağlamını ayarlamak için:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
```

- Tüm bağlamı ayarlamak için:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
```

Not: `setid` ya da `setall` yetkisini kullanmak için, yetkilerin hem uygun kuyruk nesnesinde, hem de kuyruk yöneticisi nesnesinde verilmesi gerekir.

- IBM iiçin aşağıdaki komutlardan birini yayınlayın:
  - Yalnızca kimlik bağlamını ayarlamak için:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('
QMgrName ')
```

  - Tüm bağlamı ayarlamak için:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME('
QMgrName ')
```

- z/OSiçin aşağıdaki komut kümelerinden birini yayınlayın:
  - Yalnızca kimlik bağlamını ayarlamak için:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

  - Tüm bağlamı ayarlamak için:

```
RDEFINE MQQUEUE QMgrName. ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bağlam geçişi için yetki verilmesi
Bir iş gereksinimi olan her bir kullanıcı grubuna, alınan bir iletinin bağlamı konulmakta olan bir iletiyi bağlayacak şekilde yetki verir.

Bu görev hakkında

Bazı kuyruklara bağlam geçirme yetkisi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- ULW

  UNIX, Linux, and Windows sistemleri için aşağıdaki komutlardan birini çalıştırın:

  - Yalnızca kimlik bağlamını geçirmek için:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
    ```

  - Tüm bağlamı geçirmek için:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
    ```

- IBM i

  IBM iiçin aşağıdaki komutlardan birini yayınlayın:

  - Yalnızca kimlik bağlamını geçirmek için:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID) MQMNAME('
    QMgrName ')
    ```

  - Tüm bağlamı geçirmek için:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL) MQMNAME('
    QMgrName ')
    ```

- z/OS

  z/OSiçin, kimlik bağlamını geçirmek ya da tüm bağlamı geçirmek için aşağıdaki komutları yazın:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

İletileri yerel bir kuyruğa koyma yetkisi verilmesi
Bir iş gereksinimi olan her kullanıcı grubuna, iletileri yerel bir kuyruğa ya da kuyruk kümesine koyma yetkisi verin.

Bu görev hakkında

Bazı yerel kuyruklara ileti koyma yetkisi vermek için, işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX

- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Bir model kuyruğuna ileti koymak için yetki verilmesi
Bir iş gereksinimi olan her kullanıcı grubuna, iletileri bir model kuyruğuna ya da model kuyrukları kümesine koyma yetkisine sahip olun.

Bu görev hakkında

Dinamik kuyruklar yaratmak için model kuyrukları kullanılır. Bu nedenle, hem model hem de dinamik kuyruklar için yetki vermelisiniz. Bu yetkileri vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutları verin:

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- IBM iiçin aşağıdaki komutları verin:

```
GRTMQMAUT OBJ(' ModelQueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- z/OSiçin aşağıdaki komutları verin:

```
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)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ModelQueueAdı
Dinamik kuyrukların dayalı olduğu model kuyruğunun adı.

ObjectProfile
Yetkilerin değiştirileceği dinamik kuyruk ya da genel tanıtımın adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

İletileri uzak bir küme kuyruğuna koyma yetkisi verilmesi
Bir iş gereksinimi olan her kullanıcı grubuna, iletileri uzak bir küme kuyruğuna ya da kuyruk kümesine koyma yetkisine sahip olun.

Bu görev hakkında

Uzak bir küme kuyruğuna ileti koymak için, bu iletiyi uzak bir kuyruğun yerel tanımlamasına ya da tam olarak nitelenmiş bir uzak kuyruğa yerleştirebilirsiniz. If you are using a local definition of a remote queue, you need authority to put to the local object: see "İletileri yerel bir kuyruğa koyma yetkisi verilmesi" sayfa 379. Tam olarak nitelenmiş bir uzak kuyruk kullanıyorsanız, uzak kuyruğa konmak için gereken yetkiye sahip olduğunuzu belirleyin. Bu yetkiyi, işletim sisteminiz için uygun komutları kullanarak verin.

Varsayılan davranış, SYSTEM.CLUSTER.TRANSMIT.QUEUE' a karşı erişim denetiminin gerçekleştirilmesine neden olur. Birden çok iletim kuyruğu kullansanız da, bu davranışın geçerli olduğunu unutmayın.

The specific behavior described in this topic applies only when you have configured the **ClusterQueueAccessControl** attribute in the qm.ini file to be *RQMAdı*, as described in the Güvenlik stanzası topic, and restarted the queue manager.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

rqmname nesnesini yalnızca uzak küme kuyrukları için kullanabildiğinizi unutmayın.

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

  RMTMQMNAME nesnesini yalnızca uzak küme kuyrukları için kullanabildiğinizi unutmayın.

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQQUEUE)
ID(GroupName) ACCESS(UPDATE)
```

  Uzak kuyruk yöneticisi (ya da kuyruk paylaşım grubu) adını, yalnızca uzak küme kuyrukları için kullanabildiğinizi unutmayın.

  Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

  ObjectProfile
  Yetkilerin değiştirileceği uzak kuyruk yöneticisinin ya da genel tanıtımın adı.

  GroupName
  Verilecek erişim izni verilecek grubun adı.

Konulara kullanıcı erişimini denetleme

Konulara ilişkin uygulamaların erişimini denetlemeniz gerekir. Hangi işlemlerin yapılması gerektiğini belirlemek için bu konuyu kullanın.

İlk kolondaki her doğru deyim için, ikinci kolonda belirtilen işlemi gerçekleştirin.

Çizelge 71. Konulara kullanıcı erişimini denetleme

Bildirim	**İşlem**
Uygulama bir konuya ileti yayınlar	Bkz. “Bir konuya ileti yayınlamak için yetki verilmesi” sayfa 382
Uygulama bir konuya abone olur	Bkz. “Konulara abone olmak için yetki verilmesi” sayfa 383

Bir konuya ileti yayınlamak için yetki verilmesi

Bir konuya ya da konu kümesine ileti yayınlama yetkisi vermek için, iş gereksinimi olan her kullanıcı grubuna ilişkin yetki verin.

Bu görev hakkında

Bazı konulara ileti yayınlama yetkisi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('
QMgrName ')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Konulara abone olmak için yetki verilmesi
Bir konuya ya da konu kümesine abone olma yetkisi vermek için, bir iş gereksinmesi olan her kullanıcı grubuna abone olun.

Bu görev hakkında

Bazı konulara abone olma yetkisi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('
QMgrName ')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Kuyruk Yöneticisi üzerinde sorgulama için yetki verilmesi

Bir iş gereksinimi olan her kullanıcı grubuna, kuyruk yöneticisiyle ilgili bilgi verme yetkisi verin.

Bu görev hakkında

Bir kuyruk yöneticisini sorgulama yetkisi vermek için işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName
')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Bu komutlar, belirtilen kuyruk yöneticisine erişim sağlar. Kullanıcının MQINQ komutunu kullanmasına izin vermek için aşağıdaki komutları girin:

```
RDEFINE MQCMDS QMgrName.MQINQ.QMGR UACC(NONE)
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Süreçlere erişim yetkisi verilmesi
Bir iş gereksinimi olan her kullanıcı grubuna, bir süreç ya da süreç kümesine erişim yetkisi verin.

Bu görev hakkında
Bazı süreçlere erişim yetkisi vermek için işletim sisteminize uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam
- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName
')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

Ad listelerine erişim yetkisi verilmesi
Bir iş gereksinimi olan her kullanıcı grubuna, bir ad listesine ya da ad listesi kümesine erişim yetkisi verin.

Bu görev hakkında
Bazı ad listelerine erişme yetkisi vermek için işletim sisteminiz için uygun komutları kullanın.

Aşağıdaki altyapılarda, SET AUTHREC komutunu da kullanabilirsiniz:

- IBM i IBM i
- Linux Linux
- UNIX UNIX

- IBM i Windows

Not: MQ Appliance IBM MQ Appliance üzerinde yalnızca **SET AUTHREC** komutunu kullanabilirsiniz.

Yordam

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
+all
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

ObjectProfile
Yetkilerin değiştirileceği nesnenin ya da soysal profilin adı.

GroupName
Verilecek erişim izni verilecek grubun adı.

ULW UNIX, Linux, and Windowsüzerinde IBM MQ yönetimi yetkisi

IBM MQ yöneticileri tüm IBM MQ komutlarını kullanabilir ve diğer kullanıcılar için yetki verebilir. Denetimciler uzak kuyruk yöneticilerine komut verdiklerinde, uzak kuyruk yöneticisine gereken yetkiyi edinmeleri gerekir. Further considerations apply to Windows systems.

IBM MQ denetimcileri, tüm IBM MQ komutlarını kullanma yetkisine sahiptir (diğer kullanıcılar için IBM MQ yetkileri vermek üzere komutlar da içinde olmak üzere).

Bir IBM MQ yöneticisi olmak için, **mqm** grubu adı verilen özel bir grubun üyesi olmanız gerekir.

Windows Alternatif olarak, yalnızca Windows üzerinde, yerel hesaplar Windows sistemlerinde Administrators (Yöneticiler) grubunun üyesiyse, IBM MQ ' i yönetebilir.

Uyarı: You can add your Azure AD user to the mqm group by using an administrator command. Örneğin, `net localgroup mqm AzureAD\<your userID> /add`komutunu kullanın. Bundan sonra IBM MQ denetim komutlarını çalıştırın ya da IBM MQ Explorerkomutunu kullanın.

mqm grubu, IBM MQ kurulduğunda otomatik olarak yaratılır. Yönetim gerçekleştirmelerine izin vermek için gruba daha fazla kullanıcı ekleyebilirsiniz. Bu grubun tüm üyelerinin tüm kaynaklara erişimleri vardır. Bu erişim, yalnızca **mqm** grubundan bir kullanıcı kaldırılarak ve **REFRESH SECURITY** komutu verilerek iptal edilebilir.

Yöneticiler, IBM MQ' ı yönetmek için denetim komutlarını kullanabilir. One of these control commands is **setmqaut**, which is used to grant authorities to other users to enable them to access or control IBM MQ resources. Yetki kayıtlarının yönetilmesine ilişkin PCF komutları, kuyruk yöneticisininde dsp ve chg

yetkileri verilen denetimciler tarafından kullanılabilir. PCF komutlarını kullanarak yetkilerin yönetilmesine ilişkin ek bilgi edinmek için Programlanır Komut Biçimlerikonusuna bakın.

Denetimcilerin, uzak kuyruk yöneticisi tarafından işlenecek MQSC komutlarına ilişkin gerekli yetkileri olmalıdır. IBM MQ Explorer , denetim görevlerini gerçekleştirmek için PCF komutları verir. Denetimciler, yerel sistemde kuyruk yöneticisini denetlemek için IBM MQ Explorer ' i kullanmak üzere ek yetkilere gerek duymaz. IBM MQ Explorer , bir kuyruk yöneticisini başka bir sistemde denetlemek için kullanıldığında, denetimcilerin, PCF komutlarının uzak kuyruk yöneticisi tarafından işlenmesine ilişkin gerekli yetkilere sahip olması gerekir.

Uyarı: From IBM MQ 8.0, you do not have to be an administrator to use the control command **runmqsc**, that issues IBM MQ Script (MQSC) commands.

runmqsc uzak kuyruk yöneticisine MQSC komutları göndermek için dolaylı kipte kullanıldığında, her MQSC komutu bir Escape PCF komutu içinde kapsüllenmiş olur.

PCF ve MQSC komutları işlendiğinde yetki denetimlerine ilişkin ek bilgi için aşağıdaki konulara bakın:

- Kuyruk yöneticileri, kuyruklar, işlemler, ad listeleri ve kimlik doğrulama bilgileri nesneleri üzerinde işlem yapan PCF komutları için bkz. IBM MQ nesneleriyle çalışma yetkisi. Escape PCF komutlarında kapsüllenmiş eşdeğer MQSC komutları için bu bölüme bakın.
- Kanallar, kanal başlatıcıları, dinleyiciler ve kümelerde çalışan PCF komutları için bkz. Kanal güvenliği.
- Yetki kayıtlarında çalışan PCF komutları için PCF komutlarına ilişkin yetki denetimibaşlıklı konuya bakın.
- z/OS IBM MQ for z/OSüzerinde komut sunucusu tarafından işlenen MQSC komutları için bkz. z/OS üzerinde komut güvenliği ve komut kaynağı güvenliği..

Ayrıca, Windows sistemlerinde, SYSTEM hesabında IBM MQ kaynaklarına tam erişim olanağı bulunur.

UNIX and Linux altyapılarında, yalnızca ürün tarafından kullanılmak üzere, **mqm** özel kullanıcı kimliği de yaratılır. Bu, ayrıcalıklı olmayan kullanıcılar için hiçbir zaman kullanılabilir olmamalıdır. Tüm IBM MQ nesneleri **mqm**kullanıcı kimliğine aittir.

Windows sistemlerinde, Administrators (Yöneticiler) grubunun üyeleri, SYSTEM hesabı olarak herhangi bir kuyruk yöneticisini da yönetebilir. Etki alanı içinde etkin olan tüm ayrıcalıklı kullanıcı kimliklerini içeren etki alanı denetleyicisi üzerinde bir etki alanı **mqm** grubu da oluşturabilir ve bunu yerel **mqm** grubuna ekleyebilirsiniz. Some commands, for example **crtmqm**, manipulate authorities on IBM MQ objects and so need authority to work with these objects (as described in the following sections). **mqm** grubunun üyeleri tüm nesnelerle çalışma yetkisine sahiptir, ancak aynı adı taşıyan bir yerel kullanıcı ve etki alanı kimliği doğrulanmış bir kullanıcıyla sahipseniz, yetki reddedildiğinde Windows sistemlerinde durumlar olabilir. Bu, “UNIX, Linux, and Windowsüzerindeki birincil kullanıcılar ve gruplar” sayfa 390içinde açıklanmaktadır.

Kullanıcı Hesabı Denetimi (UAC) özelliği olanWindows sürümleri, Administrators (Yöneticiler) grubunun üyeleri olsalar bile, kullanıcıların belirli işletim sistemi tesislerinde gerçekleştirebileceği işlemleri kısıtlar. If your userid is in the Administrators group but not the **mqm** group you must use an elevated command prompt to issue IBM MQ admin commands such as **crtmqm**, otherwise the error `AMQ7077: İstenen işlemi gerçekleştirme yetkiniz yok` is generated. Yükseltilmiş bir komut istemini açmak için, komut isteminin başlangıç menüsü öğesini ya da simgesini sağ tıklatın ve **Run as administrator**(Yönetici olarak çalıştır) seçeneğini belirleyin.

Aşağıdaki işlemleri yapmak için **mqm** grubunun bir üyesi olmanız gerekmez:

- Komut, kanal başlatıcılarını işlemediği sürece, bir Escape PCF komutu içinde PCF komutları ya da MQSC komutları veren bir uygulama programından komut verin. (Bu komutlar “Kanal başlatıcı tanımlarının korunması” sayfa 105 içinde açıklanmıştır).
- Bir uygulama programından MQI çağrıları yayınlayın (`MQCONNX` çağrısında hızlı yol bağ tanımlarını kullanmak istemiyorsanız).
- Veri tipi yapıları üzerinde veri dönüştürme işlemini gerçekleştiren bir kod parçası oluşturmak için `crtmqcvx` komutunu kullanın.
- Kuyruk yöneticilerini görüntülemek için `dspmq` komutunu kullanın.
- IBM MQ ile biçimlendirilmiş izleme çıkışını görüntülemek için `Dspmqtrc` komutunu kullanın.

12 karakter sınırlaması hem grup hem de kullanıcı kimlikleri için geçerlidir.

UNIX and Linux platformları genel olarak bir kullanıcı kimliğinin uzunluğunu 12 karakterle sınırlar. AIX 5.3 bu sınırı yükseltti, ancak IBM MQ , tüm UNIX and Linux platformlarında 12 karakterlik bir kısıtlamayı gözlemlemeye devam eder. 12 karakterden daha büyük bir kullanıcı kimliği kullanıyorsanız, IBM MQ bu kullanıcı kimliğini UNKNOWN değeriyle değiştirir. Do not define a user ID with a value of UNKNOWN .

ULW UNIX, Linux, and Windowsüzerinde mqm grubunun yönetilmesi

Mqm grubundaki kullanıcıların IBM MQüzerinde tam yönetici ayrıcalıkları verilir. Bu nedenle, uygulamaları ve olağan kullanıcıları mqm grubuna kaydetmemeniz gerekir. mqm grubu yalnızca IBM MQ denetimcilerinin hesaplarını içermelidir.

Bu görevler aşağıda açıklanmıştır:

- Windows Creating and managing groups on Windows
- AIX Creating and managing groups on AIX
- Solaris Creating and managing groups on Solaris
- Linux Creating and managing groups on Linux

Windows Etki alanı denetleyiciniz Windows 2000 ya da Windows 2003 ' ta çalışıyorsa, etki alanı yöneticiniz IBM MQ için özel bir hesap ayarlamak zorunda kalabilirler. Daha fazla bilgi için bkz. IBM MQ , Prepare IBM MQ Wizardile yapılandırılıyor ve IBM MQiçin Windows etki alanı hesaplarını oluşturma ve ayarlama.

ULW UNIX, Linux, and Windowsüzerinde IBM MQ nesneleriyle çalışma yetkisi

Tüm nesneler IBM MQile korunuyor ve birincil kullanıcılara bu nesnelere erişmek için uygun yetki verilmelidir. Farklı birincil kullanıcıların farklı nesnelere erişim hakları olması gerekir.

Kuyruk yöneticileri, kuyruklar, süreç tanımlamaları, ad listeleri, kanallar, istemci bağlantı kanalları, dinleyiciler, hizmetler ve kimlik doğrulama bilgileri nesnelerine, MQI çağrıları ya da PCF komutlarını kullanan uygulamalardan erişilir. Bu kaynakların tümü IBM MQile korunuyor ve uygulamalara erişmek için izin verilmesi gerekiyor. İsteği yapan varlık, bir kullanıcı, bir MQI çağrısı yapan bir uygulama programı ya da bir PCF komutu veren bir denetim programı olabilir. İstekte bulunanın tanıtıcısı, *asıl ad*olarak adlandırılır.

Farklı birincil kullanıcı gruplarına aynı nesne için farklı erişim yetkisi tipleri verilebilir. Örneğin, belirli bir kuyruk için, bir grubun hem put, hem de alma işlemlerini gerçekleştirmesine izin verilebilir; başka bir gruba yalnızca kuyruğa göz atma izni verilebilir (göz atma seçeneği bulunan MQGET). Benzer şekilde, bazı gruplar bir kuyruğa yerleştirip yetki alabilir, ancak kuyruğun özniteliklerini değiştirmesine ya da silmesine izin verilmeyebilir.

Bazı işlemler özellikle hassas ve ayrıcalıklı kullanıcılarla sınırlandırılmış olmalıdır. Örneğin:

- İletim kuyrukları ya da komut kuyruğu SYSTEM.ADMIN.COMMAND.QUEUE
- Tüm MQI bağlam seçeneklerini kullanan programlar çalıştırılıyor
- Uygulama kuyruklarının yaratılması ve silinmesi

Bir nesneye tam erişim izni, nesneyi yaratan kullanıcı kimliğine ve mqm grubunun tüm üyelerine (ve Windows sistemlerindeki yerel denetimciler grubunun üyelerine) otomatik olarak verilir.

İlgili kavramlar

“UNIX, Linux, and Windowsüzerinde IBM MQ yönetimi yetkisi” sayfa 386
IBM MQ yöneticileri tüm IBM MQ komutlarını kullanabilir ve diğer kullanıcılar için yetki verebilir. Denetimciler uzak kuyruk yöneticilerine komut verdiklerinde, uzak kuyruk yöneticisine gereken yetkiyi edinmeleri gerekir. Further considerations apply to Windows systems.

ULW UNIX, Linux, and Windowsüzerinde güvenlik denetimleri yapıldığında

Güvenlik denetimleri genellikle bir kuyruk yöneticisine bağlanma, nesneleri açma ya da kapatma ve ileti koyma ya da alma konusunda yapılır.

Tipik bir uygulama için yapılan güvenlik denetimleri aşağıdaki gibidir:

Kuyruk yöneticiyle bağlantı kuruluyor (MQCONN ya da MQCONNX çağrıları)
Bu, uygulamanın belirli bir kuyruk yöneticisiyle ilk kez ilişkilendirilir. Kuyruk yöneticisi, uygulamayla ilişkili kullanıcı kimliğini bulmak için işletim ortamını sorgular. IBM MQ daha sonra, kullanıcı kimliğinin kuyruk yöneticisine bağlanma yetkisi olduğunu doğrular ve ileride yapılacak denetimlere ilişkin kullanıcı kimliğini korur.

Kullanıcıların IBM MQ' ta oturum açması gerekmez; IBM MQ , kullanıcıların temeldeki işletim sisteminde oturum açmış ve bunun için kimlik doğrulaması gerçekleştirmiş olduğu varsayılmıştır.

Nesnenin açılması (MQOPEN ya da MQPUT1 çağrıları)
IBM MQ nesnelerine nesne açılarak ve bu nesnelere ilişkin komut verilmesiyle erişilir. Tüm kaynak denetimleri, nesne açıldığında, gerçekten erişildiği zaman değil, gerçekleştirilir. Bu, **MQOPEN** isteğinin gereken erişim tipini (örneğin, kullanıcının yalnızca nesneye göz atmak ya da bir kuyruğa ileti koymak gibi bir güncelleme işlemi gerçekleştirmesini istemesi gibi) belirtmesi gerektiği anlamına gelir.

IBM MQ , **MQOPEN** isteğinde adı geçen kaynağı denetler. Bir diğer ad ya da uzak kuyruk nesnesi için, kullanılan yetki, diğer adın ya da uzak kuyruğun çözülen kuyruğun kendisi değil, nesnenin kendisidir. Bu, kullanıcının ona erişmek için izin gerekmediği anlamına gelir. Ayrıcalıklı kullanıcılara kuyruk yaratma yetkisi sınırlayın. Bunu yapmazsanız, kullanıcılar bir diğer ad oluşturarak normal erişim denetimini atlayabilirler. Uzak bir kuyruğun hem kuyruk, hem de kuyruk yöneticisi adlarıyla açık bir şekilde adlandırılması durumunda, uzak kuyruk yöneticisiyle ilişkili iletim kuyruğu denetlenir.

Dinamik bir kuyruğa alma yetkisi, türetildiği model kuyruğunun temel alınarak, ancak aynı zamanda aynı şekilde olması gerekmez. This is described in Note “1” sayfa 124.

Erişim denetlerine ilişkin kuyruk yöneticisi tarafından kullanılan kullanıcı kimliği, kuyruk yöneticisine bağlı uygulamanın işletim ortamından elde edilen kullanıcı kimliğidir. Uygun bir şekilde yetkili bir uygulama, alternatif bir kullanıcı kimliği belirterek bir **MQOPEN** çağrısı yayınlayabilir; daha sonra alternatif kullanıcı kimliği üzerinde erişim denetimi denetimleri yapılır. Bu, uygulamayla ilişkili kullanıcı kimliğini değiştirmez, yalnızca erişim denetimi denetimleri için kullanılır.

İletilerin alınması ve alınması (MQPUT ya da MQGET çağrıları)
Erişim denetimi denetimi gerçekleştirilmez.

Nesnenin kapatılması (MQCLOSE)
Bir dinamik kuyrukta **MQCLOSE** sonuçları silinmedikçe, erişim denetimi denetimi gerçekleştirilmez. Bu durumda, kullanıcı kimliğinin kuyruğu silme yetkisi olup olmadığını denetleyin.

Bir konuya abone olma (MQSUB)
Bir uygulama bir konuya abone olduğunda, gerçekleştirmesi gereken işlem tipini belirtir. Yeni bir abonelik yaratır, var olan bir aboneliği değiştirir ya da değiştirmeden var olan bir aboneliğin sürdürülmesini sağlar. Her işlem tipi için, kuyruk yöneticisi, uygulamayla ilişkili kullanıcı kimliğinin, işlemi gerçekleştirme yetkisine sahip olduğunu denetler.

Bir uygulama bir konuya abone olduğunda, yetki denetimleri, uygulamanın abone olduğu konu ağacındaki konu ağacında ya da üstünde bulunan konu nesnelerine göre gerçekleştirilir. Yetki denetimleri birden fazla konu nesnesi üzerinde denetim içerebilir.

Kuyruk yöneticisinin yetki denetimi için kullandığı kullanıcı kimliği, uygulama kuyruk yöneticisine bağlandığında, işletim sisteminden alınan kullanıcı kimliğidir.

Kuyruk yöneticisi, yetki denetimlerini abone kuyruklarında gerçekleştirir, ancak yönetilen kuyruklarda işlem yapar.

ULW Erişim denetimi UNIX, Linux, and Windowstarafından IBM MQ tarafından nasıl uygulanmaktadır?

IBM MQ , nesne yetkili yöneticisi kullanılarak, temeldeki işletim sistemi tarafından sağlanan güvenlik hizmetlerini kullanır. IBM MQ , erişim denetimi listelerini oluşturmak ve korumak için komutlar sağlar.

Yetkilendirme Hizmeti Arabirimi adı verilen bir erişim denetimi arabirimi, IBM MQ' nin bir parçasıdır. IBM MQ supplies an implementation of an access control manager (conforming to the Authorization Service Interface) known as the *nesne yetkisi yöneticisi (OAM)*. Tersi durumda ("UNIX, Linux, and Windows sistemlerinde güvenlik erişimi denetimlerinin önlenmesi" sayfa 346 içinde açıklandığı gibi) belirtilmedikçe, yarattığınız her kuyruk yöneticisi için bu özellik otomatik olarak kurulur ve etkinleştirilir. OAM, Yetkilendirme Hizmeti Arabirimine uygun olan herhangi bir kullanıcı ya da satıcı tarafından yazılmış herhangi bir bileşenle değiştirilebilir.

OAM, işletim sistemi kullanıcı ve grup kimliklerini kullanarak, temel işletim sisteminin güvenlik özelliklerinden yararlanır. Kullanıcılar yalnızca doğru yetkiye sahip oldukları takdirde IBM MQ nesnelerine erişebilirler. "Controlling access to objects by using the OAM on UNIX, Linux, and Windows" sayfa 336 , bu yetkinin nasıl ödeneceğini ve iptal etmeyi açıklar.

OAM, denetleyen her kaynak için bir erişim denetleme listesi (EDL) sağlar. Yetki verileri, SYSTEM.AUTH.DATA.QUEUE. Bu kuyruğa erişim, mqm grubundaki kullanıcılarla ve ek olarak Windows' ta, Yöneticiler grubundaki kullanıcılara ve sistem tanıtıcısı ile oturum açan kullanıcılarla sınırlanmıştır. Kuyruğa kullanıcı erişimi değiştirilemez.

IBM MQ , erişim denetimi listelerini oluşturmak ve korumak için komutlar sağlar. Bu komutlarla ilgili daha fazla bilgi için bkz. "Controlling access to objects by using the OAM on UNIX, Linux, and Windows" sayfa 336.

IBM MQ , OAM ' ı bir birincil kullanıcı, bir kaynak adı ve bir erişim tipi içeren bir istek iletir. OAM, sağladığı EDL ' ye dayalı olarak erişim verir ya da erişimi reddeder. IBM MQ , OAM kararını izler; ÖAM bir karar veremezse, IBM MQ erişime izin vermez.

ULW UNIX, Linux, and Windowsüzerindeki kullanıcı kimliğinin tanımlanması

Nesne yetkilisi yöneticisi, bir kaynağa erişim isteğinde bulunan asıl adı tanıtır. Birincil kullanıcı olarak kullanılan kullanıcı kimliği bağlama göre değişir.

Nesne yetkisi yöneticisi (OAM), belirli bir kaynağa kimlerin erişmeyi istediğini tanımlayabilmelidir. IBM MQ , bu tanıtıcıyı belirtmek için *birincil kullanıcı* terimini kullanır. Birincil kullanıcı, uygulama kuyruk yöneticisine ilk bağlandığında kurulur; bu uygulama, bağlanan uygulamayla ilişkili kullanıcı kimliğinden kuyruk yöneticisi tarafından belirlenir. (Uygulama, kuyruk yöneticisine bağlanmadan XA çağrılarını yayınlarsa, xa_open çağrısını içeren uygulamayla ilişkili kullanıcı kimliği, kuyruk yöneticisi tarafından yetki denetimleri için kullanılır.)

UNIX and Linux sistemlerinde, yetkilendirme yordamları gerçek (logged-in) kullanıcı kimliğini ya da uygulamayla ilişkili etkin kullanıcı kimliğini denetler. Denetlenecek kullanıcı kimliği bağ tanımlama tipine bağlı olabilir; ayrıntılar için Kurulabilir hizmetlerkonusuna bakın.

IBM MQ , sistemden alınan kullanıcı kimliğini, her iletinin ileti üstbilgisindeki (MQMD yapısı) kullanıcının tanımlaması olarak geçirir. Bu tanıtıcı, ileti bağlamı bilgilerinin bir parçasıdır ve "UNIX, Linux, and Windows üzerinde bağlam yetkisi" sayfa 393içinde açıklanmıştır. Uygulamalar, bağlam bilgilerini değiştirme yetkisine sahip olmadıkları sürece bu bilgileri değiştiremez.

ULW *UNIX, Linux, and Windowsüzerindeki birincil kullanıcılar ve gruplar*

Birincil kullanıcılar gruplara ait olabilir. Bireylere değil, gruplara kaynak erişimi vererek, gereken yönetim miktarını azaltabilirsiniz. Erişim Denetimi Listeleri (EDL ' ler) hem grupları hem de kullanıcı kimliklerini temel alır.

Örneğin, belirli bir uygulamayı çalıştırmak isteyen kullanıcılardan oluşan bir grup tanımlayabilirsiniz. Diğer kullanıcılara, gereken kullanıcı kimliğini uygun gruba ekleyerek, gereksinim duydukları tüm kaynaklara erişim verilebilir.

Grupların tanımlanması ve yönetilmesine ilişkin bu işlem belirli platformlar için açıklanmıştır:

- Windows Creating and managing groups on Windows
- AIX Creating and managing groups on AIX
- Solaris Creating and managing groups on Solaris
- Linux Creating and managing groups on Linux

Bir birincil kullanıcı, birden çok gruba (grup kümesi) ait olabilir. Grup, grup grubundaki her gruba verilen bütün yetkilerin toplamını içeriyor. These authorities are cached, so any changes you make to the group membership of the principal are not recognized until the queue manager is restarted, unless you issue the MQSC command **REFRESH SECURITY** (or its PCF equivalent).

Linux UNIX **UNIX and Linux sistemleri**

From IBM MQ 8.0, access control lists (ACLs) are based on both user IDs and groups and you can use either for authorization by setting the **SecurityPolicy** attribute to the appropriate value as described in Kurulabilir hizmetlerin yapılandırılması and UNIX ve Linuxüzerinde yetkilendirme hizmeti dayanaklarının yapılandırılması.

IBM MQ 8.0olanağından, yetkilendirme için *kullanıcı tabanlı modeli* kullanabilir ve bu, hem kullanıcıları hem de grupları kullanabilmenize olanak tanır. Ancak, setmqaut komutunda bir kullanıcı belirttiğinizde, yeni izinler o kullanıcı için geçerli olacak ve kullanıcının ait olduğu hiçbir grup için geçerli değildir. Daha fazla bilgi için bakınız: OAM user-based permissions on UNIX and Linux systems.

Yetkilendirme için *grup-tabanlı model* 'i kullandığınızda, kullanıcı kimliğinin ait olduğu birincil grup EDL' ye dahil edilir. Tek tek kullanıcı kimliği dahil değildir ve bu grubun tüm üyelerine yetki verilir. Bu yüzden, aynı gruptaki başka bir birincil kullanıcının yetkisini değiştirerek, bir birincil kullanıcının yetkisini istemeden değiştirebileceğinin farkında olun.

Tüm kullanıcılar `Kimse` varsayılan kullanıcı grubuna atanmış olarak atanır ve varsayılan olarak, bu gruba yetki verilmez. Belirli yetkileri olmayan kullanıcılara IBM MQ kaynaklarına erişim izni vermek için `Kimse` grubundaki yetkiyi değiştirebilirsiniz.

Do not define a user ID with the value `BILINMIYOR`. Kullanıcı kimliği çok uzun olduğunda, isteğe bağlı kullanıcı kimlikleri `BILINMIYOR`erişim yetkilerini kullanacakken `BILINMIYOR` değeri kullanılır.

Kullanıcı kimlikleri en çok 12 karakter içerebilir ve 12 karaktere kadar grup adı içerebilir.

Windows **Windows sistemleri**

ACL ' ler hem kullanıcı kimlikleri, hem de gruplar temel alınarak kullanılabilir. Denetimler, UNIXile aynı olup olmadığını denetler. Aynı kullanıcı kimliğine sahip farklı etki alanlarında farklı kullanıcılarınız olabilir. IBM MQ , kullanıcı kimliklerinin bir etki alanı adıyla nitelenmesine izin verir; böylece, bu kullanıcılara farklı düzeylerde erişim verilebilir.

Grup adı, isteğe bağlı olarak aşağıdaki biçimlerde belirtilmiş bir etki alanı adı içerebilir:

```
GroupName@domain domain_name\group_name
```

Genel gruplar OAM tarafından yalnızca iki durumda kontrol edilir:

1. Kuyruk yöneticisi güvenlik kısmı şu ayarı içerir: `GroupModel=GlobalGroups`. Bkz. Securing.
2. Kuyruk yöneticisi, alternatif bir güvenlik erişim grubu kullanıyor. Bkz. **crtmqm** .

Kullanıcı kimlikleri en çok 20 karakter içerebilir, etki alanı en çok 15 karakter, grup adları ise en çok 64 karakter içerebilir.

OAM önce yerel güvenlik veritabanını, daha sonra birincil etki alanının veritabanını ve son olarak da güvenilir etki alanlarının veritabanını denetler. Saptanan ilk kullanıcı kimliği OAM tarafından denetlenmek üzere kullanılır. Bu kullanıcı kimliklerinin her biri, belirli bir bilgisayarda farklı grup üyeliklerine sahip olabilir.

Bazı denetim komutları (örneğin, **crtmqm**), nesne yetkisi yöneticisini (OAM) kullanarak IBM MQ nesnelerine ilişkin yetkileri değiştirir. OAM, belirli bir kullanıcı kimliğine ilişkin yetki haklarını belirlemek için yukarıdaki paragrafta belirtilen sırayla güvenlik veri tabanlarını arar. Sonuç olarak, OAM tarafından belirlenen yetki, bir kullanıcı kimliğinin yerel mqm grubunun bir üyesi olması nedeniyle geçersiz kılınabilir. Örneğin,localkomutunu, yerel bir grup aracılığıyla yerel mqm grubunun üyeliği içeren bir etki alanı denetleyicisi tarafından doğrulanan bir kullanıcı kimliğinden **crtmqm** komutunu verdiyseniz, sistemde yerel mqm grubunda olmayan aynı adı taşıyan bir yerel kullanıcı varsa komut başarısız olur.

Windowsüzerinde **SecurityPolicy** özniteliğini ayarlama hakkında daha fazla bilgi için bkz. Kurulabilir hizmetler ve Windows üzerinde yetkilendirme hizmeti dayanaklarının yapılandırılması.

Windows *Windows güvenlik tanıtıcıları (SID ' ler)*

Windows üzerindeIBM MQ , kullanılabilir olduğu SID ' yi kullanır. Bir yetki isteğiyle Windows SID sağlanmıyorsa, IBM MQ kullanıcı adına bağlı olarak kullanıcıyı tanımlar; ancak bu, yanlış yetkinin verilmesiyle sonuçlanabilir.

Windows sistemlerinde, kullanıcı kimliğini tamamlamak için güvenlik tanıtıcısı (SID) kullanılır. SID, kullanıcının tanımlı olduğu Windows güvenlik hesabı yöneticisi (SAM) veritabanında bulunan tüm kullanıcı hesabı ayrıntılarını tanımlayan bilgileri içerir. IBM MQ for Windowsüzerinde bir ileti oluşturulduğunda, IBM MQ ileti tanımlayıcısında SID ' yi saklar. Windows üzerinde IBM MQ yetki denetimi gerçekleştirdiğinde, SAM veritabanından tam bilgileri sorgulamak için SID ' yi kullanır. (Bu sorgunun başarılı olması için kullanıcının tanımlı olduğu SAM veritabanına erişilir olmalıdır.)

Varsayılan olarak, bir yetki isteğiyle Windows SID sağlanmıyorsa, IBM MQ kullanıcı adına bağlı olarak kullanıcıyı tanımlar. Bunu, güvenlik veritabanlarında aşağıdaki sırayla arama yaparak gerçekleştirir:

1. Yerel güvenlik veritabanı
2. Birincil etki alanının güvenlik veritabanı
3. Güvenilen etki alanlarına ilişkin güvenlik veritabanı

Kullanıcı adı benzersiz değilse, yanlış IBM MQ yetkisi verilmiş olabilir. Bu sorunu önlemek için, her yetki isteğine bir SID ekleyin; SID, kullanıcı kimlik bilgilerini oluşturmak için IBM MQ tarafından kullanılır.

Tüm yetki isteklerinin bir SID içermesi gerektiğini belirtmek için **regedit**değerini kullanın. SecurityPolicy ' yi NTSIDsRequiredolarak ayarlayın.

ULW UNIX, Linux, and Windowsüzerinde diğer kullanıcı yetkisi

Bir kullanıcı kimliğinin, bir IBM MQ nesnesine erişirken başka bir kullanıcının yetkisini kullanabileceğini belirtebilirsiniz. Buna *diğer-kullanıcı yetkisi*adı verilir ve bunu herhangi bir IBM MQ nesnesinde de kullanabilirsiniz.

Diğer-kullanıcı yetkisi, bir sunucunun bir programdan gelen istekleri aldığı ve programın istek için gerekli yetkiye sahip olduğundan emin olmak istediği durumlarda gereklidir. Sunucu gerekli yetkiye sahip olabilir, ancak programın istediği işlemler için yetkiye sahip olup olmadığını bilmesi gerekir.

For example, assume that a server program running under user ID PAYSERV retrieves a request message from a queue that was put on the queue by user ID USER1. Sunucu programı istek iletisini aldığında, isteği işler ve yanıtı, istek iletisiyle belirtilen yanıtlama kuyruğuna yerleştirir. Yanıt kuyruğu açılmasına yetki vermek için kendi kullanıcı kimliğini (PAYSERV) kullanmak yerine, sunucu farklı bir kullanıcı kimliği belirtebilir (bu durumda USER1). Bu örnekte, yanıt kuyruğu açıldığında, PAYSERV ' in diğer kullanıcı kimliği olarak USER1 belirtmesine izin verilip verilmeyeceğini denetlemek için diğer kullanıcı yetkisini kullanabilirsiniz.

Alternatif-kullanıcı kimliği, nesne tanımlayıcısının **AlternateUserId** alanında belirtilir.

ULW UNIX, Linux, and Windows üzerinde bağlam yetkisi

Bağlam, belirli bir ileti için geçerli olan ve iletinin bir parçası olan ileti tanımlayıcısı MQMD ' de bulunan bilgilerdir. Uygulamalar, MQOPEN ya da MQPUT çağrısı yapıldığında bağlam verilerini belirtebilir.

Bağlam bilgileri iki kısımdan oluşur:

Kimlik bölümü
Mesajın geldiği kişi. UserIdentifier, AccountingTokenve ApplIdentityData alanlarından oluşur.

Kaynak bölümü
Mesajın nereden geldiği ve ne zaman kuyruğa konduğu. PutApplType, PutApplName, PutDate, PutTimeve ApplOriginData alanlarından oluşur.

Uygulamalar, MQOPEN ya da MQPUT çağrısı yapıldığında bağlam verilerini belirtebilir. Bu veriler uygulama tarafından oluşturulabilir, başka bir iletiden iletilebilir ya da varsayılan olarak kuyruk yöneticisi tarafından oluşturulabilir. Örneğin, bağlam verileri sunucu programları tarafından istekte bulunanın kimliğini denetlemek ve iletinin yetkili kullanıcı kimliği altında çalışan bir uygulamadan gelip gelmediğini sınamak için kullanılabilir.

Bir sunucu programı, alternatif bir kullanıcının kullanıcı kimliğini belirlemek için UserIdentifier ' i kullanabilir. Bağlam yetkisi, kullanıcının herhangi bir MQOPEN ya da MQPUT1 çağrısında bağlam seçeneklerinden herhangi birini belirtip belirtemeyeceğini denetlemek için kullanılır.

Bağlam seçenekleriyle ilgili bilgi için Bağlam bilgilerini denetleme başlıklı konuya ve bağlamla ilgili ileti tanımlayıcı alanlarının açıklamaları için MQMD ' ye genel bakış başlıklı konuya bakın.

Güvenlik çıkışlarında erişim denetiminin uygulanması

Erişim denetimini, MCAUserIdentifier ya da nesne yetkili yöneticisi kullanarak bir güvenlik çıkışta uygulayabilirsiniz.

MCAUserIdentifier

Geçerli olan bir kanalın her yönetim ortamı, ilişkili bir kanal tanımlama yapısına, MQCD ' ye sahiptir. MQCD ' deki alanların ilk değerleri, bir IBM MQ yöneticisi tarafından yaratılan kanal tanımlamasıyla belirlenir. Özellikle, alanlardan birinin (*MCAUserIdentifier*) ilk değeri, DEFINE CHANNEL komutundaki MCAUSER parametresinin değeri ya da kanal tanımlaması başka bir şekilde yaratıldıysa MCAUSER değerine göre belirlenir.

MQCD yapısı, bir MCA tarafından çağrıldığında kanal çıkış programına geçirilir. MCA tarafından bir güvenlik çıkışı çağrıldığında, güvenlik çıkışı, kanal tanımında belirtilen herhangi bir değeri değiştirerek *MCAUserIdentifier*değerini değiştirebilir.

Multi Multiplatformsüzerinde, *MCAUserIdentifier* değeri boşluksa, kuyruk yöneticisi, bir MCA kuyruk yöneticisine bağlandıktan sonra kuyruk yöneticisinin kaynaklarına erişmeye çalıştığında, yetki denetimi için kullanıcı kimliği olarak *MCAUserIdentifier* değerini kullanır. *MCAUserIdentifier* değeri boşsa, kuyruk yöneticisi bunun yerine MCA ' nın varsayılan kullanıcı kimliğini kullanır. Bu, RCVR, RQSTR, CLUSRCVR ve SVRCONN kanallarına uygulanır. MCA ' ların gönderilmesi için, *MCAUserIdentifier* değeri boş olmasa da, varsayılan kullanıcı kimliği her zaman yetki denetimleri için kullanılır.

z/OS z/OSüzerinde, kuyruk yöneticisi, boş olmadığı sürece yetki denetimleri için *MCAUserIdentifier* değerini kullanabilir. Kuyruk yöneticisinin yetki denetimleri için *MCAUserIdentifier* değerini kullanıp kullanmadığı, MCA 'ları ve sunucu bağlantısı MCA' ları almak için aşağıdakine bağlıdır:

- Kanal tanımlamasındaki PUUTUT parametresinin değeri
- Çekler için kullanılan RACF profili
- Kanal başlatıcı adres alanı kullanıcı kimliğinin RESLEVL tanıtıma erişim düzeyi

MCA ' ları gönderirken aşağıdakine bağlıdır:

- Gönderen MCA ' nın bir çağıran mı, yoksa yanıt veren mi olduğu
- Kanal başlatıcı adres alanı kullanıcı kimliğinin RESLEVL tanıtıma erişim düzeyi

The user ID that a security exit stores in *MCAUserIdentifier* can be acquired in various ways. Bazı örnekler:

- Bir MQI kanalının istemci ucunda herhangi bir güvenlik çıkışı olmaması koşuluyla, istemci uygulaması bir MQCONN çağrısı yayınlarken, IBM MQ istemci uygulaması ile ilişkilendirilmiş bir kullanıcı kimliği istemci bağlantısından sunucu bağlantısı MCA ' ya akıp gönderir.Sunucu bağlantısı MCA, kanal tanımlama yapısındaki *RemoteUserIdentifier* (Uzak Kullanıcı Kimliği) alanında bu kullanıcı kimliğini saklar, MQCD ' dir. *MCAUserIdentifier* değeri şu anda boşsa, MCA *MCAUserIdentifier*içinde aynı kullanıcı kimliğini saklar. If the MCA does not store the user ID in *MCAUserIdentifier*, a security exit can do it later by setting *MCAUserIdentifier* to the value of *RemoteUserTanıtıcısı*.

  İstemci sisteminden akan kullanıcı kimliği yeni bir güvenlik etki alanına giriyorsa ve sunucu sisteminde geçerli değilse, güvenlik çıkışı, geçerli olan bir kullanıcı kimliğinin yerine konabilir ve yerine koyulan kullanıcı kimliğini *MCAUserIdentifier*' ta saklayabilir.
- Kullanıcı kimliği, bir güvenlik iletisinde iş ortağı güvenlik çıkışı tarafından gönderilebilir.

  Bir ileti kanalında, MCA gönderme işlemi tarafından çağrılan bir güvenlik çıkışı, gönderen MCA ' nın çalıştığı kullanıcı kimliğini gönderebiliyor. Alıcı MCA tarafından çağrılan bir güvenlik çıkışı, kullanıcı kimliğini *MCAUserIdentifier*içinde saklayabilir. Benzer şekilde, bir MQI kanalında, kanalın istemci ucundaki güvenlik çıkışı, IBM MQ MQI client uygulamasıyla ilişkili kullanıcı kimliğini gönderebilir. Kanal sonunda bir güvenlik çıkışı, *MCAUserIdentifier*içindeki kullanıcı kimliğini saklayabilir. Önceki örnekte olduğu gibi, kullanıcı kimliği hedef sistemde geçerli değilse, güvenlik çıkışı, geçerli olan kullanıcı kimliğinin yerine konabilir ve yerine koyma değeri olan kullanıcı kimliğini *MCAUserIdentifier*içinde saklayabilir.

  Kimlik doğrulama ve kimlik doğrulama hizmetinin bir parçası olarak bir sayısal sertifika alınırsa, bir güvenlik çıkışı, sertifikadaki Ayırt Edici Adı, hedef sistemde geçerli olan bir kullanıcı kimliğiyle eşleyebilir. Daha sonra kullanıcı kimliğini *MCAUserIdentifier*içinde saklayabilir.
- Kanalda TLS kullanılırsa, iş ortağının Ayırt Edici Adı (DN), MQCD 'nin SSLPeerNamePtr alanında çıkışa geçirilir ve bu sertifikanın yayıncısının ayırt edici adı, MQCXP' nin SSLRemCertIssNamePtr alanındaki çıkışa iletilir.

MCAUserIdentifier alanı, kanal tanımlama yapısı, MQCD ve kanal çıkış parametresi yapısı, MQCXP hakkında daha fazla bilgi için Kanal çıkışı aramaları ve veri yapılarıbaşlıklı konuya bakın. Bir MQI kanalındaki bir istemci sisteminden akan kullanıcı kimliğine ilişkin daha fazla bilgi için bkz. Erişim denetimi.

Not: IBM WebSphere MQ 7.1 yayın düzeyinden önce oluşturulan güvenlik çıkış uygulamalarının güncellenmesi gerekebilir. Ek bilgi için bkz. Kanal güvenlik çıkış programları.

IBM MQ nesne yetkisi yöneticisi kullanıcı kimlik doğrulaması

IBM MQ MQI client bağlantılarında, nesne yetkilisi yöneticisi (OAM) kullanıcı kimlik doğrulamasında kullanılan MQCSP yapısını değiştirmek ya da yaratmak için güvenlik çıkışı kullanılabilir. Bu, ileti alışverişi kanallarına ilişkin kanal çıkışı programlarındaaçıklanmıştır.

İleti çıkışlarında erişim denetiminin uygulanması

Bir kullanıcı kimliğini diğeriyle değiştirmek için bir ileti çıkışı kullanmanız gerekebilir.

Bir sunucu uygulamasına ileti gönderen bir istemci uygulamasını göz önünde bulundurun. Sunucu uygulaması, ileti tanımlayıcısındaki *UserIdentifier* (Kullanıcı Kimliği) alanından kullanıcı kimliğini ayıklayabilir ve diğer kullanıcı yetkisine sahip olması koşuluyla, istemci adına IBM MQ kaynaklarına eriştiğinde yetki denetimi için kuyruk yöneticisinden bu kullanıcı kimliğini kullanmasını isteyin.

PUUTAT parametresi CTX olarak ayarlandıysa (ya da z/OS üzerinde ALTMCA) kanal tanımında, her gelen iletinin *UserIdentifier* alanında kullanıcı kimliği, MCA hedef kuyruğu açtığında yetki denetimleri için kullanılır.

Belirli durumlarda, bir rapor iletisi oluşturulduğunda, raporun neden olduğu iletinin *UserIdentifier* alanında kullanıcı kimliğinin yetkisi kullanılarak konmaktadır. Özellikle, teslim edilme (COD) raporları ve süre bitim raporları her zaman bu yetkiyle ortaya konudur.

Bu durumlar nedeniyle, yeni bir güvenlik etki alanına giren bir ileti olarak *UserIdentifier* (Kullanıcı Kimliği) alanında bir kullanıcı kimliğinin yerine başka bir kullanıcı kimliğinin yerine geçilmesi gerekebilir. Bu işlem, kanalın giriş ucundaki bir ileti çıkışı tarafından yapılabilir. Diğer bir seçenek olarak, gelen bir iletinin *UserIdentifier* alanındaki kullanıcı kimliğinin yeni güvenlik etki alanında tanımlı olduğunu doğrulayabilirsiniz.

Gelen bir ileti, iletiyi gönderen uygulamanın kullanıcısına ilişkin bir sayısal sertifika içeriyorsa, bir ileti çıkışı sertifikanda doğrulanabilir ve sertifikadaki Ayırt Edici Ad 'ı, giriş sisteminde geçerli olan bir kullanıcı kimliğine eşleyebilir. Daha sonra, ileti tanımlayıcısındaki *UserIdentifier* alanını bu kullanıcı kimliğine ayarlayabilir.

Gelen iletilerde *UserIdentifier* alanının değerini değiştirmek için bir ileti çıkışı gerekliyse, iletiyi gönderenin aynı anda kimliğini doğrulamak için ileti çıkışı için uygun olabilir. Daha fazla ayrıntı için bkz. “İleti çıkışlarında kimlik eşlemesi” sayfa 322.

API çıkışta ve API ' den geçiş çıkışındaki erişim denetimi uygulanıyor

Bir API ya da API geçiş çıkışı, IBM MQtarafından sağlananlara ek olarak erişim denetimleri sağlayabilir. Çıkış, özellikle ileti düzeyinde erişim denetimi sağlayabilir. Çıkış, bir uygulamanın bir kuyruğa yerleştirilmesini ya da kuyruktan alıkonmasını, yalnızca belirli ölçütlere uyan iletileri alıkoymasını sağlar.

Aşağıdaki örnekleri göz önünde bulundurun:

- Bir ileti, bir siparişe ilişkin bilgi içerir. Bir uygulama bir kuyruğa ileti yerleştirmeyi denediğinde, bir API ya da API geçiş çıkışı, siparişin toplam değerinin belirtilen sınırdan daha az olduğunu denetleyebilir.
- İletiler, uzak kuyruk yöneticilerinden bir hedef kuyruğa ulaşır. Bir uygulama kuyruktan ileti alma girişiminde bulunduğunda, bir API ya da API geçiş çıkışı, iletiyi gönderenin kuyruğa ileti gönderme yetkisine sahip olduğunu denetleyebilir.

LDAP Yetkilendirmesi

Yerel bir kullanıcı kimliğine olan gereksinimi kaldırmak için LDAP yetkilendirmesini kullanabilirsiniz.

Desteklenen platformlarda LDAP yetkilendirmesi kullanılabilirliği

LDAP yetkilendirmesi şu altyapılarda kullanılabilir:

- UNIX
- IBM i
- Windows

Uyarı:

IBM MQ 9.0 genel kullanılabilirliğinden itibaren, bu işlevsellik, yeni ya da yeni bir yayın düzeyinden geçirilmiş olan tüm kuyruk yöneticilerinde kullanılabilir.

LDAP yetkilendirmesine genel bakış

LDAP yetkilendirmesi ile, **setmqaut** ve **DISPLAY AUTHREC**gibi yetkilendirme yapılandırmasını işleyen komutlar Ayırt Edici Adları işleyebilirler. Daha önce, kullanıcıların kimlik bilgilerini, yerel işletim sistemindeki kullanıcılar ve gruplar için var olan en yüksek karakter üst sınırlarıyla karşılaştırarak kimlikleri doğrulanır.

Uyarı: DEFINE AUTHINFO komutunu çalıştırdıysanız, kuyruk yöneticisini yeniden başlatmanız gerekir. Kuyruk yöneticisini yeniden başlatmadıysanız, setmqaut komutu doğru sonucu döndürmez.

Bir kullanıcı Ayırt Edici Ad yerine bir kullanıcı kimliği sağlıyorsa, kullanıcı kimliği işlenir. Örneğin, PUTAUT (CTX) içeren bir kanalda bir gelen ileti varsa, kullanıcı kimliğindeki karakterler bir LDAP Ayırt Edici Adı ile eşlenir ve uygun yetkilendirme denetimleri yapılır.

Other commands such as **DISPLAY CONN**, continue to work with and show the actual value for the user ID, even though that user ID might not actually exist on the local OS.

UNIX When LDAP authorization is in place, the queue manager always uses the user model of security on UNIX platforms, regardless of the **SecurityPolicy** attribute in the `qm.ini` file. Dolayısıyla, tek bir kullanıcının izinlerini ayarlamak yalnızca o kullanıcıyı etkiler ve bu kullanıcının gruplarından herhangi birine ait olan başka biri değil.

İşletim sistemi modelinde olduğu gibi, bir kullanıcı, kullanıcının ait olduğu tüm gruplara (varsa) ve her birine atanmış olan birleşik yetkisine sahiptir.

Örneğin, bir LDAP havuzunda aşağıdaki kayıtların tanımlandığını varsayın.

- **inetOrgPerson** sınıfında:

```
dn="cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
        email=JohnDoe1@yourcompany.com [longer than 12 characters]
        shortu=jodoe
        Phone=1234567
```

- **groupOfNames** sınıfında:

```
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"
```

Kimlik doğrulama amacıyla, bu LDAP sunucusunu kullanan bir kuyruk yöneticisinin, `IDPWLDAP`tipindeki bir **AUTHINFO** nesnesinde **CONNAUTH** değer noktalarının ve ilgili ad çözme öznitelikleri büyük olasılıkla aşağıdaki gibi ayarlandığı şekilde tanımlanmış olmalıdır:

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

Kimlik doğrulama için bu yapılandırma verilirse, uygulama, aşağıdaki değer kümelerinden biriyle birlikte, MQCNO çağrısında kullanılan CSPUserID alanını tamamlayabilir:

```
" cn=JohnDoe ", " JohnDoe1@yourcompany.com ", " email=JohnDoe1@yourcompany.com "
```

ya da

```
" cn=JohnDoe, ou=users, o=ibm, c=uk ", " shortu=jodoe "
```

Her iki durumda da, sistem, işletim sistemi bağlamını doğrulamak için sağlanan değerleri kullanabilir. "`jodoe`".

Yetkilerin ayarlanması

Yetkileri ayarlamak için kısa adı ya da **USRFIELD** ' ı kullanabilirsiniz.

The approach of working with multiple formats, described in “LDAP Yetkilendirmesi” sayfa 395, continues into the authorization commands, with a further extension that either the `shortname` or the USRFIELD can be used in an unadorned fashion.

Yetki için kullanıcılar (asıl adlar) adlandırılırken, LDAP kaydındaki belirli bir özniteliği karakter dizilimi belirler.

Önemli: Bir işletim sistemi kullanıcı kimliğiyle bu karakter kullanılamadığı için, karakter dizgisi = karakteri içermemelidir.

Potansiyel olarak `shortname`olan yetki için bir birincil kullanıcı adını OAM ' a geçirseniz, karakter dizgisi 12 karaktere sığmalıdır. Eşleme algoritması ilk olarak, LDAP sorgusuna SHORTUSR özniteliğini kullanarak bunu bir DN ' ye çözümlemeyi dener.

Bu bir UNKNOWN_ENTITY hatasıyla başarısız olursa ya da belirtilen dizgi bir `shortname`olamaz ise, LDAP sorgusını oluşturmak için USRFIELD özniteliği kullanılarak başka bir girişimde bulunulması gerekir.

Uyarı: DEFE AUTHINFO komutunu çalıştırdıysanız, kuyruk yöneticisini yeniden başlatmanız gerekir. Kuyruk yöneticisini yeniden başlatmadıysanız, setmqaut komutu doğru sonucu döndürmez.

Kullanıcı yetkilerinin işlenmesi için, aşağıdaki setmqaut komut ayarları eşdeğerdir.

Çizelge 72. Kullanıcı yetkilendirme ayarları

Komut	**Not**
`setmqaut -m QM -t qmgr -p jodoe +connect`	Bu, SHORUSR ile çözülen düz, nitelenmemiş bir addır.
`setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect`	Aynı zamanda, USRFIELD yoluyla aynı varlık için düz, nitelenmemiş bir ad.
`setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect`	Adlandırılmış bir öznitelik kullanılıyor.
`setmqaut -m QM -t qmgr -p "phone=1234567" +connect`	AUTHINFO nesnesinde yapılandırılanların hiçbiri olması gerekmeyen başka bir adlandırılmış öznitelik kullanılıyor.

AUTHREC MQSC komutunu **`setmqaut`** komutuna bir alternatif olarak kullanabilirsiniz:

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

ya da dizgiyi içeren MQCACF_PRINCIPAL_ENTITY_NAMES öğesindeki Set Authority Record (MQCMD_SET_AUTH_REC) PCF komutu:

```
 "cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Grupları işlerken, grup adının 12 karaktere sığması için herhangi bir gereksinim olmadığından, `shortname` işlemleriyle ilgili belirsizlik yoktur. Bu nedenle, gruplar için SHORUSR özniteliğe eşdeğer bir değer yoktur.

That means that the syntax examples described in Çizelge 73 sayfa 397 are valid, assuming that you have configured the AUTHINFO object with the extended attributes, and set to:

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Çizelge 73. Grup yetkilendirme ayarları

Komut	**Not**
`setmqaut -m QM -t qmgr -g ApplicationGroupA +connect`	Çözümlemek için GRPFIELD kullanılıyor
`setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect`	Tek bir özniteliğin adlandırılıyor

Çizelge 73. Grup yetkilendirme ayarları (devamı var)	
Komut	**Not**
`setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect`	Tam DN ' nin kullanılması

You can use the AUTHREC MQSC command as an alternative to the preceding **setmqaut** command:

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
      AUTHADD(connect)
```

ya da dizgiyi içeren MQCACF_GROUP_ENTITY_NAMES öğesindeki Set Authority Record (MQCMD_SET_AUTH_REC) PCF komutu:

```
  "ApplicationGroupA"
```

Önemli:

Bir adı belirtmek için hangi biçimi kullanırsanız kullanın, kullanıcı ya da grup için benzersiz bir ayırt edici ad (DN) türetilmesi mümkün olmalıdır.

Bu nedenle, örneğin, her ikisinin de "`shortu=jodoe`" sahip olduğu iki ayrı kayıtınız olmamalıdır.

Tek bir benzersiz DN saptanamazsa, OAM MQRC_UNKNOWN_ENTITY dizgisini döndürür.

Yetkilerin görüntülenmesi

Kullanıcı ya da grup yetkilendirmesini görüntüleme yöntemleri çeşitli yöntemler.

dspmqaut komutu

Bir kullanıcı ya da grup için kullanılabilir yetkilerin görüntülenmesine ilişkin en basit yöntem, dspmqaut komutunu kullanmandır.

Bir kullanıcıyı ya da grubu tanımlamak için sözdizimi varyasyonlarından herhangi birinde bir sorgu kullanabilirsiniz. Komut çıktısının, tanıtıcısı komut satırında belirtilen biçimde yinelediğine dikkat edin. Çıktı, tam çözülmüş DN ' de raporlanmaz.

Örneğin:

```
dspmqaut -m QM -t qmgr -p johndoe
Entity johndoe has the following authorizations for object QM:
    connect
```

ya da

```
dspmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com
Entity email=JohnDoe1@yourcompany.com has the following authorizations for object QM:
    connect
```

dmpmqaut ve dmpmqcfg komutları

dmpmqaut komutu ve MQSC ya da PCF eşdeğerleri, “Yetkilerin ayarlanması” sayfa 396içinde açıklanan **setmqaut** çizelgeleri gibi, birincil kullanıcı ya da grubu desteklenen biçimlerden herhangi birinde belirtebilir. Ancak, **dspmqaut**'tan farklı olarak, **dmpmqaut** komutu her zaman tam DN' yi bildirir.

```
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
```

Benzer şekilde, seçilen kayıtlarda süzgeç uygulanmamış olan dmpmqcfg komutu, daha sonra yeniden yürütülebilecek bir biçimde her zaman tam DN ' yi gösterir.

```
dmpmqcfg -m QM -x authrec
-----------------------------------
SET AUTHREC PROFILE(SELF) +
    PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
    OBJTYPE(QMGR)
    AUTHADD(CONNECT)
```

LDAP yetkilendirmesi kullanılırken dikkate alınması gereken diğer noktalar

Message Queue Interface (MQI) ve diğer MQSC ve PCF komutlarındaki değişikliklerin kısa bir tanımı, IBM MQ 9.0.0' den LDAP yetkilendirmesi kullanılırken bilmeniz gerekir.

ADOPTCTX

Uygulamaların kimlik doğrulama bilgilerini sağlamasına ya da ADOPTTCTX özniteliğinin YES değerine ayarlanabilmesine gerek yoktur.

Bir uygulama belirtik olarak kimlik doğrulamazsa ya da **ADOPTCTX** , etkin CONNAUTH nesnesi için NO olarak ayarlandıysa, uygulamayla ilişkili kimlik bağlamı, işletim sistemi kullanıcı kimliğinden alınır.

Yetkilerin uygulanması gerektiğinde, bu bağlam, setmqaut komutlarıyla aynı kuralları kullanan bir LDAP kimliğine eşlenmektedir.

MQI çağrılarına değiştirge giriş değiştirgeleri

MQOPEN, MQPUT1, and MQSUB have structures that allow an alternative user ID to be specified.

Bu alanlar kullanılırsa, 12 karakterlik kullanıcı kimliği, **setmqaut**, **dmpmqaut**ve **dspmqaut** komutlarında olduğu gibi aynı kuralları kullanan bir DN ile eşlenir.

MQPUT ve MQPUT1 , ayrıca, MQMD UserIdentifier (Kullanıcı Kimliği) alanını ayarlamak için uygun yetkili programlara da izin verir. Bu alanın değeri, PUT işlemi sırasında ilkeye bağlı değildir ve herhangi bir değere ayarlanabilir.

Ancak her zamanki gibi, **UserIdentifier** değeri ileti işleme aşamalarında yetkilendirme için kullanılabilir; örneğin, PUTAUT (CTX) alıcı bir kanalda tanımlandığında.

Bu noktada, LDAP ya da OS-tabanlı olabilen alan kuyruk yöneticisinin yapılandırması kullanılarak kimlik denetimi için kimlik denetimi yapılacaktır.

MQI çağrılarına ilişkin çıkış değiştirgeleri

Bir MQI yapısındaki bir programa kullanıcı kimliği sağlansa, bu, bağlantıyla ilişkili 12 karakterlik kısa ad sürüsüdür.

Örneğin, API Exits için **MQAXC.UserId** değeri, LDAP eşlemesinden döndürülen kısa addır.

Diğer denetim MQSC ve PCF komutları

GöRüNEN EKRAN USERID gibi nesne durumlarında kullanıcı bilgilerini gösteren komutlar, bağlamla ilişkili 12 karakterlik kısa adı döndürür. Tam ayırt edici ad (DN) gösterilmez.

Kanallara ilişkin CHLAUTH eşleme kuralları ya da MCAUSER değerleri gibi kimliklerin değerlendirilmesine izin veren komutlar, bu öznitelikler için tanımlanan uzunluk üst sınırına kadar değer alabilir (şu an 64 karakter).

Sözdiziminde değişiklik yok. Bu kimlik için yetkilendirme gerekli olduğunda, **setmqaut**, **dmpmqaut**ve **dspmqaut** komutlarıyla aynı kuralları kullanan bir DN ' ye dahili olarak eşlenir.

Başka bir deyişle, bir kanal tanımlamasındaki MCAUSER değeri, DISPLAY CHSTATUS ile aynı dizgi olarak görüntülenmeyebilir, ancak bunlar aynı tanıtıcıyı gösterirler.

Örneğin:

```
DEFINE CHL(SV1) CHLTYPE(SVRCONN) MCAUSER('cn=JohnDoe')
DEFINE CHL(SV2) CHLTYPE(SVRCONN) MCAUSER('jodoe')
DEFINE CHL(SV3) CHLTYPE(SVRCONN) MCAUSER('JohnDoe1@yourcompany.com')
```

Sonra DISPLAY CHSTATUS (*) ALL, tüm bağlantılar için SHORTUSR değerini, *MCAUSER (jodoe)* değerini gösterir.

İşletim sistemi ile LDAP yetkilendirme modelleri arasında geçiş yapılması

Farklı platformlarda farklı yetkilendirme yöntemleri arasında geçiş yapmak.

Bir AUTHINFO nesnesinde kuyruk yöneticisinin CONNAUTH özniteliği noktalıyor. Nesne IDPWLDAP tipinden olduğunda, kimlik doğrulaması için bir LDAP havuzu kullanılır.

Şimdi aynı nesneye bir yetkilendirme yöntemi uygulayabilir, böylece işletim sistemi tabanlı yetkilendirme ile devam edebilirsiniz ya da LDAP yetkilendirmesi ile çalışabilirsiniz.

UNIX platformları ve IBM i

IBM i UNIX

Kuyruk yöneticisi, işletim sistemi ile LDAP modelleri arasında herhangi bir zamanda değişimli olarak kullanılabilir. Yapılandırmayı değiştirebilir ve GüVENLIK TIPINI YENILE (CONNAUTH) komutunu kullanarak bu yapılandırmayı etkin hale getirebilirsiniz.

Örneğin, bu nesne kimlik doğrulamaya ilişkin bağlantı bilgisiyle önceden yapılandırıldıysa:

```
ALTER AUTHINFO(MYLDAP) AUTHTYPE(IDPWLDAP) +
        AUTHORMD(SEARCHGRP) +
        BASEDNG('ou=groups,o=ibm,c=uk') +
        <other attributes>
ALTER QMGR CONNAUTH(MYLDAP)
REFRESH SECURITY
```

Windows

Windows

Bir yetki yapılandırması değişikliği, işletim sistemi ve LDAP modelleri arasında geçiş yapmayı gerektiriyorsa, değişikliğin yürürlüğe girmesi için kuyruk yöneticisinin yeniden başlatılması gerekir. Otherwise, you can make the change active by using the GüVENLIK TIPINI YENILE (CONNAUTH) command.

İşleme kuralları

OS ' den LDAP yetkilendirmesine geçilirken, ayarlanmış olan var olan işletim sistemi yetkisi kuralları etkin değil ve görünmez olur.

dmpmqaut gibi komutlar bu işletim sistemi kurallarını görüntülemez. Benzer şekilde, LDAP ' den işletim sistemine geçildiğinde, tanımlı olan herhangi bir LDAP yetkilendirmesi devre dışı ve görünmez hale gelir ve özgün işletim sistemi kurallarını geri yükler.

Bir kuyruk yöneticisinin tanımlarını herhangi bir nedenle yedeklemek istiyorsanız, **dmpmqcfg** komutunu kullanarak, yedekleme işlemi yalnızca yedekleme sırasında yürürlükte olan yetkilendirme yöntemi için tanımlanmış kuralları içerir.

LDAP denetimi

Her bir platformun LDAP ' a nasıl sahip olduğu hakkında genel bir bakış.

LDAP yetkilendirmesi kullanılırken, işletim sistemindeki mqm grubunun (ya da eşdeğer) üyeliği o kadar önemli değildir. Bu grubun bir üyesi olmak, yalnızca belirli komut satırı komutlarının işlenip işlenemeyeceğini denetler.

Özellikle, strmqm ve endmqm komutlarını vermek için o grupta yer almalısınız.

Kuyruk yöneticisi çalıştırıldıktan sonra, tamamen ayrıcalıklı hesapla ilgili sınırlar vardır. **strmqm** komutunu veren kişinin kullanıcı kimliği dışında, işletim sistemi mqm (ya da eşdeğeri) grubuna ait olan diğer kullanıcılar özel ayrıcalıklar elde etmiŸler.

Diğer kullanıcıların yetkileri, ait oldukları LDAP gruplarını temel alır. An unqualified use of the mqm group name in commands such as **setmqaut** is not allowed to map to any LDAP group.

UNIX Platformlar

Kuyruk yöneticisi çalışır durumda olduğunda, otomatik olarak tam olarak ayrıcalıklı hesap, kuyruk yöneticisini başlatan gerçek kullanıcı olur.

mqm kimliği hala var ve dosyalar gibi işletim sistemi kaynaklarının sahibi olarak kullanılıyor; çünkü mqm , kuyruk yöneticisinin çalışmakta olduğu etkin tanıtıcıdır. Ancak, mqm kullanıcısı, OAM tarafından denetlenen yönetim görevlerini otomatik olarak yapamayacaktır.

IBM i

IBM i' ta, otomatik olarak ayrıcalıklı hesaplar, kuyruk yöneticisini ve QMQM tanıtıcısını başlatan en ayrıcalıklı hesaplardır.

Kuyruk yöneticisini başlatan kullanıcı kimliği, yalnızca sistemi başlatmak için gerekli olduğundan, her iki tanıtıma da gereksinim duyarsınız. Kuyruk yöneticisi işlemleri yürütüldükten sonra yalnızca QMQM yetkisine sahiptir.

Windows Platformlar

Windowsüzerinde, otomatik olarak tam olarak ayrıcalıklı hesaplar, kuyruk yöneticisini başlatan işletim sistemi kullanıcıdır ve kuyruk yöneticisi Windows hizmeti olarak başlatıldıysa, MUSR_MQADMIN gibi çekirdek kuyruk yöneticisi işlemlerini çalıştıran kullanıcı da.

LDAP yetkilendirme kipinde çalışırken, Windows , UNIX platformlarına çok benzer şekilde davranır. 12 karakterlik kısa adlarla ve tam DN ' lerle ilgilenir.

Örnek komut dosyası

Bir kuyruk yöneticisi üzerinde bir grubun tam olarak yönetilebilir olması yararlı olduğu için, UNIX platformlarında aşağıdaki gibi örnek bir komut dosyası gönderilir:

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

Bu örnek iki parametre alır:

- Kuyruk yöneticisi adı
- Bir LDAP grubu adı

Örnek, tüm nesneler için tam yetki vermek üzere setmqaut komutları işlemektedir. Bu, yönetim rolleri için IBM MQ Explorer OAM Wizard tarafından oluşturulan komut dosyasıdır. Örneğin, kod aşağıdaki gibi başlar:

```
setmqaut -t q -m qmgr -n "**" +alladm +allmqi -g
      groupname
```

İletilerin gizliliği

Gizliliği korumak için, mesajlarınızı şifreleyin. Gereksinimlerinize bağlı olarak IBM MQ ' ta iletileri şifrelemenin çeşitli yöntemleri vardır.

Your choice of CipherSpec determines what level of confidentiality you have.

İleti düzeyinde, uçtan uca ileti sistemi altyapısı için uçtan uca veri koruması gerekiyorsa, İletileri şifrelemek için Advanced Message Security kullanın ya da kendi API çıkışınızı ya da API geçiş çıkışınızı yazabilirsiniz.

İletileri yalnızca bir kanaldan aktarırken şifrelemeniz gerekiyorsa, kuyruk yöneticilerinizde yeterli güvenliğiniz olduğundan, TLS ' yi kullanabilir ya da kendi güvenlik çıkışınızı, ileti çıkışınızı yazabilir ya da çıkış programlarını gönderebilir ya da alabilirsiniz.

z/OS V 9.1.4 Bir kuyruk yöneticisinde kalan iletileri şifrelemeniz gerekiyorsa, o kuyruk yöneticisinde z/OS veri kümesi şifrelemesini kullanabilirsiniz.

Advanced Message Securityile ilgili daha fazla bilgi için bkz. “Advanced Message Securityplanlaması” sayfa 99. The use of TLS with IBM MQ is described at “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22. İleti şifrelemesinde çıkış programlarının kullanımı şu adreste açıklanmıştır: “Kullanıcı çıkış programlarında gizliliği uygulama” sayfa 430.

confidentiality for data at rest on IBM MQ for z/OS with data set encryption.bölümüne bakın. z/OS veri kümesi şifrelemesi hakkında daha fazla bilgi için.

İlgili görevler

İki kuyruk yöneticisinin TLS ' yi kullanarak bağlanması

İstemcinin kuyruk yöneticisine güvenli bir şekilde bağlanması

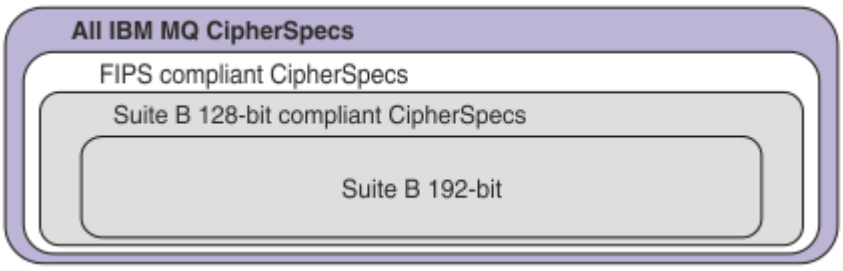
CipherSpecs' in etkinleştirilmesi

Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

IBM MQ ile kullanabileceğiniz bazı CipherSpecs , FIPS uyumludur. Some of the FIPS compliant CipherSpecs are also Suite B compliant although others, such as TLS_RSA_WITH_AES_256_CBC_SHA, are not.

Tüm Suite B uyumlu CipherSpecs da FIPS uyumludur. Tüm Suite B uyumlu CipherSpecs iki gruba ayrılır: 128 bit (örneğin, ECDHE_ECDSA_AES_128_GCM_SHA256) ve 192 bit (örneğin, ECDHE_ECDSA_AES_256_GCM_SHA384),

Aşağıdaki şemada bu altkümeler arasındaki ilişki gösterilir:



IBM MQ 8.0.0 Fix Pack 3 ' tan desteklenen CipherSpecs sayısı azaltıldı.

V 9.1.1 Varsayılan CipherSpecs' ı yapılandırma hakkında bilgi için bkz. “Default CipherSpec values enabled in IBM MQ” sayfa 406. Ayrıca, MQ kanallarıyla birlikte kullanılmak üzere etkinleştirilen alternatif bir CipherSpecs kümesi de sağlayabilirsiniz. Bkz. “Çoklu Platformlar üzerinde etkinleştirilen CipherSpecs özel bir listesini sağlama” sayfa 407.

Kullanımdan kaldırılan CipherSpecs' nin etkinleştirilmesiyle ilgili bilgi için bkz. “Kullanımdan kaldırılan CipherSpecs on Multiplatforms özelliğinin” sayfa 407 ya da “z/OSüzerinde kullanımdan kaldırılan CipherSpecs ' in etkinleştirilmesi” sayfa 408. For a list of CipherSpecs that you can re-enable to use with IBM MQ, see “Kullanımdan kaldırılan CipherSpecs” sayfa 411.

ULW V 9.1.4 From IBM MQ 9.1.4, IBM MQ supports the TLS 1.3 security protocol on UNIX, Linux, and Windows. Bu CipherSpecs' in kullanılmasıyla ilgili bilgi için bkz. “Using TLS 1.3 in IBM MQ” sayfa 405 ve “IBM MQ MQI client ve TLS 1.3” sayfa 406.

IBM MQ TLS desteğiyle kullanabileceğinizCipherSpecs

IBM MQ kuyruk yöneticisiyle birlikte kullanabileceğiniz şifreleme belirtimleri, aşağıdaki çizelgede otomatik olarak listelenir. Kişisel bir sertifika istediğinizde, genel ve özel anahtar çifti için bir anahtar boyutu belirtiyorsunuz. The key size that is used during the TLS handshake is the size stored in the certificate unless it is determined by the CipherSpec, as noted in the table.

Çizelge 74. CipherSpecs IBM MQ TLS desteği ile kullanabilirsiniz

Platform desteği “1” sayfa 405	CipherSpec adı	Onaltılı kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS “2” sayfa 405	Takım B
V 9.1.4 V 9.1.4 **Diğer Ad CipherSpecs**							
Tümü	ANY_TLS13_OR_HIGHER “3” sayfa 405 “4” sayfa 405 “5” sayfa 405	Yok	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı
Tümü	ANY_TLS13 “4” sayfa 405 “5” sayfa 405 “6” sayfa 405	Yok	TLS 1.3	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı
Tümü	ANY_TLS12_OR_HIGHER “4” sayfa 405 “5” sayfa 405 “7” sayfa 405	Yok	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı
Tümü	ANY_TLS12 “8” sayfa 405	Yok	TLS 1.2	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı
Tümü	ANY “9” sayfa 405	Yok	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı	Anlaşmalı
V 9.1.4 V 9.1.4 **CipherSpecs for TLS 1.3**							
Tümü	TLS_AES_128_GCM_SHA256 “4” sayfa 405	1301	TLS 1.3	GCM	AES-128 (GCM ile) (128)	Evet	Hayır
Tümü	TLS_AES_256_GCM_SHA384 “4” sayfa 405	1302	TLS 1.3	GCM	AES-256 (GCM ile) (256)	Evet	Hayır
Tümü	TLS_CHACHA20_POLY1305_SHA256 “4” sayfa 405	1303	TLS 1.3	POLY1305	CHACHA20 (256)	Hayır	Hayır
ULW	TLS_AES_128_CCM_SHA256	1304	TLS 1.3	CBC-MAC	AES-128 (CTR ile) (128)	Evet	Hayır

Çizelge 74. CipherSpecs IBM MQ TLS desteği ile kullanabilirsiniz (devamı var)

Platform desteği "1" sayfa 405	CipherSpec adı	Onaltılık kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS "2" sayfa 405	Takım B
ULW	TLS_AES_128_CCM_8_SHA256 "11" sayfa 405	1305	TLS 1.3	CBC-MAC	AES-128 (CTR ile) (128)	Evet	Hayır
CipherSpecs for TLS 1.2							
Tümü	TLS_RSA_WITH_AES_128_CBC_SHA256 "10" sayfa 405	003C	TLS 1.2	SHA-256	AES (128)	Evet	Hayır
Tümü	TLS_RSA_WITH_AES_256_CBC_SHA256 "10" sayfa 405 "12" sayfa 405	003D	TLS 1.2	SHA-256	AES (256)	Evet	Hayır
Tümü	TLS_RSA_WITH_AES_128_GCM_SHA256 "10" sayfa 405 "13" sayfa 405	009C	TLS 1.2	SHA-256 ve AEAD GCM	AES (128)	Evet	Hayır
Tümü	TLS_RSA_WITH_AES_256_GCM_SHA384 "10" sayfa 405 "12" sayfa 405 "13" sayfa 405	009D	TLS 1.2	SHA-384 ve AEAD GCM	AES (256)	Evet	Hayır
Tümü	ECDHE_ECDSA_AES_128_CBC_SHA256 "10" sayfa 405	C023	TLS 1.2	SHA-256	AES (128)	Evet	Hayır
Tümü	ECDHE_ECDSA_AES_256_CBC_SHA384 "10" sayfa 405 "12" sayfa 405	C024	TLS 1.2	SHA-384	AES (256)	Evet	Hayır
Tümü	ECDHE_RSA_AES_128_CBC_SHA256 "10" sayfa 405	C027	TLS 1.2	SHA-256	AES (128)	Evet	Hayır
Tümü	ECDHE_RSA_AES_256_CBC_SHA384 "10" sayfa 405 "12" sayfa 405	C028	TLS 1.2	SHA-384	AES (256)	Evet	Hayır
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 "12" sayfa 405 "13" sayfa 405	C02B	TLS 1.2	SHA-256 ve AEAD GCM	AES (SHA384)	Evet	128 bit
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 "12" sayfa 405 "13" sayfa 405	C02C	TLS 1.2	SHA-384 ve AEAD GCM	AES (SHA384)	Evet	192 bit
Tümü	ECDHE_RSA_AES_128_GCM_SHA256 "13" sayfa 405	C02F	TLS 1.2	SHA-256 ve AEAD GCM	AES (128)	Evet	Hayır
Tümü	ECDHE_RSA_AES_256_GCM_SHA384 "12" sayfa 405 "13" sayfa 405	C030	TLS 1.2	AEAD AES-128 GCM	AES (SHA384)	Evet	Hayır

Çizelge 74. CipherSpecs IBM MQ TLS desteği ile kullanabilirsiniz (devamı var)

Platform desteği "1" sayfa 405	CipherSpec adı	Onaltılı kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS "2" sayfa 405	Takım B

Notlar:

1. Her platform simgesinin kapsadığı platformların bir listesi için ürün belgelerinde Yayın ve platform simgeleribaşlıklı konuya bakın.
2. CipherSpec ' in FIPS onaylı bir platformda FIPS onaylı olup olmadığını belirtir. FIPS ' ye ilişkin açıklamalar için bkz. Federal Information Processing Standards (FIPS) .
3. ULW ANY_TLS13_OR_HIGHER diğer adı CipherSpec , uzak ucun izin vereceği, ancak yalnızca TLS 1.3 ya da daha yüksek bir iletişim kuralı kullanılarak bağlanacağı en yüksek güvenlik düzeyini kararlaştırır.
4. z/OS IBM MQ for z/OSüzerinde TLS 1.3ya da ANY CipherSpeckullanmak için işletim sisteminin z/OS 2.4 ya da üstü olması gerekir.
5. IBM i TLS 1.3ya da ANY CipherSpeckullanmak için IBM i üzerindeki temel işletim sistemi sürümü TLS 1.3' ü desteklemelidir. Daha fazla bilgi için bkz. TLSv1.3 .
6. ULW ANY_TLS13 diğer adı CipherSpec , her platform için bu tabloda listelendiği şekilde TLS 1.3 iletişim kuralını kullanan kabul edilebilir CipherSpecs alt kümesini temsil eder.
7. ULW ANY_TLS12_OR_HIGHER diğer adı CipherSpec , uzak ucun izin vereceği en yüksek güvenlik düzeyini kararlaştırır, ancak yalnızca TLS 1.2 ya da daha yüksek bir iletişim kuralı kullanılarak bağlanır.
8. ANY_TLS12 CipherSpec , her platform için bu tabloda listelendiği şekilde TLS 1.2 protokolünü kullanan kabul edilebilir CipherSpecs alt kümesini temsil eder.
9. ULW ANY diğer adı CipherSpec , uzak ucun izin vereceği en yüksek güvenlik düzeyini kararlaştırır.
10. IBM i Bu CipherSpecs , QSSLCSLCTL Sistem Değeri *OPSSYS olarak ayarlanmış IBM i 7.4 sistemlerinde etkinleştirilmez.
11. ULW Bu CipherSpecs , 16 oktet ICV yerine 8 oktet Bütünlük Denetimi Değeri (ICV) kullanır.
12. Bu CipherSpec , Gezgin tarafından kullanılan JRE ' ye uygun kısıtlamasız ilke dosyaları uygulanmadıkça, IBM MQ Explorer ile bir kuyruk yöneticisi arasındaki bağlantıyı güvenli kılmak için kullanılamaz.
13. Windows Linux GSKittarafından yapılan bir öneriyi takiben TLS 1.2 GCM CipherSpecs ' I ileti ile sınırlama vardır; bu kısıtlama ve üzerinden eleri geçtikten sonra24.5 TLS kayıtları aynı oturum anahtarı kullanılarak gönderildikten sonra bağlantının AMQ9288Eiletisiyle sonlandırıldığı anlamına gelir. Bu GCM kısıtlaması, kullanılmakta olan FIPS kipinden bağımsız olarak etkindir.

    Bu hatanın oluşmasını önlemek için TLS 1.2 GCM şifrelemeleri kullanmaktan kaçının, gizli anahtar sıfırlamasını etkinleştirin ya da IBM MQ kuyruk yöneticinizi ya da istemcinizi `GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE` ortam değişkeniyle başlatın. GSKit kitaplıkları için, bu ortam değişkenini bağlantının her iki tarafına da ayarlamalı ve hem kuyruk yöneticisi bağlantıları için istemciye hem de kuyruk yöneticisi bağlantıları için kuyruk yöneticisine uygulamalısınız. Bu ayarın yönetilmeyen .NET istemcilerini etkilediğini, ancak Java ya da yönetilen .NET istemcilerini etkilemediğini unutmayın. Daha fazla bilgi için bkz. AES-GCM şifre sınırlaması.

    Bu kısıtlama IBM MQ for z/OSiçin geçerli değildir.

Using TLS 1.3 in IBM MQ

ULW V 9.1.4

IBM MQ 9.1.4içinden IBM MQ , UNIX, Linux, and Windowsüzerinde TLS 1.3 ' ü destekler. Desteklenen herhangi bir kurulumda, yeni kuyruk yöneticileri qm.iniSSL stanza dosyasındaki bir girişle yaratılır:

```
SSL:
  AllowTLSV13=TRUE
```

Not: The file qm.ini can be found in the directory <*data directory*>/qmgrs/<*qmgr name*>.

Kuyruk yöneticisi IBM MQ 9.1.4sürümünden önceki bir IBM MQ sürümü kullanılarak yaratıldıysa, ancak daha sonra IBM MQ 9.1.4 ya da daha yüksek bir sürümünü kullanmaya başladıysa, **AllowTLSV13** özellik kümesine sahip olmaz. TLS 1.3'ü etkinleştirmek istiyorsanız, qm.ini file dosyasını düzenlemeniz ve örnekte gösterildiği gibi ("SSL:" kısmı da dahil olmak üzere) " zellik' i (varsa) eklemeniz gerekir.

Bu .ini dosyası özelliği, TLS 1.3 CipherSpecs'ın kullanılmasına izin veren TLS 1.3' ün geçerli olduğunu sağlar. In accordance with the TLS 1.3 belirtimi, any attempts to communicate with a weak CipherSpec, regardless of whether they are enabled in IBM MQ or not, will be rejected. TLS 1.3 'in zayıf olarak kabul ettiği CipherSpecs , aşağıdaki ölçütlerden birini ya da birkaçını karşılayan CipherSpecs ' dır.

- SSL 3.0 iletişim kuralını kullanır.
- Şifreleme algoritması olarak RC4 ya da RC2 ' yi kullanır.
- Bir şifreleme anahtarı büyüklüğü (bit) 112 'ye eşit ya da daha düşük bir değere sahiptir.

These restrictions are flagged with Note [10] in Kullanımdan Kaldırılan CipherSpecsçizelgesi 1.

Bu tür CipherSpecsözelliğini kullanmaya devam etmeniz gerekiyorsa, TLS 1.3 kipini devre dışı bırakmanız gerekir. Bunu yapmak için, kuyruk yöneticisinin qm.ini dosyasını düzenleyerek ve **AllowTLSV13** özelliğinin ayarını şu şekilde değiştirerek yapın:

```
SSL:
  AllowTLSV13=FALSE
```

Not: Bu ayarla, TLS 1.3 CipherSpecsolanağını kullanamazsınız.

IBM MQ MQI client ve TLS 1.3

ULW V 9.1.4

When using the IBM MQ MQI client client, the value of **AllowTLSV13** is inferred unless it is explicitly specified in the SSL stanza of the mqclient.ini file that is being used by the application.

- Herhangi bir zayıf CipherSpecs etkinleştirildiyse, **AllowTLSV13** değeri FALSE değerine ayarlıdır ve TLS 1.3 CipherSpecs kullanılamaz.
- Tersi durumda, **AllowTLSV13** değeri TRUE olarak ayarlanır ve yeni TLS 1.3 CipherSpecs ve diğer ad CipherSpecs kullanılabilir.

Default CipherSpec values enabled in IBM MQ

Multi V 9.1.1

Varsayılan yapılandırmada, IBM MQ , TLS 1.2 protokolü ve CipherSpecskullanılarak çeşitli şifreleme algoritmaları için destek sağlar. Uyumluluk açısından, IBM MQ , SSL 3.0 ve TLS 1.0 protokollerini ve güvenlik açıklarına zayıf ya da duyarlı olduğu bilinen bir dizi şifreleme algoritmasını kullanacak şekilde de yapılandırılabilir. Varsayılan yapılandırmada geçerli kılınan CipherSpecs listesi bakım uygulanarak değişebilir.

Aşağıdaki denetim öğelerini kullanarak CipherSpecs kullanımını kısıtlamak ya dapermitkullanımına izin vermek için IBM MQ ' ı yapılandırmak mümkün:

- Yalnızca SSLFIPS kullanan FIPS 140-2 uyumlu CipherSpecs izin verir.
- ULW SUITEB kullanarak yalnızca NSA Suite B uyumlu CipherSpecs izin verir.
- ULW Permit a custom list of CipherSpecs using **AllowedCipherSpecs** or the **AMQ_ALLOWED_CIPHERS** environment variable.

- ULW Permit the use of deprecated CipherSpecs using **AllowWeakCipher** or the **AMQ_SSL_WEAK_CIPHER_ENABLE** environment variable.
- z/OS CHINIT JCL ' de DD deyimleri kullanılarak kullanımdan kaldırılan CipherSpecs kullanımına izin verir.

Not: If you specify a custom list of CipherSpecs using **AllowedCipherSpecs** or **AMQ_ALLOWED_CIPHERS** this overrides enablement of any deprecated CipherSpecs. Özel bir CipherSpec listesiyle birlikte NSA Suite B ya da FIPS 140-2 sınırlamalarını kullanırken, özel listenin yalnızca Suite B ya da FIPS 140-2 ayarları tarafından izin verilen CipherSpecs değerini içerdiğinden emin olun.

Çoklu Platformlar üzerinde etkinleştirilen CipherSpecs özel bir listesini sağlama

Multi V 9.1.1

AMQ_ALLOWED_CIPHERS ortam değişkeni ya da `.ini` dosyasının **AllowedCipherSpecs** SSL stanza özniteliği kullanılarak, IBM MQ kanallarıyla birlikte kullanılmak üzere etkinleştirilen alternatif bir CipherSpecs kümesi sağlamanız mümkündür. You may wish to use this setting to restrict IBM MQ listeners from accepting incoming channel start requests, unless they use one of the named CipherSpecs. Bu işlevsellik, ANY* CipherSpecsiçinde yer alan CipherSpecs ' i (CipherSpecs) denetlemek için kullanılabilir.

AMQ_ALLOWED_CIPHERS ortam değişkeni ya da **AllowedCipherSpecs** SSL stanza özniteliği şunları kabul eder:

- Tek bir CipherSpec adı ya da
- Yeniden etkinleştirilecek IBM MQ CipherSpec adlarının virgülle ayrılmış listesi; ya da
- Tüm CipherSpecs (önerilmez) tümünü gösteren ALL' ın özel değeri.

Not: SSLSSL'un SSL 3.0 ve TLS 1.0 iletişim kurallarını ve çok sayıda zayıf şifreleme algoritmasını geçerli kılacağı için **ALL** CipherSpecs ' in etkinleştirilmesi önerilmez.

If this setting is configured, it overrides the default CipherSpec list and causes IBM MQ to ignore weak cipher deprecation settings (see below):

- IBM MQ dinleyicileri yalnızca, adı belirtilen CipherSpecs' den birini kullanan SSL/TLS önerilerini kabul eder.
- IBM MQ channels will only allow a blank SSLCIPH value, or one of the named CipherSpecs.
- **runmqsc** tab completion of SSLCIPH values restricts the completion values to one of the name CipherSpecs.

Örneğin, yalnızca kanalların tanımlanmasına/değiştirilmesine ve dinleyicilerin ECDHE_RSA_AES_128_GCM_SHA256 ya da ECDHE_ECDSA_AES_256_GCM_SHA384 kabul etmesini kabul etmek istiyorsanız, `qm.ini` dosyasında aşağıdaki bilgileri ayarlayabilirsiniz:

```
SSL:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384
```

AMQP ya da MQTT kanalları tarafından kullanılan şifrelemelerin java.security dosya ayarları kullanılarak kısıtlanabileceğini unutmayın.

Kullanımdan kaldırılan CipherSpecs on Multiplatforms özelliğinin

Multi

Varsayılan olarak, kanal tanımlarında kullanımdan kaldırılmış bir CipherSpec belirtmenize izin verilmez. If you attempt to specify a deprecated CipherSpec on Multiplatforms, you receive message AMQ8242: SSLCIPH definition wrong, and PCF returns MQRCCF_SSL_CIPHER_SPEC_ERROR.

Kullanımdan kaldırılmış bir kanalı (CipherSpec) başlatamazsınız. If you attempt to do so with a deprecated CipherSpec, the system returns `MQCC_FAILED (2)`, together with a **Reason** of `MQRC_SSL_INITIALIZATION_ERROR (2393)` to the client.

You can re-enable one or more of the deprecated CipherSpecs for defining channels, at runtime on the server, by setting the environment variable **AMQ_SSL_WEAK_CIPHER_ENABLE**.

AMQ_SSL_WEAK_CIPHER_ENABLE ortam değişkeni şunları kabul eder:

- Tek bir CipherSpec adı ya da
- Yeniden etkinleştirilecek IBM MQ CipherSpec adlarının virgülle ayrılmış listesi; ya da
- Tüm CipherSpecs (önerilmez) tümünü gösteren `ALL`' ın özel değeri.

Not: Re-enabling `TüM` CipherSpecs is not recommended, as this will enable SSL 3.0 and TLS 1.0 protocols and a large number of weak cryptographic algorithms.

Örneğin, ECDHE_RSA_RC4_128_SHA256yeniden geçerli kılınmasını istiyorsanız, aşağıdaki ortam değişkenini ayarlayın:

```
export AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RSA_RC4_128_SHA256
```

ya da yerel olarak, `qm.ini` dosyasındaki SSL stanza ayarlarını değiştirin:

```
SSL:
  AllowTLSV1=Y
  AllowWeakCipherSpec=ECDHE_RSA_RC4_128_SHA256
```

z/OSüzerinde kullanımdan kaldırılan CipherSpecs ' in etkinleştirilmesi

z/OS

Varsayılan olarak, kanal tanımlarında kullanımdan kaldırılmış bir CipherSpec belirtmenize izin verilmez. If you attempt to specify a deprecated CipherSpec on z/OS, you receive message CSQM102E or message CSQX674E.

Zayıf (kullanımdan kaldırıldı) şifreleme belirtimlerini etkinleştirmek için, CHINIT JCL ' de aşağıdaki DD deyimini tanımlamanız gerekir:

```
JCL: //CSQXWEAK DD DUMMY
```

Not: Kullanımdan kaldırılan tüm CipherSpecs , bu DD deyiminin kullanılmasını gerektirmiyor, “Kullanımdan kaldırılan CipherSpecs” sayfa 411içindeki tabloda not 11 'e bakın.

Kullanımdan kaldırılan SSL 3.0 protokolünün geçerli kılınmasını sağlamak için, CHINIT JCL ' de aşağıdaki DD deyimini de tanımlamanız gerekir:

```
JCL: //CSQXSSL3 DD DUMMY
```

V 9.1.0 Kullanımdan kaldırılan TLS 1.0 protokolünün etkinleştirilmesi için, CHINIT JCL ' de aşağıdaki DD deyimini de tanımlamanız gerekir:

```
JCL: //TLS10ON DD DUMMY
```

DD kartının adının `TLS100N`olduğunu belirtmek için, TLS 1.0 'ın açıldığını belirtmek için `TLS100N`' e dikkat edin.

TLS 1.0 ' ı kapatmak için aşağıdaki deyimi kullanın:

```
JCL: //TLS10OFF DD DUMMY
```

Zayıf ya da bozuk şifre belirtimleri kullanarak dinleyiciyle anlaşma yapmak istemiyorsanız, CHINIT JCL ' de aşağıdaki DD deyimini tanımlamanız gerekir:

```
JCL: //WCIPSOFF DD DUMMY
```

Yalnızca **System SSL** varsayılan şifre belirtimi listesinde listelenen şifre belirtimlerini kullanarak dinleyiciyle görüşmek istiyorsanız, CHINIT JCL ' de aşağıdaki DD deyimini tanımlamanız gerekir:

```
JCL: //GSKDCIPS DD DUMMY
```

En düşük düzey ve sabit seviye CipherSpecs

ULW V 9.1.4

IBM MQ supports two different types of CipherSpecs:

- **Minimum düzey** CipherSpecs , bir üst sınır ayarlamayanların (ANY, ANY_TLS12_OR_HIGHER ya da ANY_TLS13_OR_HIGHERgibi).
- **Sabit düzey** CipherSpecs , belirli bir protokolü (örneğin, ANY_TLS12 ve ANY_TLS13) ya da ECDHE_ECDSA_3DES_EDE_CBC_SHA256gibi belirli bir algoritmayı tanımlayanlardır.

Güvenliği korurken yapılandırmanın basitliğini en üst düzeye çıkarmak için, kanalın her iki tarafında da **en düşük düzey** CipherSpecs kullanılması önerilir. Bu, her iki taraf da her iki tarafın yapılanışını değiştirmeye gerek duymadan yeni bir sürümü desteklerken, iletişiminizin daha yüksek bir TLS iletişim kuralı sürümünü otomatik olarak desteklemesini ve kullanmasını sağlar.

Using a **en düşük düzey** CipherSpec on the initiating side, but a **sabit düzey** CipherSpec on the receiving side could result in the connection being rejected and messages AMQ9631 and AMQ9641 being issued.

Diğer Ad CipherSpec ayarları için farklı sonuçlar içeren tablolar için “Diğer Ad CipherSpec ayarları arasındaki ilişki” sayfa 415 ' e bakın.

İlgili kavramlar

“IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42
Bu konuda, IBM MQiçinde CipherSpecs ile dijital sertifikalar arasındaki ilişkiyi özetleyerek güvenlik ilkeniz için uygun CipherSpecs ve dijital sertifikaların nasıl seçileceğine ilişkin bilgiler sağlanır.

“CipherSpecs ve CipherSuites” sayfa 18
Şifreleme güvenlik protokolleri, güvenli bir bağlantı tarafından kullanılan algoritmalar üzerinde kabul etmelidir. CipherSpecs ve CipherSuites , algoritmaların belirli bileşimlerini tanımlar.

“IBM MQ ürününü Suite B için yapılandırma” sayfa 40
IBM MQ , Windows, UNIX and Linux platformlarında NSA Suite B standardına uygun olarak çalışacak şekilde yapılandırılabilir.

“Federal Bilgi İşleme Standartları (FIPS)” sayfa 31
Bu konuda, US National Institute of Standards and Technology 'nin Federal Bilgi İşleme Standartları (FIPS) Cryptomol Validation Programı ve TLS kanallarında kullanılabilecek şifreleme işlevleri ele alınmıştır.

İlgili görevler

Migrating existing security configurations to use the ANY_TLS12_OR_HIGHER CipherSpec

İlgili başvurular

KANAL TANIMLA

KANALı ALTER

Kanal Oluştur, Kopyala ve Oluştur

ULW AES-GCM şifre kısıtlaması

TLS Şifreleme için kullanıldığında AES-GCM şifrelemelerine uygulanan kısıtlamalara ilişkin bir kılavuz. Bu kısıtlamalar IETF ve NIST kuruluşları tarafından uygulanır ve AES-GCM şifrelemeleri kullanılırken aynı oturum anahtarının 2 'den fazla$^{24.5}$ TLS kaydını güvenli bir şekilde aktarmak için kullanılmamasını gerektirir.

Bu kısıtlamalarla ilgili daha fazla bilgi için bkz. RFC 9325 Section 4.4 Limits on Key Usage ve RFC 8446 section 5.5.

IBM MQ , doğrudan şifreleme işlevselliğini uygulamaz. Bunun yerine, TLS ve Advanced Message Security işlevselliğini sağlamak için birkaç farklı şifreleme kitaplığı kullanılır. Windows, Linuxve AIX işletim sistemlerinde, IBM MQ 'in kullandığı şifreleme kitaplığı GSKit' dir. Uygulamalar için, C ve yönetilmeyen .NET kitaplıkları şifreleme işlevi için GSKit kullanır. AES-GCM şifreleme algoritmalarının GSKit tarafından uygulanması, standartlar grubu tarafından belirtilen kısıtlamaları içerir. Ayrıca, bu kısıtlamalar varsayılan olarak etkinleştirilir. Bu nedenle IBM MQ TLS iletişimi, AES-GCM şifrelerini kullanırken, aynı oturum anahtarı kullanılarak 2 'den fazla$^{24.5}$ TLS kaydı iletildiğinde sona erer.

Not: Farklı şifreleme kitaplıkları kullanıldığından ve bu kitaplıklar aynı kısıtlamayı uygulamadığından, IBM i, IBM Z ya da IBM MQ for HPE NonStop platformları ya da Java/JMS, yönetilen .NET uygulamalarda bu kısıtlama yoktur.

Bir IBM MQ kanalı, 2 'den fazla$^{24.5}$ TLS kaydı aynı oturum anahtarı kullanılarak iletilecek kadar uzun süre çalışır durumda kalırsa, temeldeki şifreleme kitaplığı bağlantıyı sonlandırır. Bu, kanalın sonlandırılmasına ve bir AMQ9288E hata iletisinin oluşturulmasına neden olur. İletişimi bu şekilde sonlandırılan uygulamalar, gerçekleştirilmekte olan IBM MQ işleminden bir `MQRC_CONNECTION_BROKEN` dönüş kodu alır.

Bağlantının sonlandırılması iletişimin her iki ucunda da gerçekleştirilebilir, ancak yalnızca şifreleme işlevi için GSKit kullanan uçlarda gerçekleştirilebilir.

Kısıtlamanın hafifletilmesine ilişkin öneriler

Bu sınırlama nedeniyle sonlandırılan iletişimin nasıl önleneceğine ya da işleneceğine ilişkin bazı seçenekler şunlardır:

Yeniden bağlanabilir istemcileri kullan

Bir bağlantı başarısız olursa, uygulamaların konfigürasyonu otomatik olarak yeniden bağlanma girişiminde bulunacak şekilde tanımlanabilir. Bu, GCM kısıtlaması nedeniyle sonlandırılan bağlantıları içerir. Yeniden bağlantı için yapılandırıldığında, istemci uygulaması herhangi bir hata noktasında otomatik olarak geri yüklenir ve nesneleri açma tanıtıcıları geri yüklenir. Bu, uygulama koduna geri dönülmeden yapılır.

Daha fazla bilgi için bkz. Otomatik istemci yeniden bağlantısı.

Gizli anahtar sıfırlama değeri ayarla

IBM MQ , bir kanal üzerinden yapılandırılabilir bayt sayısı aktarıldıktan sonra oturum anahtarını ilk durumuna getirme isteğinde bulunacak şekilde yapılandırılabilir. Bu sınıra ulaştıktan sonra IBM MQ , şifreleme katmanının oturum anahtarını ilk durumuna getirmesini ister ve yeni bir oturum anahtarıyla sonuçlanır.

Belirtilen değerin, IBM MQtarafından gönderilen iletilerin boyutuyla ilgili olarak aktarılan bayt sayısı olduğunu unutmayın. Kısıtlama, gönderilen TLS kaydı sayısı üzerindedir. TLS kaydı, ağın İletim Birimi Üst Sınırı 'na (MTU) bağlı bayt sayısı üst sınırını gönderebileceği için, ileti baytları ile TLS kayıtları arasında doğrudan eşleme yoktur. Bu değerden büyük olan iletiler birden çok TLS kaydı olarak iletilir. MTU değeri ağlar arasında değişir. Ayrıca, TLS kaydının IBM MQ ileti verilerini iletme dışında gönderilmesi gerekmesinin başka nedenleri de vardır; örneğin, IBM MQ Heartbeat denetimleri, TLS uyarıları, diğer IBM MQ iletişim kuralı iletileri. Bu ek TLS kayıtları, TLS kaydı sayısı üst sınırına doğru sayılır, ancak IBM MQ gizli anahtar sıfırlama değerinde sayılmaz.

Gizli anahtar sıfırlaması kullanılarak bir oturum anahtarının düzenli olarak sıfırlanması, AES-GCM kısıtlaması nedeniyle kanalın sonlandırılmasını önleyebilir.

Daha fazla bilgi için SSL ve TLS gizli anahtarlarını sıfırlamabaşlıklı konuya bakın.

V 9.1.4 **TLS 1.3 şifreleme belirtimlerini kullan**

TLS 1.3 iletişim kuralı kullanılırken AES-GCM kısıtlaması hala varken TLS 1.3 iletişim kuralı, TLS iletişimini kesme gereksinimi olmadan otomatik olarak bir oturum anahtarı sıfırlama işleminin gerçekleştirilmesini destekler. Bu, GSKit 'in gerektiğinde oturum anahtarını sıfırlamayı, IBM MQ ' un gizli anahtar sıfırlaması istemesine gerek kalmadan yönetmesini sağlar.

Daha fazla bilgi için bkz. “CipherSpecs' in etkinleştirilmesi” sayfa 402içinde IBM MQ içinde TLS 1.3 kullanma .

AES-GCM kısıtlamasını devre dışı bırak

Gerekirse, **GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE** ortam değişkeni AES-GCM kısıtlamasını devre dışı bırakacak şekilde ayarlanarak kısıtlama devre dışı bırakılabilir. Bunu yapmak, aynı oturum anahtarı kullanılarak herhangi bir sayıda TLS kaydının gönderilmesine olanak sağlar. Bu azaltma seçiliyorsa, ortam değişkeni, güvenli iletişim için GSKit kullanan iletişimin her bir ucunda ayarlanmalıdır.

Uyarı: Bu seçenek, 2 'den fazla$^{24.5}$ TLS kaydı gönderildikten sonra, saldırganların kullanılmakta olan oturum anahtarını belirlemek için gönderilen kayıtlar üzerinde analiz gerçekleştirmeleri mümkün olduğu için önerilmez. Oturum anahtarı belirlendikten sonra, bu oturum anahtarını kullanarak var olan ve gelecekteki tüm iletişim tehlikeye atılır.

Kullanımdan kaldırılan CipherSpecs

A list of deprecated CipherSpecs that you are able to use with IBM MQ if necessary.

Kullanımdan kaldırılan CipherSpecs' nin etkinleştirilmesiyle ilgili bilgi için bkz. “Kullanımdan kaldırılan CipherSpecs on Multiplatforms özelliğinin” sayfa 407 ya da “z/OSüzerinde kullanımdan kaldırılan CipherSpecs ' in etkinleştirilmesi” sayfa 408.

IBM MQ TLS desteği ile kullanabileceğiniz, kullanımdan kaldırılan CipherSpecs komutu aşağıdaki tabloda listelenir.

Çizelge 75. IBM MQ ile kullanmak üzere yeniden etkinleştirebileceğiniz kullanımdan kaldırılmış CipherSpecs

Platform desteği “1” sayfa 414	CipherSpec adı	Onaltılı kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS “2” sayfa 414	Takım B	Kullanımdan kaldırıldığında güncelle
CipherSpecs for SSL 3.0								
IBM i	AES_SHA_US “3” sayfa 414	002F	SSL 3.0	SHA-1	AES (128)	Hayır	Hayır	9.0.0.0
Tümü	DES_SHA_EXPORT “3” sayfa 414 “4” sayfa 414 “5” sayfa 414	0009	SSL 3.0	SHA-1	DES (56)	Hayır	Hayır	9.0.0.0
ULW	DES_SHA_EXPORT1024 “3” sayfa 414 “6” sayfa 414	0062	SSL 3.0	SHA-1	DES (56)	Hayır	Hayır	9.0.0.0
ULW	FIPS_WITH_DES_CBC_SHA “3” sayfa 414	FEFE	SSL 3.0	SHA-1	DES (56)	Hayır “7” sayfa 414	Hayır	9.0.0.0
ULW	FIPS_WITH_3DES_EDE_CBC_SHA “3” sayfa 414	FEFF	SSL 3.0	SHA-1	3DES (168)	Hayır “8” sayfa 414	Hayır	9.0.0.1 ve 9.0.1
Tümü	NULL_MD5 “3” sayfa 414	0001	SSL 3.0	MD5	Yok	Hayır	Hayır	9.0.0.1
Tümü	NULL_SHA “3” sayfa 414	0002	SSL 3.0	SHA-1	Yok	Hayır	Hayır	9.0.0.1
Tümü	RC2_MD5_EXPORT “3” sayfa 414 “4” sayfa 414 “5” sayfa 414	0006	SSL 3.0	MD5	RC2 (40)	Hayır	Hayır	9.0.0.0
Tümü	RC4_MD5_EXPORT “4” sayfa 414 “3” sayfa 414	0003	SSL 3.0	MD5	RC4 (40)	Hayır	Hayır	9.0.0.0

Çizelge 75. IBM MQ ile kullanmak üzere yeniden etkinleştirebileceğiniz kullanımdan kaldırılmış CipherSpecs (devamı var)

Platform desteği "1" sayfa 414	CipherSpec adı	Onaltılı kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS "2" sayfa 414	Takım B	Kullanımdan kaldırıldığında güncelle
Tümü	RC4_MD5_US "3" sayfa 414	0004	SSL 3.0	MD5	RC4 (128)	Hayır	Hayır	9.0.0.0
Tümü	RC4_SHA_US "3" sayfa 414 "5" sayfa 414	0005	SSL 3.0	SHA-1	RC4 (128)	Hayır	Hayır	9.0.0.0
ULW	RC4_56_SHA_EXPORT1024 "3" sayfa 414 "6" sayfa 414	0064	SSL 3.0	SHA-1	RC4 (56)	Hayır	Hayır	9.0.0.0
Tümü	TRIPLE_DES_SHA_US "3" sayfa 414 "5" sayfa 414	000A	SSL 3.0	SHA-1	3DES (168)	Hayır	Hayır	9.0.0.1 ve 9.0.1
CipherSpecs for TLS 1.0								
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5 "3" sayfa 414	0006	TLS 1.0	MD5	RC2 (40)	Hayır	Hayır	9.0.0.0
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5 "3" sayfa 414 "4" sayfa 414	0003	TLS 1.0	MD5	RC4 (40)	Hayır	Hayır	9.0.0.0
Tümü	TLS_RSA_WITH_DES_CBC_SHA "3" sayfa 414	0009	TLS 1.0	SHA-1	DES (56)	Hayır "9" sayfa 414	Hayır	9.0.0.0
IBM i	TLS_RSA_WITH_NULL_MD5 "3" sayfa 414	0001	TLS 1.0	MD5	Yok	Hayır	Hayır	9.0.0.1
IBM i	TLS_RSA_WITH_NULL_SHA "3" sayfa 414	0002	TLS 1.0	SHA-1	Yok	Hayır	Hayır	9.0.0.1
IBM i	TLS_RSA_WITH_RC4_128_MD5 "3" sayfa 414	0004	TLS 1.0	MD5	RC4 (128)	Hayır	Hayır	9.0.0.0
z/OS ULW	TLS_RSA_WITH_AES_128_CBC_SHA "10" sayfa 414	002F	TLS 1.0	SHA-1	AES (128)	Evet	Hayır	9.0.5
z/OS ULW	TLS_RSA_WITH_AES_256_CBC_SHA "6" sayfa 414 "10" sayfa 414	0035	TLS 1.0	SHA-1	AES (256)	Evet	Hayır	9.0.5
Tümü	TLS_RSA_WITH_3DES_EDE_CBC_SHA	000A	TLS 1.0	SHA-1	3DES (168)	Evet	Hayır	9.0.0.1 ve 9.0.1
CipherSpecs for TLS 1.2								
ULW	ECDHE_ECDSA_NULL_SHA256 "3" sayfa 414	C006	TLS 1.2	SHA-1	Yok	Hayır	Hayır	9.0.0.1
ULW	ECDHE_ECDSA_RC4_128_SHA256 "3" sayfa 414	C007	TLS 1.2	SHA-1	RC4 (128)	Hayır	Hayır	9.0.0.0

Çizelge 75. IBM MQ ile kullanmak üzere yeniden etkinleştirebileceğiniz kullanımdan kaldırılmış CipherSpecs (devamı var)

Platform desteği "1" sayfa 414	CipherSpec adı	Onaltılı kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS "2" sayfa 414	Takım B	Kullanımdan kaldırıldığında güncelle
IBM i ULW	ECDHE_RSA_NULL_SHA256 "3" sayfa 414	C010	TLS 1.2	SHA-1	Yok	Hayır	Hayır	9.0.0.1
IBM i ULW	ECDHE_RSA_RC4_128_SHA256 "3" sayfa 414	C011	TLS 1.2	SHA-1	RC4 (128)	Hayır	Hayır	9.0.0.0
ULW	TLS_RSA_WITH_NULL_NULL "3" sayfa 414	0000	TLS 1.2	Yok	Yok	Hayır	Hayır	9.0.0.1
Tümü	TLS_RSA_WITH_NULL_SHA256 "3" sayfa 414	003B	TLS 1.2	SHA-256	Yok	Hayır	Hayır	9.0.0.1
ULW	TLS_RSA_WITH_RC4_128_SHA256 "3" sayfa 414	0005	TLS 1.2	SHA-1	RC4 (128)	Hayır	Hayır	9.0.0.0
ULW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	C0008	TLS 1.2	SHA-1	3DES (168)	Evet	Hayır	9.0.0.1 ve 9.0.1
IBM i ULW	ECDHE_RSA_3DES_EDE_CBC_SHA256	C012	TLS 1.2	SHA-1	3DES (168)	Evet	Hayır	9.0.0.1 ve 9.0.1

Çizelge 75. IBM MQ ile kullanmak üzere yeniden etkinleştirebileceğiniz kullanımdan kaldırılmış CipherSpecs (devamı var)

Platform desteği "1" sayfa 414	CipherSpec adı	Onaltılı kod	Kullanılan protokol	Veri bütünlüğü	Şifreleme algoritması (şifreleme bitleri)	FIPS "2" sayfa 414	Takım B	Kullanımdan kaldırıldığında güncelle

Notlar:

1. Her platform simgesinin kapsadığı platformların bir listesi için ürün belgelerinde Yayın ve platform simgeleribaşlıklı konuya bakın.
2. CipherSpec ' in FIPS onaylı bir platformda FIPS onaylı olup olmadığını belirtir. FIPS ' ye ilişkin açıklamalar için bkz. Federal Information Processing Standards (FIPS) .
3. ULW Bu CipherSpecs , TLS 1.3 etkinleştirildiğinde (`qm.ini`içindeki AllowTLSV13 özelliği aracılığıyla) devre dışı bırakılır.

   z/OS IBM MQ for z/OS 9.2.0 ya da daha sonraki bir sürümde oluşturulan kuyruk yöneticileri varsayılan olarak TLS 1.3 'u etkinleştirerek bu CipherSpecs' i devre dışı bırakır. Gerekirse, TLS V1.3'i kapatarak bu CipherSpecs' i etkinleştirebilirsiniz. Bu, kuyruk yöneticisi JCL ' deki QMINI veri kümesinin TransportSecurity kısmına **AllowTLSV13**=*FALSE* eklenerek yapılır. Daha önceki bir sürümden IBM MQ for z/OS 9.2.0 ' a geçirilen kuyruk yöneticilerinin varsayılan olarak TLS 1.3 etkinleştirilmez ve bu nedenle bu CipherSpecs etkinleştirilir.
4. El sıkışma anahtarı büyüklüğü üst sınırı 512 bittir. SSL el sıkışması sırasında değiş tokuş edilen sertifikalardan birinin anahtar boyutu 512 bitten fazlaysa, el sıkışması sırasında kullanılmak üzere geçici bir 512 bitlik anahtar oluşturulur.
5. Bu CipherSpecs artık IBM MQ classes for Java ya da IBM MQ classes for JMStarafından desteklenmez. Daha fazla bilgi için bkz. IBM MQ classes for Java içinde SSL/TLS CipherSpecs ve CipherSuites ya da IBM MQ classes for JMS içinde SSL/TLS CipherSpecs ve CipherSuites.
6. Tokalaşma anahtarı boyutu 1024 bittir.
7. Bu CipherSpec , 19 Mayıs 2007 'den önce FIPS 140-2 sertifikalıydı. `FIPS_WITH_DES_CBC_SHA` adı geçmiştir ve bu CipherSpec ' in önceden (ancak artık) FIPS uyumlu olmadığı gerçeğini yansıtır. Bu CipherSpec kullanımdan kaldırılmıştır ve kullanılması önerilmez.
8. `FIPS_WITH_3DES_EDE_CBC_SHA` adı geçmiştir ve bu CipherSpec ' in önceden (ancak artık) FIPS uyumlu olmadığı gerçeğini yansıtır. Bu CipherSpec kullanımı kullanımdan kaldırılmıştır.
9. Bu CipherSpec , 19 Mayıs 2007 'den önce FIPS 140-2 sertifikalıydı.
10. z/OS Yalnızca bu CipherSpecs ' in yeniden etkinleştirilmesi, CSQXWEAK DD deyiminin kullanılmasını gerektirmez.

İlgili kavramlar

"IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu" sayfa 42

Bu konuda, IBM MQiçinde CipherSpecs ile dijital sertifikalar arasındaki ilişkiyi özetleyerek güvenlik ilkeniz için uygun CipherSpecs ve dijital sertifikaların nasıl seçileceğine ilişkin bilgiler sağlanır.

İlgili başvurular

KANAL TANIMLA

KANALı ALTER

Diğer Ad CipherSpec ayarları arasındaki ilişki

Aşağıdaki çizelgeler, istemcide, kuyruk yöneticisinde ya da her ikisinde TLS1.3 etkinleştirilmediğinde ve hem istemcide hem de kuyruk yöneticisinde TLS1.3 etkinleştirildiğinde beklenen davranışı gösterir.

Aşağıdaki çizelgelerde, farklı Diğer Ad CipherSpec ayarları ile beklenen sonuç arasındaki ilişki gösterilir. Çizelge 76 sayfa 415 , TLS 1.3 istemci, sunucu ya da her ikisinde de etkinleştirilmediğinde beklenen davranışı gösterir. Çizelge 77 sayfa 415 , hem istemcide hem de sunucuda TLS 1.3 etkinleştirildiğinde beklenen davranışı gösterir. Her iki durumda da, istemciye ilişkin CipherSpecs çizelgenin Y ekseninde gösterilir ve sunucunun CipherSpecs değeri çizelgenin X ekseninde gösterilir.

Not: Girdinin *Başarısız olma durumu* belirtmesinin nedeni, belirli TLS 1.3 ya da TLS 1.2 CipherSpec ' in istemci ve kuyruk yöneticisi için en güçlü CipherSpec olması durumunda, TLS el sıkışması bunu kullanmaya çözülür ve kanal SSCIPH değeriyle eşleşir.

Çizelge 76. İstemcide, sunucuda ya da her ikisinde TLS 1.3 etkinleştirilmediğinde beklenen davranış

	Sunucu			
Müşteri	**Belirli TLS 1.2 CipherSpec**	**Fark Etmez**	**ANY_ TLS12**	**ANY_TLS12_ YA DA DAHA YüKSEK**
Belirli TLS 1.2 CipherSpec	Bağlanmalar	Bağlanmalar	Bağlanmalar	Bağlanmalar
Fark Etmez	*Başarısız olma olasılığı*	Bağlanmalar	Bağlanmalar	Bağlanmalar
ANY_ TLS12	*Başarısız olma olasılığı*	Bağlanmalar	Bağlanmalar	Bağlanmalar
ANY_TLS12_ YA DA DAHA YüKSEK	*Başarısız olma olasılığı*	Bağlanmalar	Bağlanmalar	Bağlanmalar

Çizelge 77. İstemcide ve sunucuda TLS 1.3 etkinleştirildiğinde beklenen davranış

	Sunucu						
Müşteri	**Belirli TLS 1.2 CipherSpec**	**Belirli TLS 1.3 CipherSpec**	**Fark Etmez**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_YüKSEK**	**ANY_TLS13_ OR_YüKSEK**
Belirli TLS 1.2 CipherSpec	Bağlanmalar	**Başarısız**	Bağlanmalar	Bağlanmalar	**Başarısız**	Bağlanmalar	**Başarısız**
Belirli TLS 1.3 CipherSpec	**Başarısız**	Bağlanmalar	Bağlanmalar	**Başarısız**	Bağlanmalar	Bağlanmalar	Bağlanmalar
Fark Etmez	**Başarısız**	*Başarısız olma olasılığı*	Bağlanmalar	**Başarısız**	Bağlanmalar	Bağlanmalar	Bağlanmalar
ANY_TLS12	*Başarısız olma olasılığı*	**Başarısız**	Bağlanmalar	Bağlanmalar	**Başarısız**	Bağlanmalar	**Başarısız**
ANY_TLS13	**Başarısız**	*Başarısız olma olasılığı*	Bağlanmalar	**Başarısız**	Bağlanmalar	Bağlanmalar	Bağlanmalar
ANY_TLS12_ OR_üST	**Başarısız**	*Başarısız olma olasılığı*	Bağlanmalar	**Başarısız**	Bağlanmalar	Bağlanmalar	Bağlanmalar

Çizelge 77. İstemcide ve sunucuda TLS 1.3 etkinleştirildiğinde beklenen davranış (devamı var)							
	Sunucu						
Müşteri	**Belirli TLS 1.2 CipherSpec**	**Belirli TLS 1.3 CipherSpec**	**Fark Etmez**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_YüKSEK**	**ANY_TLS13_ OR_YüKSEK**
ANY_TLS13_ OR_üST	**Başarısız**	*Başarısız olma olasılığı*	Bağlanmalar	**Başarısız**	Bağlanmalar	Bağlanmalar	Bağlanmalar

İlgili kavramlar

"IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu" sayfa 42
Bu konuda, IBM MQiçinde CipherSpecs ile dijital sertifikalar arasındaki ilişkiyi özetleyerek güvenlik ilkeniz için uygun CipherSpecs ve dijital sertifikaların nasıl seçileceğine ilişkin bilgiler sağlanır.

"CipherSpecs ve CipherSuites" sayfa 18
Şifreleme güvenlik protokolleri, güvenli bir bağlantı tarafından kullanılan algoritmalar üzerinde kabul etmelidir. CipherSpecs ve CipherSuites , algoritmaların belirli bileşimlerini tanımlar.

"CipherSpecs' in etkinleştirilmesi" sayfa 402
Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

İlgili görevler

Var olan güvenlik yapılandırmalarının ANY_TLS12_OR_HIGHER CipherSpec ' i kullanacak şekilde geçirilmesi

IBM MQ Explorerkullanılarak CipherSpecs hakkında bilgi edinilmesi

CipherSpecs'in açıklamalarını görüntülemek için IBM MQ Explorer ' u kullanabilirsiniz.

"CipherSpecs' in etkinleştirilmesi" sayfa 402içindeki CipherSpecs ile ilgili bilgi edinmek için aşağıdaki yordamı kullanın:

1. IBM MQ Explorer dosyasını açın ve **Kuyruk Yöneticileri** klasörünü genişletin.
2. Kuyruk yöneticinizi başlattığınızdan emin olun.
3. Çalışmak istediğiniz kuyruk yöneticisini seçin ve **Kanallar**' ı tıklatın.
4. Üzerinde çalışmak istediğiniz kanalı farenin sağ düğmesiyle tıklatın ve **Özellikler**seçeneğini belirleyin.
5. **SSL** özellik sayfasını seçin.
6. Çalışmak istediğiniz CipherSpec listeden seçim yapın. Listenin altındaki pencerede bir açıklama görüntülenir.

CipherSpecsbelirtme alternatifleri

İşletim sisteminin TLS desteğini sağladığı platformlarda, sisteminiz yeni CipherSpecs' ı (CipherSpecs) destekleyebilir. SSLCIPH parametresiyle yeni bir CipherSpec belirtebilirsiniz, ancak sağladığınız değer platformunuza bağlıdır.

Not: This section does not apply to UNIX, Linux or Windows systems, because the CipherSpecs are provided with the IBM MQ product, so new CipherSpecs do not become available after shipment.

İşletim sisteminin TLS desteğini sağladığı platformlar için sisteminiz, "CipherSpecs' in etkinleştirilmesi" sayfa 402içinde bulunmayan yeni CipherSpecs ' ı destekleyebilir. SSLCIPH parametresiyle yeni bir CipherSpec belirtebilirsiniz, ancak sağladığınız değer platformunuza bağlıdır. Tüm durumlarda, belirtimin hem geçerli hem de sistemin TLS sürümü tarafından desteklenen bir TLS CipherSpec ' e karşılık gelmesi gerekir.

IBM i
Onaltılı bir değeri gösteren iki karakterlik bir dizilim.

İzin verilen değerler hakkında daha fazla bilgi için, Güvenli bir oturum için karakter bilgileri ayarla' nın Kullanım Notları bölümündeki üç nokta yer alın.

Uyarı: SSLCIPH ' de onaltılı şifreleme değerleri belirtmemelisiniz; bu, şifrelemeyi hangi değerin kullanılacağı belirsiz olduğundan ve kullanılacak protokolün seçimi belirsiz. Onaltılı şifreleme değerlerinin kullanılması CipherSpec yanlış eşleşme hatalarına yol açabilir.

Değeri belirtmek için CHGMQMCHL ya da CRTMQMCHL komutunu kullanabilirsiniz; örneğin:

```
CRTMQMCHL CHLNAME(' channel name ') SSLCIPH(' hexadecimal value ')
```

You can also use the ALTER QMGR MQSC command to set the **SSLCIPH** parameter.

z/OS
Onaltılı bir değeri gösteren dört karakterlik bir dizilim. Onaltılı kodlar, TLS iletişim kuralı içinde tanımlanan değerlere karşılık gelir.

Daha fazla bilgi için, desteklenen tüm TLS 1.0, TLS 1.2ve TLS 1.3 şifre belirtimlerinin, 4 basamaklı onaltılı kodlar biçiminde bir listesi olduğu Cipher Suite Tanımları konusuna bakın.

IBM MQ kümeleri için dikkat edilecek noktalar

IBM MQ kümesiyle birlikte, “CipherSpecs' in etkinleştirilmesi” sayfa 402içinde CipherSpec adlarının kullanılması en güvenli olur. Alternatif bir belirtim kullanırsanız, belirtimin diğer platformlarda geçerli olmayabileceğini göz üstüne Edin. Daha fazla bilgi için bkz. “SSL/TLS ve kümeler” sayfa 444.

IBM MQ MQI clientiçin bir CipherSpec belirtme

IBM MQ MQI clientiçin bir CipherSpec belirtmek için üç seçeneğiniz vardır.

Bu seçenekler şunlardır:

- Kanal tanımlama çizelgesinin kullanılması
- Using the SSLCipherSpec field in the MQCD structure, at MQCD_VERSION_7 or higher, on an MQCONNX call.
- Active Directory (Active Directory desteğiyle Windows sistemlerinde) kullanılması

IBM MQ classes for Java ve IBM MQ classes for JMSile bir CipherSuite belirtilmesi

IBM MQ classes for Java ve IBM MQ classes for JMS , diğer altyapılardan farklı CipherSuites öğesini belirtir.

IBM MQ classes for Javaile bir CipherSuite belirtilmesine ilişkin bilgi edinmek için bkz. Transport Layer Security (TLS) support for Java

IBM MQ classes for JMSile bir CipherSuite belirtilmesine ilişkin bilgi edinmek için bkz. Using Transport Layer Security (TLS) with IBM MQ classes for JMS

IBM MQ.NETiçin bir CipherSpec belirtme

IBM MQ.NET için, MQEnvironment sınıfını kullanarak ya da bağlantı özelliklerinin HASH çizelgesinde MQC.SSL_CIPHER_SPEC_PROPERTY kullanarak CipherSpec belirtilebilir.

For information about specifying a CipherSpec for the .NET unmanaged client, see Yönetilmeyen .NET istemcisi için TLS ' nin etkinleştirilmesi

For information about specifying a CipherSpec for the .NET managed client, see Yönetilen .NET istemcisi içinCipherSpec desteği

z/OS Use of AT-TLS with IBM MQ for z/OS

Uygulama Şeffaf Taşıma Katmanı Güvenliği (AT-TLS), TLS desteğini uygulamak zorunda kalmadan z/OS uygulamaları için TLS desteği sağlar ya da TLS ' nin kullanılmakta olduğunun farkında bile olur. AT-TLS, yalnızca z/OSüzerinde kullanılabilir.

AT-TLS, IBM MQ for z/OStüm sürümleriyle kullanılabilir.

Before making use of AT-TLS with IBM MQ for z/OS, make sure you understand the “Kısıtlamalar” sayfa 420 involved.

Uygulama Saydam Aktarım Katmanı Güvenliğini kullanmak için, z/OS Communications Server tarafından hangi TCP/IP bağlantısının TLS saydam olarak etkinleştirileceğine karar vermek için kullanılan bir kural kümesi içeren ilke deyimleri tanımlırsınız.

IBM MQ for z/OS has its own TLS implementation, which requires that channels have the SSLCIPH parameter configured with a supported CipherSpec.

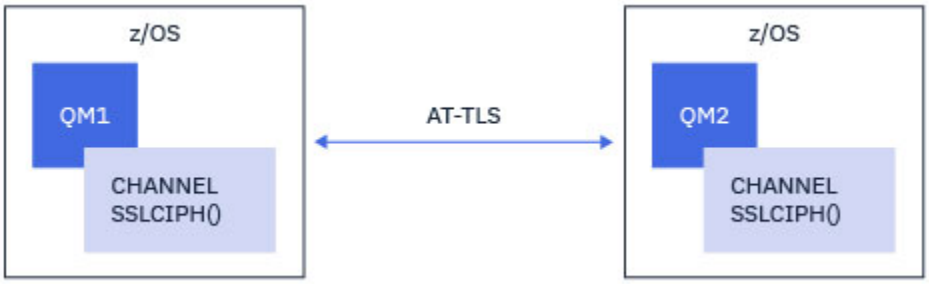
Bir kanalda TLS 'yi etkinleştirmeye karar verilirken, IBM MQ yöneticisi AT-TLS ya da IBM MQ TLS' yi kullanmaya karar verebilir. Karar genellikle, AT-TLS ' nin diğer ara katman yazılımları için mi, yoksa performans etkileri nedeniyle mi temel alınarak yapılır. At-TLS ve IBM MQ TLS performansının temel bir karşılaştırması için bkz. MP16: Capacity Planning and Tuning for IBM MQ for z/OS.

Senaryolar

Aşağıdaki senaryolarda, AT-TLS ' nin IBM MQ ile kullanılması desteklenir:

1. senaryo

Kanalların her iki tarafından AT-TLS kullandığı iki IBM MQ for z/OS kuyruk yöneticisi arasında. Diğer bir seçenek de, hiçbir kanalda SSLCIPH özniteliğini belirtmez. Bu yaklaşım, herhangi bir ileti kanalıyla kullanılabilir.

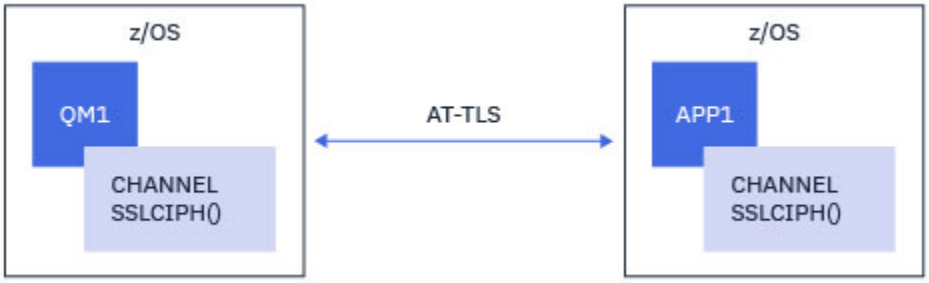


Bu senaryonun uygulanması, kanalın her bir tarafı için bir adet olmak üzere iki AT-TLS ilkesi tanımlanmaktan oluşur. Bu ilkeler, Senaryo 3ile kullanılanlarla aynıdır.

For example, if the channel was being changed from using a single, named CipherSpec to using AT-TLS, the outbound channel would use the policy from “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak giden kanalda AT-TLS ' nin IBM MQ for Multiplatforms kuyruk yöneticisine yapılandırılması” sayfa 421 and the inbound channel would use the policy from “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak IBM MQ for Multiplatforms kuyruk yöneticisinden gelen kanalda AT-TLS ' nin yapılandırılması” sayfa 424.

2. senaryo

Between an IBM MQ for z/OS queue manager and an IBM MQ Java client application running on z/OS where both sides of the channel use AT-TLS. Yani, ne sunucu-bağlantı kanalı, ne de istemci-bağlantı kanalı SSLCIPH özniteliğini belirtmez.

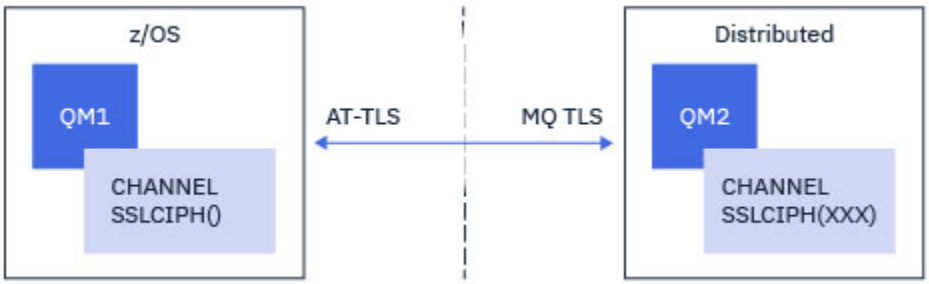


Bu senaryonun uygulanması, kanalın her bir tarafı için bir adet olmak üzere iki AT-TLS ilkesi tanımlanmaktan oluşur. Bu ilkeler, Senaryo 3ile kullanılanlarla aynıdır.

For example, if the channel was being changed from using a single, named CipherSpec to using AT-TLS the client-connection channel would use the policy from “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak giden kanalda AT-TLS ' nin IBM MQ for Multiplatforms kuyruk yöneticisine yapılandırılması” sayfa 421 and the server-connection channel would use the policy from “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak IBM MQ for Multiplatforms kuyruk yöneticisinden gelen kanalda AT-TLS ' nin yapılandırılması” sayfa 424.

3. senaryo

Between an IBM MQ for z/OS queue manager and a queue manager running on IBM MQ for Multiplatforms, where the IBM MQ for z/OS queue manager uses AT-TLS and the IBM MQ for Multiplatforms queue manager uses IBM MQ TLS. Bu, küme-gönderici ve küme-alıcı dışındaki tüm ileti kanalı tipleri için geçerlidir.

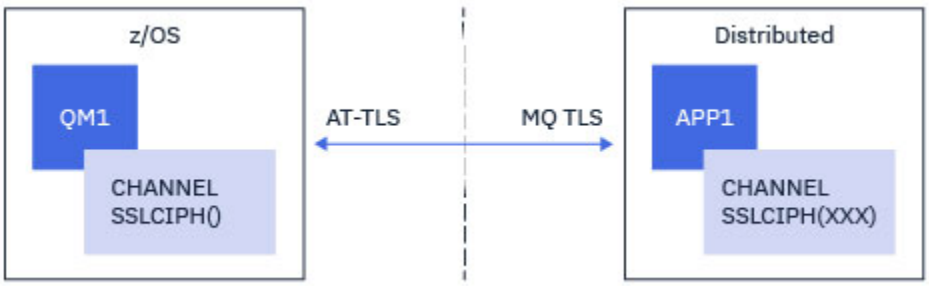


See “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak giden kanalda AT-TLS ' nin IBM MQ for Multiplatforms kuyruk yöneticisine yapılandırılması” sayfa 421 for an example AT-TLS configuration for outbound channels from the IBM MQ for z/OS queue manager to the IBM MQ for Multiplatforms queue manager, and “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak IBM MQ for Multiplatforms kuyruk yöneticisinden gelen kanalda AT-TLS ' nin yapılandırılması” sayfa 424 for an example AT-TLS configuration for inbound channels from the IBM MQ for Multiplatforms queue manager to the IBM MQ for z/OS queue manager.

Aynı AT-TLS yapılandırması, hem kuyruk yöneticisi z/OS' de olduğunda, ancak sağ taraftaki kuyruk yöneticisi AT-TLS kullanacak şekilde yapılandırılmadığında da kullanılabilir.

4. senaryo

IBM MQ for Multiplatforms' ta çalışan bir IBM MQ for z/OS kuyruk yöneticisi ve istemci uygulaması arasında, burada IBM MQ for z/OS kuyruk yöneticisi AT-TLS kullanır ve istemci uygulaması, SSLCIPH özniteliğini tek bir CipherSpecolarak belirterek IBM MQ TLS kullanır.



Bu senaryo, bir gelen ileti kanalı tarafından kullanılanlarla aynı gereksinimleri karşılayan tek bir AT-TLS ilkesi gerektirir; bkz. “CipherSpec adlı tek bir kuyruk yöneticisini kullanarak IBM MQ for Multiplatforms kuyruk yöneticisinden gelen kanalda AT-TLS ' nin yapılandırılması” sayfa 424.

Aynı AT-TLS yapılandırması, istemci uygulaması bir Java uygulaması olduğunda ve z/OSüzerinde çalışırken kullanılabilir, ancak AT-TLS kullanacak şekilde yapılandırılmamıştır.

Kısıtlamalar

IBM MQ for z/OS , AT-TLS ' ye duyarlı değildir; bu nedenle, önceki senaryolarla geçerli olan birkaç kısıtlama vardır:

- IBM MQ TLS ile birlikte AT-TLS, küme gönderici ve kümeli alıcı kanallarıyla çalışmaz.
- IBM MQ for z/OS kuyruk yöneticileri, AT-TLS kullandıklarını ve iş ortağı kuyruk yöneticisinden ya da istemcisinden herhangi bir sertifika bilgisi almadıklarını dikkate almaz. Bu nedenle, aşağıdaki özniteliklerin AT-TLS kullanan bir kanalda z/OS tarafında hiçbir etkisi yoktur:
  - SSLCAUTH ve SSLPEER kanal öznitelikleri
  - SSLRKEYC kuyruk yöneticisi özniteliği
  - CHLAUTH kurallarına ilişkin SSLPEERMAP öznitelikleri
- TLS gizli anahtarının yeniden görüşmesinin kullanılması, kanaldaki her iki tarafın da IBM MQ TLS ' yi kullanmasını gerektirir. Bu nedenle, bir IBM MQ for Multiplatforms kuyruk yöneticisi ya da istemcisi, AT-TLS kullanılarak bir IBM MQ for z/OS kuyruk yöneticisine bağlanıyorsa TLS gizli anahtarı yeniden görüşme etkinleştirilmemelidir.

  Bir kuyruk yöneticisi için TLS gizli anahtarını yeniden görüşme işlemini devre dışı bırakmak için, kuyruk yöneticisi SSLRKEYC değiştirgesini 0olarak ayarlayın. Bir istemci için, istemci tipine bağlı olarak, ilgili parametreyi 0 olarak ayarlayın. Bunun nasıl yapacağına ilişkin ayrıntılı bilgi için bkz. “SSL ve TLS gizli anahtarlarını sıfırlama” sayfa 428.

At-TLS yapılandırma deyimleri

At-TLS, bir deyim kümesi kullanılarak yapılandırılır. Bu konuda belgelenen senaryolarda kullanılanlar şunlardır:

TTLSRule
TLS yapılandırmasıyla bir TCP/IP bağlantısı eşleştirmesi için bir ölçüt kümesi belirtir. Bu işlem, diğer deyim tipleriyle ilgilidir.

TTLSGroupAction
Başvuran TTLSRule ' in etkinleştirilip etkinleştirilmediğini belirtir.

TTLSEnvironmentAction
Başvuruda bulunan TTLSRule ' e ilişkin ayrıntılı yapılandırmayı belirtir ve bir dizi diğer deyimlere başvuruda bulunur.

TTLSKeyringParms
AT-TLS tarafından kullanılacak anahtarlık (key-ring) başvurularına gönderme yapar.

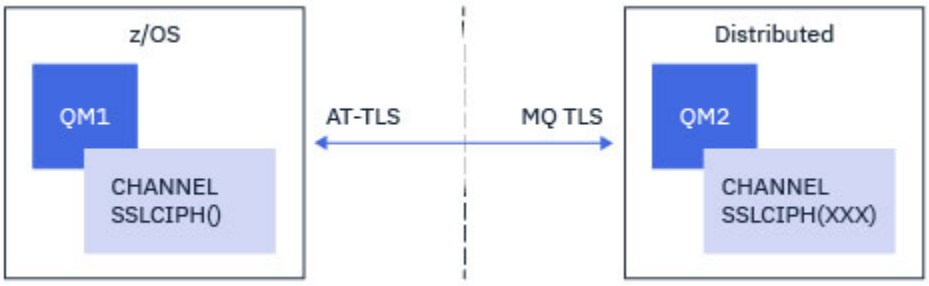
TTLSCipherParms
Kullanılacak şifreleme takımlarını tanımlar.

TTLSEnvironmentAdvancedParms
Hangi TLS ya da SSL protokollerinin etkinleştirildiğini tanımlar.

Uyarı: Burada, AT-TLS ' ye sahip başka AT-TLS ilkesi deyimleri belgelenmedi ve gereksinimlere bağlı olarak IBM MQ ile birlikte kullanılabilir. Ancak, IBM MQ yalnızca bu konuda açıklanan ilkelerle sınanmıştır.

CipherSpec adlı tek bir kuyruk yöneticisini kullanarak giden kanalda AT-TLS ' nin IBM MQ for Multiplatforms kuyruk yöneticisine yapılandırılması

IBM MQ for z/OS kuyruk yöneticisinden IBM MQ for Multiplatforms kuyruk yöneticisine giden bir kanalda AT-TLS ' yi ayarlama. Bu durumda, z/OS kuyruk yöneticisindeki kanal, SSLCIPH özniteliği ayarlanmamış bir gönderen kanaldır vez/OS kuyruk yöneticisindeki kanal, SSLCIPH özniteliği tek bir CipherSpecolarak ayarlanmış bir alıcı kanaldır.



Bu örnekte, TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec kullanan var olan bir gönderici-alıcı kanal çifti IBM MQ TLS yerine AT-TLS kullanacak şekilde ayarlanacak.

Yapılandırmada küçük ayarlamalar yapılarak diğer TLS iletişim kuralları ve CipherSpecs kullanılabilir. Küme gönderen ve küme alıcı kanalları dışında, AT-TLS yapılandırmasında herhangi bir değişiklik olmadan diğer ileti kanalı tipleri de kullanılabilir.

Yordam

Adım 1: Kanalın durdurulması

Adım 2: AT-TLS ilkesi oluşturma ve uygulama

Bu senaryo için aşağıdaki AT-TLS deyimlerini oluşturmanız gerekir:

1. Kanal başlatıcı adres alanındaki giden bağlantıları hedef alıcı kanalının IP adresi ve kapı numarasıyla eşleştirmek için bir TTLSRule deyimi. Bu değerler, gönderen kanalının CONNAME içinde kullanılan bilgilerle eşleşmelidir. Burada, belirli bir kanal başlatıcı iş adıyla eşleşmesi için daha fazla süzgeç eklenmiştir.

```
TTLSRule                        CSQ1-TO-REMOTE
{
  LocalAddr                     ALL
  RemoteAddr                    123.456.78.9
  RemotePortRange               1414
  Jobname                       CSQ1CHIN
  Direction                     OUTBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}
```

   Önceki kural, CSQ1CHIN işinden 1414 numaralı kapıdaki 123.456.78.9 IP adresine giden bağlantılarla eşleşir.

Daha ileri düzey süzgeç uygulama seçenekleri için TTLSRulekonusuna bakın.

2. Kuralı etkinleştiren bir TTLSGroupAction deyimi. TTLSRule , **TTLSGroupActionRef** özelliğini kullanarak TTLSGroupAction ' a başvurur.

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. **TTLSEnvironmentActionRef** özelliği tarafından TTLSRule ile ilişkili bir TTLSEnvironmentAction deyimi. TTLSEnvironmentAction , TLS Ortamını yapılandırır ve hangi anahtarın kullanılacağını belirtir.

```
TTLSEnvironmentAction               CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                     CLIENT
  TTLSKeyringParmsRef               CSQ1-KEYRING
  TTLSCipherParmsRef                CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef   CSQ1-ENVIRONMENT-ADVANCED
}
```

4. **TTLSKeyringParmsRef** özelliği tarafından TTLSEnvironmentAction ile ilişkili bir TTLSKeyringParms deyimi ve AT-TLS tarafından kullanılan anahtar halkasını tanımlar.

   Anahtarlık,z/OS dışı uzak kuyruk yöneticisi tarafından güvenilen sertifikaları içermelidir. Bu anahtarlık, kanal başlatıcısı tarafından kullanılan bir anahtarlık ile aynı şekilde tanımlanabilir; bkz. “Configuring your z/OS system to use TLS” sayfa 244.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. **TTLSCipherParmsRef** özelliği tarafından TTLSEnvironmentAction ile ilişkili bir TTLSCipherParms deyimi.

   Bu deyim, hedef alıcı kanalında kullanılan IBM MQ CipherSpec adının eşdeğeri olması gereken tek bir şifreleme takımı adı içermelidir.

   Not: AT-TLS şifreleme takımı adlarının IBM MQ CipherSpec adlarıyla eşleşmesi gerekmez. Ancak, aşağıdaki tabloda IBM MQ CipherSpec adını bularak ve TTLSCipherParms konusunda Tablo 2 'deki genişletilmiş karakter sütunuyla dört karakterli kod sütununu çapraz başvurarak bir IBM MQ CipherSpec adıyla eşleşen AT-TLS şifre grubu adı bulunabilir.

Çizelge 78. Dört karakterli kodlardan CipherSpec adlarına dönüştür

Dört karakterli kod	Protokol	Varsayılan olarak etkindir	CipherSpec adı
0001	SSL 3.0	Hayır	NULL_MD5
0002	SSL 3.0	Hayır	NULL_SHA
0003	SSL 3.0	Hayır	RC4_MD5_EXPORT
0004	SSL 3.0	Hayır	RC4_MD5_US
0005	SSL 3.0	Hayır	RC4_SHA_US
0006	SSL 3.0	Hayır	RC2_MD5_EXPORT
0008	SSL 3.0	Hayır	DES_SHA_EXPORT (DışA AKTARMA)
0009	TLS 1.0	Evet	TLS_RSA_WITH_DES_CBC_SHA

Çizelge 78. Dört karakterli kodlardan CipherSpec adlarına dönüştür (devamı var)

Dört karakterli kod	Protokol	Varsayılan olarak etkindir	CipherSpec adı
000A	SSL 3.0	Hayır	TRIPLE_DES_SHA_US
000A	TLS 1.0	Evet	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	Evet	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	Evet	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	Evet	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	Evet	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	Evet	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	Evet	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	Evet	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	Evet	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	Evet	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. TTLSEnvironmentAdvancedParms deyimi, **TTLSEnvironmentAdvancedParmsRef** özelliği tarafından TTLSEnvironmentAction ile ilişkilendirilir.

   Bu deyim, hangi SSL ve TLS iletişim kurallarının etkinleştirildiğini belirtmek için kullanılabilir. IBM MQ ile yalnızca, TTLSCipherParms deyiminde kullanılan şifre takımı adıyla eşleşen tek iletişim kuralını etkinleştirmeniz gerekir.

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3           OFF
  TLSv1           OFF
  TLSv1.1         OFF
  SecondaryMap    OFF
  TLSv1.2         ON
  TLSv1.3         OFF
}
```

Tüm deyim kümesi aşağıdaki gibidir ve ilke aracısına uygulanmalıdır:

```
TTLSRule                      CSQ1-TO-REMOTE
{
  LocalAddr                   ALL
  RemoteAddr                  123.456.78.9
  RemotePortRange             1414
  Jobname                     CSQ1CHIN
  Direction                   OUTBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        ON
  TLSv1.3        OFF
}
```

Adım 3: z/OS kanalından SSLCIPH ' nin kaldırılması

Aşağıdaki komutu kullanarak z/OS kanalından CipherSpec ' i kaldırın:

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

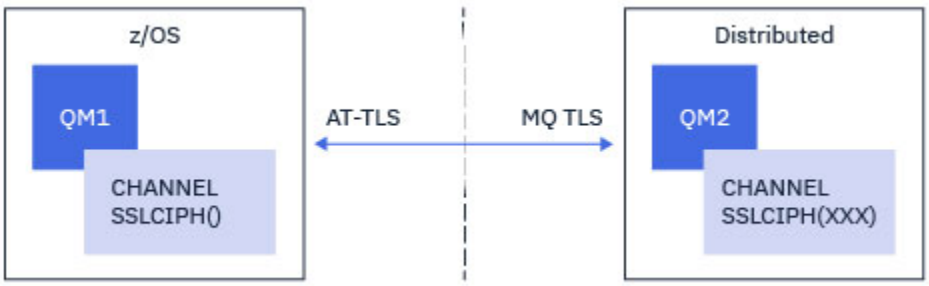
Adım 4: Kanalın başlatılması

Kanal başlatıldıktan sonra AT-TLS ve IBM MQ TLS birleşimini kullanacak.

Uyarı: Önceki AT-TLS bildirimleri çok az bir yapılandırmadır. Burada belgelenmemiş AT-TLS ile birlikte başka AT-TLS ilke bildirimleri vardır ve gereksinimine bağlı olarak IBM MQ ile birlikte kullanılabilir. Ancak, IBM MQ yalnızca açıklanan ilkelerle sınanmıştır.

CipherSpec adlı tek bir kuyruk yöneticisini kullanarak IBM MQ for Multiplatforms kuyruk yöneticisinden gelen kanalda AT-TLS ' nin yapılandırılması

IBM MQ for Multiplatforms kuyruk yöneticisinden IBM MQ for z/OS kuyruk yöneticisine gelen bir kanalda AT-TLS ' yi ayarlama. Bu durumda, z/OS kuyruk yöneticisindeki kanal SSLCIPH özniteliği ayarlanmamış bir alıcı kanaldır vez/OS dışı kuyruk yöneticisindeki kanal, SSLCIPH özniteliği tek bir CipherSpecolarak ayarlanmış bir gönderen kanaldır.



Bu örnekte, TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec alıcı kanalı IBM MQ TLS yerine AT-TLS kullanacak şekilde ayarlanacak.

Yapılandırmada küçük ayarlamalar yapılarak diğer TLS iletişim kuralları ve CipherSpecs kullanılabilir. Küme gönderen ve küme alıcı kanalları dışında, AT-TLS yapılandırmasında herhangi bir değişiklik olmadan diğer ileti kanalı tipleri de kullanılabilir.

Yordam

Adım 1: Kanalın durdurulması

Adım 2: AT-TLS ilkesi oluşturma ve uygulama

Bu senaryo için aşağıdaki AT-TLS deyimlerini oluşturmanız gerekir:

1. Gönderen kanalın IP adresinden kanal başlatıcı adres alanıyla gelen bağlantıları eşleştirmek için bir TTLSRule deyimi. Burada, belirli bir kanal başlatıcı iş adıyla eşleşmesi için daha fazla süzgeç eklenmiştir.

```
TTLSRule                        REMOTE-TO-CSQ1
{
  LocalAddr                     ALL
  LocalPortRange                1414
  RemoteAddr                    123.456.78.9
  Jobname                       CSQ1CHIN
  Direction                     INBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-INBOUND-ENVIRONMENT-ACTION
}
```

   Önceki kural, 123.456.78.9uzak IP adresinden 1414 numaralı yerel kapıdaki CSQ1CHIN işine gelen bağlantılarla eşleşir.

   Daha ileri düzey süzgeç uygulama seçenekleri için TTLSRulekonusuna bakın.

2. Kuralı etkinleştiren bir TTLSGroupAction deyimi. TTLSRule , **TTLSGroupActionRef** özelliğini kullanarak TTLSGroupAction ' a başvurur.

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. TTLSEnvironmentAction deyimi, **TTLSEnvironmentActionRef** özelliği tarafından TTLSRule ile ilişkilendirilir. TTLSEnvironmentAction , TLS Ortamını yapılandırır ve hangi anahtarın kullanılacağını belirtir.

```
TTLSEnvironmentAction                 CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                       SERVER
  TTLSKeyringParmsRef                 CSQ1-KEYRING
  TTLSCipherParmsRef                  CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef     CSQ1-ENVIRONMENT-ADVANCED
}
```

AT-TLS, SSLCAUTH kanal özniteliğini kullanmaya eşdeğer olan karşılıklı kimlik doğrulaması sağlama yeteneği sağlar. Bu, gelen TTLSEnvironmentAction deyimi için **HandshakeRole** değeri *ServerWithClientAuth* olan bir TTLSEnvironmentAction deyimi ile yapılır.

4. TTLSKeyringParms deyimi, **TTLSKeyringParmsRef** özelliği tarafından TTLSEnvironmentAction ile ilişkilendirilir ve AT-TLS tarafından kullanılan anahtar halkasını tanımlar.

   Anahtarlık,z/OS dışı uzak kuyruk yöneticisi tarafından güvenilen sertifikaları içermelidir. Bu anahtarlık, kanal başlatıcısı tarafından kullanılan bir anahtarlık ile aynı şekilde tanımlanabilir; bkz. “Configuring your z/OS system to use TLS” sayfa 244.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. **TTLSCipherParmsRef** özelliği tarafından TTLSEnvironmentAction ile ilişkili bir TTLSCipherParms deyimi.

   Bu deyim, uzak gönderen kanalında kullanılan IBM MQ CipherSpec adının eşdeğeri olması gereken tek bir şifreleme takımı adı içermelidir.

   Not: AT-TLS şifreleme takımı adlarının IBM MQ CipherSpec adlarıyla eşleşmesi gerekmez. Ancak, aşağıdaki tabloda IBM MQ CipherSpec adını bularak ve TTLSCipherParms konusunda Tablo 2 'deki genişletilmiş karakter sütunuyla dört karakterli kod sütununu çapraz başvurarak bir IBM MQ CipherSpec adıyla eşleşen AT-TLS şifre grubu adı bulunabilir.

Çizelge 79. Dört karakterli kodlardan CipherSpec adlarına dönüştür

Dört karakterli kod	Protokol	Varsayılan olarak etkindir	CipherSpec adı
0001	SSL 3.0	Hayır	NULL_MD5
0002	SSL 3.0	Hayır	NULL_SHA
0003	SSL 3.0	Hayır	RC4_MD5_EXPORT
0004	SSL 3.0	Hayır	RC4_MD5_US
0005	SSL 3.0	Hayır	RC4_SHA_US
0006	SSL 3.0	Hayır	RC2_MD5_EXPORT
0008	SSL 3.0	Hayır	DES_SHA_EXPORT (DışA AKTARMA)
0009	TLS 1.0	Evet	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	Hayır	TRIPLE_DES_SHA_US
000A	TLS 1.0	Evet	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	Evet	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	Evet	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	Evet	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	Evet	TLS_RSA_WITH_AES_128_CBC_SHA256

Çizelge 79. Dört karakterli kodlardan CipherSpec adlarına dönüştür (devamı var)

Dört karakterli kod	Protokol	Varsayılan olarak etkindir	CipherSpec adı
003D	TLS 1.2	Evet	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	Evet	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	Evet	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	Evet	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	Evet	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. TTLSEnvironmentAdvancedParms deyimi, **TTLSEnvironmentAdvancedParmsRef** özelliği tarafından TTLSEnvironmentAction ile ilişkilendirilir.

   Bu deyim, hangi SSL ve TLS iletişim kurallarının etkinleştirildiğini belirtmek için kullanılabilir. IBM MQ ile yalnızca, TTLSCipherParms deyiminde kullanılan şifre takımı adıyla eşleşen tek iletişim kuralını etkinleştirmeniz gerekir.

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3           OFF
  TLSv1           OFF
  TLSv1.1         OFF
  SecondaryMap    OFF
  TLSv1.2         ON
  TLSv1.3         OFF
}
```

Tüm deyim kümesi aşağıdaki gibidir ve ilke aracısına uygulanmalıdır:

```
TTLSRule                      REMOTE-TO-CSQ1
{
  LocalAddr                   ALL
  LocalPortRange              1414
  RemoteAddr                  123.456.78.9
  Jobname                     CSQ1CHIN
  Direction                   INBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-INBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Adım 3: z/OS kanalından SSLCIPH ' nin kaldırılması

Aşağıdaki komutu kullanarak z/OS kanalından CipherSpec ' i kaldırın:

```
ALTER CHANNEL(channel-name) CHLTYPE(RCVR) SSLCIPH(' ')
```

Adım 4: Kanalın başlatılması

Kanal başlatıldıktan sonra AT-TLS ve IBM MQ TLS birleşimini kullanacak.

Uyarı: Önceki AT-TLS bildirimleri çok az bir yapılandırmadır. Burada belgelenmemiş AT-TLS ile birlikte başka AT-TLS ilke bildirimleri vardır ve gereksinimine bağlı olarak IBM MQ ile birlikte kullanılabilir. Ancak, IBM MQ yalnızca açıklanan ilkelerle sınanmıştır.

SSL ve TLS gizli anahtarlarını sıfırlama

IBM MQ , kuyruk yöneticilerinde ve istemcilerde gizli anahtarların ilk durumuna getirilmesini destekler.

Belirtilen sayıda şifrelenmiş veri kanal boyunca aktığında gizli anahtarlar sıfırlanır. Kanal sağlıklı işletim bildirimleri etkinleştirilirse, kanal sağlıklı işletim bildirimi gönderilmeden ya da alınmadan önce gizli anahtar sıfırlanır.

Anahtar ilk duruma getirme değeri her zaman IBM MQ kanalının başlangıç tarafından ayarlanır.

Kuyruk yöneticisi

Bir kuyruk yöneticisi için, anahtar yeniden anlaşması sırasında kullanılan değerleri ayarlamak üzere **SSLRKEYC** parametresiyle birlikte **ALTER QMGR** komutunu kullanın.

IBM i IBM isistemlerinde **CHGMQM** değiştirgesini **SSLRSTCNT** değiştirgesiyle kullanın.

MQI istemcisi

Varsayılan olarak, MQI istemcileri gizli anahtarı yeniden anlaşmaz. Bir MQI istemcisinin anahtarı üç şekilde yeniden görüşmesini sağlayabilirsiniz. Aşağıdaki listede, yöntemler öncelik sırasına göre gösterilir. Birden çok değer belirtirseniz, en yüksek öncelik değeri kullanılır.

1. MQCONNX çağrısında MQSCO yapısında KeyResetSayı alanını kullanarak
2. MQSSLRESET ortam değişkenini kullanarak
3. MQI istemcisi yapılandırma dosyasında SSLKeyResetCount özniteliğini ayarlayarak

Bu değişkenler, TLS gizli anahtarı yeniden anlaşılmadan önce TLS etkileşimi içinde gönderilen ve alınan şifrelenmemiş bayt sayısını gösteren, 0-999 999 999 aralığında bir tamsayıya ayarlanabilir. 0 değerinin belirtilmesi, TLS gizli anahtarlarının hiçbir zaman yeniden anlaşılmadığını gösterir. 1-32 KB aralığında bir TLS gizli anahtar sıfırlama sayısı belirtirseniz, TLS kanalları 32 KB gizli anahtar sıfırlama sayısını kullanır. Bu, küçük TLS gizli anahtar sıfırlama değerleri için ortaya çıkabilecek aşırı anahtar sıfırlamalarını önlemektir.

Sıfırdan büyük bir değer belirtilirse ve kanal için kanal sağlıklı işletim bildirimleri etkinleştirilirse, ileti verileri bir kanal sağlıklı işletim bildirimi sonrasında gönderilmeden ya da alınmadan önce gizli anahtar da yeniden belirlenir.

Her başarılı yeniden anlaşma sonrasında bir sonraki gizli anahtar yeniden anlaşması sıfırlanıncaya kadar bayt sayısı.

MQSCO yapısının tüm ayrıntıları için bkz. KeyResetCount (MQLONG). MQSSLRESET ile ilgili tüm ayrıntılar için bkz. MQSSLRESET. İstemci yapılandırma dosyasında TLS kullanımı hakkında daha fazla bilgi için bkz. İstemci yapılandırma dosyasının SSL kısmı.

Java

IBM MQ classes for Javaiçin bir uygulama gizli anahtarı aşağıdaki yollardan biriyle sıfırlayabilir:

- MQEnvironment sınıfında sslResetSayı alanını ayarlayarak.
- Bir Hashtable nesnesinde MQC.SSL_RESET_COUNT_PROPERTY ortam özelliğini ayarlayarak. Daha sonra uygulama, MQEnvironment sınıfındaki `properties` alanına Hashtable 'ı atar ya da Hashtable 'ı oluşturucusundaki bir MQQueueManager nesnesine geçirir.

Uygulama bu yöntemlerden birden fazlasını kullanıyorsa, olağan öncelik kuralları geçerlidir. Öncelik kuralları için bkz. Class com.ibm.mq.MQEnvironment .

sslResetSayı alanı ya da ortam özelliği MQC.SSL_RESET_COUNT_PROPERTY değeri, gizli anahtar yeniden anlaşılmadan önce IBM MQ classes for Java istemci kodu tarafından gönderilen ve alınan toplam bayt sayısını gösterir. Gönderilen bayt sayısı, şifrelemeden önceki sayıdır ve alınan bayt sayısı, şifre çözmeden sonraki sayıdır. Bayt sayısı, IBM MQ classes for Java istemcisi tarafından gönderilen ve alınan denetim bilgilerini de içerir.

Sıfırlama sayısı sıfırsa (varsayılan değer), gizli anahtar hiçbir zaman yeniden anlaşılmaz. CipherSuite belirtilmezse sıfırlama sayısı yoksayılır.

JMS

IBM MQ classes for JMSiçin SSLRESETCOUNT özelliği, şifreleme için kullanılan gizli anahtar yeniden anlaşılmadan önce bir bağlantı tarafından gönderilen ve alınan toplam bayt sayısını gösterir. Gönderilen bayt sayısı, şifrelemeden önceki sayıdır ve alınan bayt sayısı, şifre çözmeden sonraki sayıdır. Bayt sayısı, IBM MQ classes for JMStarafından gönderilen ve alınan denetim bilgilerini de içerir. Örneğin, 4 MB

veri aktıktan sonra yeniden görüşülen bir gizli anahtarla TLS etkin bir MQI kanalı üzerinden bağlantı oluşturmak için kullanılabilecek bir ConnectionFactory nesnesi yapılandırmak için JMSAdmin 'e şu komutu verin:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Varsayılan değer olan SSLRESETCOUNT değeri sıfırsa, gizli anahtar hiçbir zaman yeniden anlaşılmaz. SSLCIPHERSUITE ayarlanmazsa, SSLRESETCOUNT özelliği yoksayılır.

.NET

.NET yönetilmeyen istemciler için SSLKeyResettamsayı özelliği, gizli anahtar yeniden anlaşılmadan önce TLS etkileşimi içinde gönderilen ve alınan şifrelenmemiş bayt sayısını gösterir.

IBM MQ classes for .NETiçinde nesne özelliklerinin kullanımı hakkında bilgi için bkz. Öznitelik değerlerini alma ve ayarlama.

.NET yönetilen istemciler için, SSLStream sınıfı gizli anahtar yeniden ayarlamayı/yeniden anlaşmayı desteklemez. Ancak, diğer IBM MQ istemcileriyle tutarlı olması için IBM MQ yönetilen .NET istemci, uygulamaların SSLKeyResetSayımı ayarlamasına izin verir. Daha fazla bilgi için bkz. Gizli anahtar sıfırlama ya da yeniden anlaşma.

XMS .NET

XMS .NET yönetilmeyen istemciler için IBM MQ kuyruk yöneticisine güvenli bağlantılarbaşlıklı konuya bakın.

İlgili başvurular
ALTER QMGR
QMGR ' YI GöRüNTüLE
İleti Kuyruğu Yöneticisini Değiştir (CHGMQM)
İleti Kuyruğu Yöneticisini Görüntüle (DSPMQM)

Kullanıcı çıkış programlarında gizliliği uygulama

Güvenlik çıkışlarında gizliliği uygulama

Güvenlik çıkışları, kanalda akan verilerin şifrelenmesi ve şifrelerinin çözülmesi için simetrik anahtarı üreterek ve dağıtarak gizlilik hizmetinde bir rol oynayabilir. Bu işlemi yapmak için kullanılan ortak bir teknik, PKI teknolojisini kullanır.

Bir güvenlik çıkışı rasgele bir veri değeri oluşturur, bunu kuyruk yöneticisinin ya da iş ortağı güvenlik çıkısının temsil ettiği kullanıcının ortak anahtisiyle şifreler ve şifrelenmiş verileri bir güvenlik iletisinde iş ortağına gönderir. İş ortağı güvenlik çıkışı, rasgele veri değerinin şifresini, kuyruk yöneticisinin ya da temsil ettiği kullanıcının özel anahtisiyle çözer. Her güvenlik çıkışı, her ikisi için de bilinen bir algoritma kullanarak, simetrik anahtarı diğerinden bağımsız olarak türetmek için rasgele veri değerini kullanabilir. Diğer bir seçenek olarak, rasgele veri değerini anahtar olarak da kullanabilirler.

İlk güvenlik çıkışı ortağını bu zamana kadar doğrulamamışsa, iş ortağı tarafından gönderilen bir sonraki güvenlik iletisi, simetrik anahtarla şifrelenmiş bir beklenen değeri içerebilir. İlk güvenlik çıkışı, iş ortağı güvenlik çıkısının beklenen değeri doğru şekilde şifreleyebildiğinden emin olarak iş ortağının kimliğini doğrulayabilir.

Güvenlik çıkışları, birden fazla algoritma kullanılabiliyorsa, kanalın üzerinde akan verilerin şifrelenmesi ve şifrelerinin çözülmesi için bu olanağı da kabul edebilir.

İleti çıkışlarında gizliliği uygulama

Bir kanalın gönderme bitiminde bir ileti çıkışı, bir iletteki uygulama verilerini şifreleyebilir ve kanalın giriş ucundaki başka bir ileti çıkışı verilerin şifresini çözebilir. Performans nedenlerinden dolayı, normalde bu amaçla kullanılan bir simetrik anahtar algoritması kullanılır. Simetrik anahtarın nasıl oluşturulabileceğiyle ve dağıtılabileceğiyle ilgili daha fazla bilgi için bkz. “Kullanıcı çıkış programlarında gizliliği uygulama” sayfa 430.

İleti çıkışı gibi, ileti çıkışını içeren MQXQH (iletim kuyruğu üstbilgisi) gibi bir iletteki üstbilgiler, bir ileti çıkışı tarafından şifrelenmemelidir. Bunun nedeni, ileti üstbilgilerinin veri dönüştürme işlemi, gönderme sonunda ya da ileti çıkışı çağrıldığında, ileti çıkışı çağrıldıktan sonra ya da alma uçta çağrılmadan önce gerçekleşir. Üstbilgiler şifrelenmişse, veri dönüştürme işlemi başarısız olur ve kanal durdurulur.

Gönderme ve alma çıkışlarında gizliliği uygulama

Gönder ve alma çıkışları, bir kanalda akan verileri şifrelemek ve şifrelerini çözmek için kullanılabilir. Bu hizmet, bu hizmeti sağlamak için ileti çıkışlarından daha uygun olarak aşağıdaki nedenlerle gerçekleştirilir:

- İleti kanallarında, ileti üstbilgileri, iletilerde uygulama verileri kadar şifrelenebilir.
- Gönderme ve alma çıkışları, ileti kanallarının yanı sıra, MQI kanallarında da kullanılabilir. MQI çağrılarına ilişkin parametreler, bir MQI kanalına akırken korunması gereken duyarlı uygulama verileri içerebilir. Bu nedenle, aynı gönderme ve alma çıkışlarını her iki tür kanalda da kullanabilirsiniz.

API çıkışta ve API ' den geçiş çıkışındaki gizliliği uygulama

Bir iletteki uygulama verileri, ileti gönderme uygulaması tarafından konulduğunda ikinci bir çıkış tarafından bir API ya da API geçidi çıkışı tarafından şifrelenebilir ve ileti, alıcı uygulama tarafından alındığında ikinci bir çıkış tarafından çözülür. Performans nedenlerinden dolayı, tipik olarak bu amaçla kullanılan bir simetrik anahtar algoritması kullanılır. Ancak, birçok kullanıcının birbirlerine ileti gönderebileceği uygulama düzeyinde, sorun, iletinin yalnızca amaçlanan günlük nesnesinin, iletinin şifresini çözebilmesini sağlamanın nasıl sağlanabileceğidir. Tek bir çözüm, ileti gönderen her kullanıcı çifti için farklı bir simetrik anahtar kullanmaktadır. Ancak bu çözüm, özellikle kullanıcıların farklı kuruluşlara ait olması durumunda, yönetmek için zor ve zaman alan bir çözüm olabilir. Bu sorunu çözmenin standart bir yolu *dijital zarflama* olarak bilinir ve PKI teknolojisini kullanır.

Bir uygulama bir iletiyi kuyruğa yerleştirdiğinde, bir API ya da API geçiş çıkışı rasgele bir simetrik anahtar oluşturur ve iletide uygulama verilerini şifrelemek için anahtarı kullanır. Çıkış, hedeflenen alıcının genel anahtarı ile simetrik anahtarı şifreler. Daha sonra, iletteki uygulama verilerini şifrelenmiş uygulama verileri ve şifrelenmiş simetrik anahtarla değiştirir. Bu şekilde, yalnızca amaçlanan alıcı, simetrik anahtarın ve dolayısıyla uygulama verilerinin şifresini çözebilir. Şifrelenmiş bir iletinin birden çok olası hedef nesnesi varsa, çıkış, her bir hedef günlük nesnesi için simetrik anahtarın bir kopyasını şifreleyebilir.

Uygulama verilerinin şifrelenmesi ve şifrelerinin çözülmesi için farklı algoritmalar kullanılabiliyorsa, çıkış, kullandığı algoritmanın adını içerebilir.

z/OS V 9.1.4 Confidentiality for data at rest on IBM MQ for z/OS with data set encryption

IBM MQ for z/OS , verileri etkin günlük veri kümelerine, arşiv günlüğü veri kümelerine, sayfa kümelerine, önyükleme kayışı veri kümeleri (BSDS) ve V 9.1.5 paylaşılan ileti veri kümeleri (SMDS)yazarak müşteriyi ve yapılandırma verilerini barınayabilir.

z/OS , veri kümelerinin verimli, ilkeye dayalı olarak şifrelenmesini sağlar. IBM MQ for z/OS , aşağıdakiler için z/OS veri kümesi şifrelemesini destekler:

- Etkin günlük veri kümeleri; bkz. “1” sayfa 432
- Günlük veri kümelerini arşivle; bkz. “2” sayfa 432
- Sayfa kümeleri; bkz. “1” sayfa 432

- BSDS; bkz. “2” sayfa 432
- CSQINP* veri kümeleri; bkz. “2” sayfa 432
- V 9.1.5 SMDS; bkz. “3” sayfa 432

Bu, ayrı bir z/OS kuyruk yöneticisinde verilerin geri kalanına ilişkin gizliliği sağlar.

Notlar:

1. IBM MQ 9.1.4' tan IBM MQ for z/OS , etkin günlükler ve sayfa kümeleri için z/OS veri kümesi şifrelemesini destekler.
2. Arşiv günlükleri, BSDS ve CSQINP* veri kümeleri için veri kümesi şifrelemesi, IBM MQ for z/OS' un tüm sürümlerinde desteklenir.
3. V 9.1.5 IBM MQ 9.1.5' tan IBM MQ for z/OS , SMDS için z/OS veri kümesi şifrelemesini destekler.
4. IBM MQ Advanced Message Security , verileri geri kalanıyla korumanın alternatif bir mekanizmasını sağlar. Ayrıca, AMS , bellekteki ve uçuşta verileri de korur.

z/OS veri kümesi şifrelemesine ilişkin ek bilgi için z/OS veri kümesi şifreleme geliştirmelerinin kullanılması başlıklı konuya bakın.

z/OS veri kümesi şifrelemesinin yapılandırılması, IBM MQ for z/OSdenetiminin dışındadır. Şifreleme ayarları, veri kümesi yaratıldığında yürürlüğe girmektedir.

Başka bir deyişle, yeni bir veri kümesi şifreleme ilkesi kullanılmadan önce var olan veri kümelerinin yeniden oluşturulması gerekir.

IBM MQ for z/OS şifrelenmiş ve şifrelenmemiş veri kümelerinin bir karışımıyla çalışabilir, ancak standart bir yapılandırma kullanılan veri kümelerinin tümünü ya da hiçbirini şifreleyemez.

z/OS V 9.1.4 Bir IBM MQ for z/OS veri kümesini şifrelemek için gereken adımlara genel bakış

Bir IBM MQ for z/OS veri kümesini şifrelemenizi sağlar.

Başlamadan önce

You must ensure that you have configured z/OS data set encryption correctly in your enterprise. Veri kümesi şifrelemesini bir kuyruk paylaşım grubunda ayarlıyorsanız, veri paylaşımı için z/OS veri kümesi şifrelemesini yapılandırmalısınız.

Not: A z/OS encrypted data set must be an extended format data set.

Yordam

1. Veri kümesini şifrelemek için RACF 'de şifreleme anahtarını ve `key-label` ' yi ayarlayın.
2. RACF CSFKEYS sınıfındaki `key-label` için bir tanıtım yaratın.
3. Kuyruk yöneticisinin kullanıcı kimliğine ve şifrelenmiş verilere erişmesi gereken diğer tüm kullanıcı tanıtıcılarına okuma erişimi verin.

   Bu, veri kümesine karşı yazdırma yardımcı programlarını çalıştırmak için kullanılan kullanıcı kimliklerini içerebilir. Örneğin, CSQUTIL SKOPI çalıştıran kullanıcının, ilgili sayfa kümesinin şifresini çözmek zorunda olması gerekir.
4. Associate the encryption `key-label` with the data set name.

   Bu işlemi, veri kümesi adı ya da üst düzey niteleyici için bir SMS veri sınıfı ya da RACF DFP bölümü kullanarak yapabilirsiniz.

   Ayrıca, veri kümesi ayrıldığında `key-label` ' yi veri kümesiyle de ilişkilendirebilirsiniz.
5. IDCAMS ALTER kullanarak var olan veri kümesini yeniden adlandırın.
6. Uygun özniteliklerle veri kümesini yeniden ayırın.

7. Yeniden adlandırılan veri kümesinin içeriğini IDCAMS REPRO kullanarak yeni veri kümesine kopyalayın.
   Veriler, veri kümesine kopyalamanın işlemi tarafından şifrelenir.
8. Şifrelenmesi gereken diğer veri kümeleri için “4” sayfa 432 - “6” sayfa 432 arasındaki adımları yineleyin.

z/OS V 9.1.4 Kuyruk yöneticisi etkin günlüklerinin nasıl şifreleneceğini gösteren örnek

Aşağıdaki konularda, var olan etkin günlüklerde veri kümesi şifrelemesini etkinleştirme işlemi boyunca size yol göstermektedir.

Not: Diğer veri kümelerinin süreci, etkin günlüklere benzer bir işlemdir.

Bu örnekte:

- Queue manager CSQ1 is run under user QMCSQ1, and has active log data sets CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002, and so on
- Donanım ve yazılım ortamı, z/OS veri kümesi şifrelemesini kullanma yeteneğine sahiptir.
- RACF, SAF olarak kullanılır
- Kuyruk yöneticisi durduruldu

Yordamı aşağıdaki sırada taşıyın:

1. “Kuyruk yöneticisi için veri kümesi şifreleme anahtarının yapılandırılması” sayfa 433
2. “Günlük veri kümeleri için veri kümesi şifrelemesini yapılandırma” sayfa 434

z/OS V 9.1.4 Kuyruk yöneticisi için veri kümesi şifreleme anahtarının yapılandırılması

Bir kuyruk yöneticisi için veri kümesi şifreleme anahtarını nasıl yapılandırasınız.

Bu görev hakkında

Bu görev, “Günlük veri kümeleri için veri kümesi şifrelemesini yapılandırma” sayfa 434için önkoşuldur.

Yordam

1. Set up an AES-256 bit encryption DATA key with a label, for example, CSQ1DSKY, using the z/OS key generator yardımcı programı (KGUP).
2. Aşağıdaki komutu girerek, CSQ1DSKY şifreleme anahtarı için RACF CSFKEYS tanıtımını tanımlayın:

   ```
   RDEFINE CSFKEYS CSQ1DSKY UACC(NONE)
   ```

3. Aşağıdaki komutu girerek, tanıtımın ICSF bölümünü, anahtar olarak korunan anahtar olarak kullanılmasına izin verecek şekilde yapılandırın:

   ```
   RALTER CSFKEYS CSQ1DSKY ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
   ```

4. Kuyruk yöneticisinin, aşağıdaki komutu vererek profile QMCSQ1 READ erişimi vererek şifreleme anahtarını kullanmasına izin verin:

   ```
   PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
   ```

   Şifrelenmiş veri kümesini okuması ya da yazması gereken herhangi bir yönetici kullanıcıya aynı erişimi verin.
5. Aşağıdaki komutu girerek CSFKEYS sınıfını yenileyin.

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Sonraki adım

Veri kümeleri için veri kümesi şifrelemesini “Günlük veri kümeleri için veri kümesi şifrelemesini yapılandırma” sayfa 434içinde açıklandığı gibi yapılandırın

z/OS V 9.1.4 Günlük veri kümeleri için veri kümesi şifrelemesini yapılandırma

Günlük veri kümelerinde şifrelemeyi nasıl yapılandırdığınızı belirler.

Başlamadan önce

Okuduğunuzdan emin olun:

IBM MQ for z/OS veri kümesini şifrelemeye ilişkin adımlara genel bakışve yordamı şu şekilde gerçekleştiren:
“Kuyruk yöneticisi için veri kümesi şifreleme anahtarının yapılandırılması” sayfa 433

Bu görev hakkında

This method uses the DFP segment of a RACF generic profile, so that you can use the encryption key for all new data sets that match the profile.

Diğer bir seçenek olarak, bir SMS veri sınıfı yapılandırabilir ve kullanabilir ya da anahtar etiketi, veri kümesini ayırdığınızda doğrudan belirtilebilir.

As previously described, in this example, queue manager CSQ1 is run under user QMCSQ1, and has active log data sets CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002, and so on.

Yordam

1. Aşağıdaki komutu vererek, soysal profili yaratın:

   ```
   ADDSD 'CSQ1.LOGS.*' UACC(NONE)
   ```

2. Aşağıdaki komutu girerek, tanıtıma ilişkin kuyruk yöneticisi kullanıcısının erişim erişimini değiştirmesine izin verin:

   ```
   PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
   ```

   Ayrıca, herhangi bir yönetici kullanıcı için gereken erişim iznine de izin verin.

3. Aşağıdaki komutu girerek, DFP kesimini şifreleme anahtarı etiketiyle ekleyin:

   ```
   ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
   ```

   Not: Kuyruk yöneticisi için veri kümesi şifreleme anahtarının yapılandırılmasıalanında kullandığınız şifreleme anahtarını kullanmanız gerekir.

4. Soysal veri kümesi tanıtımlarını yenileyin ve aşağıdaki komutu verin:

   ```
   SETROPTS GENERIC(DATASET) REFRESH
   ```

5. Her bir günlük verilerini yedeklemek için yeniden adlandırın, sonra IDCAMS kullanarak verileri yeniden yaratın ve geri yükleyin. Aşağıdaki JCL parçası CSQ1.LOGS.LOGCOPY1.DS001:

   a) Veri kümesini yedeklemek için yeniden adlandır

   ```
   //RENAME   EXEC PGM=IDCAMS,REGION=0M
   //SYSPRINT DD SYSOUT=*
   //SYSIN    DD *
     /*-------------------------------------------------------------*/
     /* RENAME DATASET TO BACKUP                                    */
     /*-------------------------------------------------------------*/
     ALTER 'CSQ1.LOGS.LOGCOPY1.DS001'                  -
           NEWNAME('CSQ1.BAK.LOGS.LOGCOPY1.DS001')
   ```

b) Veri kümesini yeniden tanımlayın.

Yeni veri kümesi, RACF tanıtımı nedeniyle şifrelenecek.

Not: Veri kümesi için kullanmak istediğiniz genişletilmiş biçim veri sınıfının adını + + EXTDICLASS + + yerine koyun.

```
//REDEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* REDEFINE THE DATASET                                        */
  /*-------------------------------------------------------------*/
  DEFINE CLUSTER                                    -
         (NAME(CSQ1.LOGS.LOGCOPY1.DS001)            -
         LINEAR                                     -
         SHAREOPTIONS(2 3)                          -
         MODEL(CSQ1.BAK.LOGS.LOGCOPY1.DS001)        -
         DATACLAS(++EXTDCLASS++))
```

c) Yedekten verileri yeniden yaratılmış veri kümesine kopyalayın.

Bu adım, verileri şifreler.

```
//RESTORE  EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RESTORE DATA INTO ENCRYPTED LOG                             */
  /*-------------------------------------------------------------*/
  REPRO INDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)     -
        OUTDATASET(CSQ1.LOGS.LOGCOPY1.DS001)
```

Sonraki adım

Tüm etkin günlük veri kümeleri için “5” sayfa 434 . adımı yineleyin.

Yalnızca tek bir şifreleme anahtarı gereklidir ve tüm veri kümeleri aynı anahtar etiketiyle ilişkilendirilebilir.

Yeniden başlatma kuyruk yöneticisi CSQ1. Günlük veri kümelerinin şifrelenip şifrelenmediğini doğrulamak için DISPLAY LOG (GM) komutunu kullanarak çıkışı kullanın.

z/OS V 9.1.4 Bir kuyruk paylaşım grubunda z/OS veri kümesi şifrelemesi için dikkat edilmesi gereken noktalar

Each queue manager in a queue sharing group (QSG) must be able to read the logs, BSDS V 9.1.5 Ve paylaşılan ileti veri kümeleri (SMDS), of every other queue manager in the QSG.

Bu, QSG üyesinin çalışabileceği her bir sistemin, z/OS veri kümesi şifrelemesi için gereksinimleri karşılaması ve QSG ' deki her kuyruk yöneticisine ilişkin veri kümelerini korumak için kullanılan tüm anahtar etiketlerini ve şifreleme anahtarlarını her sistemde kullanılabilir olması anlamına gelir.

IBM MQ for z/OS 9.1.3 öncesinde bir kuyruk yöneticisi, şifrelenmiş bir etkin günlük veri kümesine erişemiyor.

V 9.1.5 IBM MQ for z/OS 9.1.3 'dan önceki bir kuyruk yöneticisi şifrelenmiş bir SMDS' ye erişemez.

V 9.1.5 z/OS veri kümesi şifrelemesini kullanmadan önce, QSG içindeki tüm kuyruk yöneticilerini en az IBM MQ for z/OS 9.1.3' e geçirmeniz gerekir.

QSG 'de bir kuyruk yöneticisi şifrelenmiş herhangi bir etkin günlük veri kümesiyle başlatıldıysa ve QSG' deki başka bir kuyruk yöneticisi başlatıldıysa, ancak en son, şifrelenmiş etkin günlükleri destekleyen bir IBM MQ for z/OS sürümüyle başlamadıysa, şifrelenmiş etkin günlüğe sahip kuyruk yöneticisi olağandışı bitiş kodu 5C6-00F50033ile olağan dışı olarak sonlandırılır.

V 9.1.5 Bir QSG 'yi şifrelenmiş etkin günlükleri ve SMDS' leri tam bir kesinti olmadan kullanmak için aşağıdaki gibi dönüştürebilirsiniz:

1. Her kuyruk yöneticisinin sırayla en az IBM MQ 9.1.5 olması gerekir.
2. Etkin günlüklerin her kuyruk yöneticisi için şifrelenmiş veri kümelerine dönüştürülmesi. Bu, kuyruk yöneticisinin sona erdirilmesini ve sonra yeniden başlatılmasını gerektirir.

   Aynı zamanda, şifrelenmiş veri kümeleri için de sayfa kümeleri ve arşiv günlükleri de etkinleştirilecektir, ancak bu QSG geçişini etkilemez.

   The procedure for converting each data set is described in “Kuyruk yöneticisi etkin günlüklerinin nasıl şifreleneceğini gösteren örnek” sayfa 433
3. Her bir CF yapısı için SMDS ' nin her bir CF yapısı için şifrelenmiş veri kümelerine dönüştürülmesi:
   a. Kuyruk yöneticisi erişimini SMDS ' ye askıya almak için RESET SMDS (*) ACCESS (DISABLED) CFSTRUCT (structure-name) komutunun verilmesi.

      Bu süre içinde, SMDS ile ilişkili paylaşılan kuyruklardaki verilerin geçici olarak kullanılamadığını göz önünde bulundurun.
   b. Converting each data set that makes up the SMDS to encrypted data sets, using the procedure described in “Kuyruk yöneticisi etkin günlüklerinin nasıl şifreleneceğini gösteren örnek” sayfa 433.
   c. SDS 'ye (*) RESET SMDS (*) ACCESS (ENABLED) CFSTRUCT (structure-name) komutunun verilmesi, SMDS' ye kuyruk yöneticisi erişimini devam ettirmesini sağlar.

Uyarı: Etkin günlük veri kümelerinin geçici olarak kullanılamayacağı için, günlükleri dönüştürmeden önce kuyruk yöneticisini temiz bir şekilde kapatmanız gerekir ve dönüştürme sırasında bağlaşım olanağı yapısı kurtarma işlemi olanaklı olmayabilir.

z/OS V 9.1.4 z/OS veri kümesi şifrelemesi kullanılırken geriye doğru geçişle ilgili önemli noktalar

Bir ya da daha fazla şifrelenmiş veri kümesi olan bir kuyruk yöneticisini geriye doğru geçirirken aşağıdakileri göz önünde bulundurmanız gerekir.

z/OS veri kümesi şifrelemesi aşağıdaki IBM MQ for z/OS veri kümelerinde desteklenir:

- Etkin günlük veri kümeleri
- Günlük veri kümelerini arşivle
- Sayfa kümeleri
- BSDS (BDS)
- V 9.1.5 KOBİ ' LER
- CSQINP* veri kümeleri

BSDS, arşiv günlüğü ya da CSINP* veri kümeleri için geriye dönük geçiş konuları yoktur.

Bununla birlikte,

- V 9.1.5 KOBİ ' LER
- Sayfa kümesi ve
- Etkin günlük

z/OS veri kümesi şifrelemesiyle birlikte kullanılan veri kümeleri, IBM MQ for z/OS 9.1.0ve daha önceki uzun süreli destek yayınlarında desteklenmez.

Geri geçişten önce, V 9.1.5 SMDS, sayfa kümesi ve etkin günlük veri kümeleri için tüm şifreleme ilkelerinin kaldırılması ve verilerin şifresinin çözülmesi gerekir. Bu işlem “Veri kümesi şifrelemesini veri kümesinden kaldırma” sayfa 437içinde açıklanmıştır.

Uyarı: Geri geçirilecek kuyruk yöneticisi bir kuyruk paylaşım grubunun (QSG) parçasıysa, önce "Kuyruk paylaşım grubu ile ilgili önemli noktalar" sayfa 438 bölümünü okuyun.

Veri kümesi şifrelemesini veri kümesinden kaldırma

Bu örnek, CSQ1.LOGS.LOGCOPY1.DS001. V 9.1.5 SMDS ve sayfa kümeleri için eşdeğer bir işlem kullanabilirsiniz.

Örnek şunları varsayar:

- RACF SAF ' tır
- Veri kümesini kullanan kuyruk yöneticisi durduruldu
- Şifreleme anahtarı etiketi, soysal RACF tanıtımı CSQ1.LOGS.*

Aşağıdaki yordamı gerçekleştirin:

1. Verileri veri kümesinden bir yedek veri kümesine kopyalayın.
   a. Bir şifreleme anahtarı etiketiyle ilişkilendirilmemiş bir yedek veri kümesi tanımlayın.

      Not: + + EXTDCLASS + + veri kümesi için kullanmak istediğiniz genişletilmiş biçim veri sınıfının adıyla değiştirin.

```
//DEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* DEFINE UNENCRYPTED DATA SET                                 */
  /*-------------------------------------------------------------*/
  DEFINE CLUSTER                                  -
         (NAME(CSQ1.BAK.LOGS.LOGCOPY1.DS001)      -
         LINEAR                                   -
         SHAREOPTIONS(2 3)                        -
         MODEL(CSQ1.LOGS.LOGCOPY1.DS001)          -
         DATACLAS(++EXTDCLASS++))
/*
```

   b. Verileri özgün veri kümesinden yedeğe kopyalayın. Bu adım, verilerin şifresini çözer.

```
//COPY     EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* COPY DATA INTO UNENCRYPTED DATA SET                         */
  /*-------------------------------------------------------------*/
  REPRO INDATASET(CSQ1.LOGS.LOGCOPY1.DS001)          -
        OUTDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)
/*
```

   c. Özgün veri kümesini sil

```
//DELETE   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* DELETE ORIGINAL                                             */
  /*-------------------------------------------------------------*/
  DELETE ('CSQ1.LOGS.LOGCOPY1.DS001')
/*
```

   d. Yedeği özgün veri kümesi adıyla yeniden adlandırın. Veriler şifresiz kalır

```
//RENAME   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RENAME UNENCRYPTED DATA SET                                 */
  /*-------------------------------------------------------------*/
  ALTER CSQ1.BAK.LOGS.LOGCOPY1.DS001'                -
```

```
          NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001)
  ALTER 'CSQ1.BAK.LOGS.LOGCOPY1.DS001.*'                -
          NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001.*')
/*
```

2. İsteğe bağlı olarak, CSQ1.LOGS.* genel tanıtım.
3. İsteğe bağlı olarak, CSQ1.LOGS.* soysal tanıtımın şifresi çözüldü, soysal tanıtımla ilişkili DATAKEY ' yi kaldırmak için aşağıdaki komutu verin:

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

4. Aşağıdaki komutu vererek genel veri kümesi profillerini yenileyin:

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. Kuyruk yöneticisini yeniden başlatın.
6. Şifreleme anahtarı artık gerekmezse, anahtarı silin ve ilişkili RACF profilini CSFKEYS sınıfından silin.

Kuyruk paylaşım grubu ile ilgili önemli noktalar

Bir kuyruk paylaşım grubunun parçası olan bir kuyruk yöneticisi, veri kümesi şifrelemesini desteklemeyen bir IBM MQ for z/OS sürümüne geçirilecekse, QSG ' deki tüm kuyruk yöneticilerinin V 9.1.5 ve SMDS etkin günlük veri kümelerinin tümünün veri kümesi şifreleme ilkelerinin kaldırılması ve verilerinin şifresinin çözülmesi gerekir.

Bu, QSG 'nin tek bir üyesinin geriye doğru ya da QSG' nin tüm üyelerine ait olup olmadığına bakılmaksızın geçerlidir.

Aşağıdakiler aracılığıyla tam bir QSG kesintisi olmadan şifreleme ilkelerinin kaldırılmasını ve verilerin şifresinin çözülmesini elde edebilirsiniz:

1. “Veri kümesi şifrelemesini veri kümesinden kaldırma” sayfa 437içinde açıklanan işlemi kullanarak QSG ' deki her kuyruk yöneticisini kapatma, şifreleme ilkelerini kaldırma ve etkin günlüklerinden verilerin şifresini çözme.

   Kuyruk yöneticisinin geriye doğru geçişi yapılacaksa, sayfa kümesinin şifresi de şu anda çözülmelidir. Daha sonra kuyruk yöneticisini yeniden başlatın.

2. V 9.1.5 Şifreleme ilkelerinin kaldırılması ve her bir CF yapısının SMDS 'si için verilerin şifresinin çözülmesi:

   a. Komutun verilmesi

   ```
   RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name)
   ```

   SMDS ' ye kuyruk yöneticisi erişimini askıya almak için. Bu süre içinde, SMDS ile ilişkili paylaşılan kuyruklardaki veriler geçici olarak kullanılamaz.

   b. SMDS ' yi oluşturan her veri kümesi için “Veri kümesi şifrelemesini veri kümesinden kaldırma” sayfa 437 içindeki işlemi izleyin.

   c. Komutun verilmesi

   ```
   RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name)
   ```

   SMDS ' ye kuyruk yöneticisi erişimini sürdürmek için.

z/OS veri kümesi şifrelemesini, onu desteklemeyen bir kuyruk yöneticisiyle kullanma

Yanlışlıkla bir kuyruk yöneticisini veri kümesi şifrelemesini desteklemeyen bir IBM MQ for z/OS sürümüne geçirir ve şifreleme ilkelerini kaldırmayı unutursanız ve kuyruk yöneticisi veri kümesine erişmeye çalıştığında bir hata elde ettiğinizde verilerin şifresini çözersiniz.

Hata, veri kümesi tipine bağlıdır ve aşağıdaki çizelgede gösterilir.

Not: Bu hatalardan biri ya da birkaçı ortaya çıkarsa, etkilenen veri kümesi için “Veri kümesi şifrelemesini veri kümesinden kaldırma” sayfa 437 içinde açıklanan işlemleri izlemeniz gerekir. Bunlar, IBM MQ for z/OSsürümü değiştirilmeden gerçekleştirilebilir.

Veri kümesi	**Kuyruk yöneticisi z/OS veri kümesi şifrelemesini desteklemiyorsa hata oluştu**
Sayfa kümesi 0	Kuyruk yöneticisi başlangıcında 5C6-00C91400 olağandışı bitti
Sayfa kümeleri 1-99	MQRC 2193 Sayfa kümesine erişilirken "Sayfa kümesi hatası"; örneğin, MQPUT
Etkin günlük	Kuyruk yöneticisi başlangıcında 5C6-00E80084 olağandışı bitti
V 9.1.5 SMDS	IEC161I-122 iletisi "Veri kümesinin KEYLABEL değeri var, ancak kullanıcı uygulamanın şifrelemeyi işleyebileceğini belirtmedi". SMDS, AVAIL olarak işaretlendi (HATA).

İletilerin veri bütünlüğü

Veri bütünlüğünü korumak için, iletilerinize ilişkin ileti sindirmeleri ya da dijital imzalar sağlamak için çeşitli tiplerde kullanıcı çıkış programı türlerini kullanabilirsiniz.

Veri bütünlüğü

İletilerde veri bütünlüğünün uygulanması

TLS ' yi kullandığınızda, kuruluştaki veri bütünlüğü düzeyini CipherSpec tercihiniz belirler. IBM MQ Advanced Message Service (AMS) olanağını kullanırsanız, benzersiz bir ileti için bütünlüğü belirtebilirsiniz.

İleti çıkışlarında veri bütünlüğünün uygulanması

Bir ileti, bir kanalın gönderme bitişindeki bir ileti çıkışı tarafından dijital olarak imzalanabilir. Daha sonra, sayısal imza, iletinin kasıtlı olarak değiştirilip değiştirilmediğini saptamak için, bir kanalın alıcı ucundaki bir ileti çıkışı ile denetleyebilir.

Bazı koruma, dijital imza yerine ileti özeti kullanılarak sağlanabilir. Bir ileti özeti, gündelik ya da belirsiz kurcalamaya karşı etkili olabilir, ancak daha bilinçli bir kişinin iletiyi değiştirmesini ya da değiştirmesini ve bunun için tamamen yeni bir özet oluşturmasını engellememektedir. Bu, özellikle ileti özetini oluşturmak için kullanılan algoritmanın iyi bilinen bir algoritmaysa doğru olur.

Gönderme ve alma çıkışlarında veri bütünlüğünün uygulanması

Bir ileti kanalında, bir ileti çıkışı tüm iletiye erişimi olduğundan, ileti kanallarının bu hizmeti sağlamak için daha uygun olduğunu belirten bir ileti çıkar. Bir MQI kanalında, MQI çağrılarına ilişkin parametreler, korunması gereken uygulama verileri içerebilir ve bu korumayı yalnızca gönderme ve alma çıkışları sağlayabilir.

API çıkışında ya da API ' den geçiş çıkışındaki veri bütünlüğü uygulanıyor

İleti, gönderme uygulaması tarafından konulduğunda bir API ya da API geçiş çıkışı tarafından dijital olarak imzalanabilir. Daha sonra, iletinin kasıtlı olarak değiştirilip değiştirilmediğini algılamak için alıcı uygulama tarafından ileti alındığında, sayısal imza ikinci bir çıkış ile denetleyebilir.

Bazı koruma, dijital imza yerine ileti özeti kullanılarak sağlanabilir. Bir ileti özeti, gündelik ya da belirsiz kurcalamaya karşı etkili olabilir, ancak daha bilinçli bir kişinin iletiyi değiştirmesini ya da değiştirmesini ve bunun için tamamen yeni bir özet oluşturmasını engellememektedir. Bu özellikle, ileti özetini oluşturmak için kullanılan algoritmanın iyi bilinen bir algoritmaysa, bu özellikle doğrudur.

Ek bilgi

Veri bütünlüğünün sağlanmasına ilişkin ek bilgi için “CipherSpecs' in etkinleştirilmesi” sayfa 402 üzerindeki bölüme bakın.

İlgili görevler

İki kuyruk yöneticisinin TLS ' yi kullanarak bağlanması

İstemcinin kuyruk yöneticisine güvenli bir şekilde bağlanması

Denetleme

Olay iletilerini kullanarak, güvenlik izinsiz girişlerinin ya da izinsiz girişlerin denenmesini denetleyebilirsiniz. Ayrıca, IBM MQ Explorerkomutunu kullanarak sisteminizin güvenliğini denetleyebilirsiniz.

Bir kuyruk yöneticisine bağlanma ya da bir kuyruğa ileti koyma gibi yetkisiz işlemleri gerçekleştirme girişimlerini saptamak için, kuyruk yöneticilerinizin ürettiği olay iletilerine, özellikle de yetki olay iletilerine bakın. Kuyruk yöneticisi olay iletilerine ilişkin ek bilgi için Kuyruk yöneticisi olaylarıbaşlıklı konuya bakın ve genel olarak olay izleme hakkında daha fazla bilgi için Olay izlemekonusuna bakın.

Kümeleri güvenli tutma

Kuyruklara katılan kuyruk yöneticilerine ya da küme kuyruklarına ileti yerleştirmeyi yetkilendirin ya da engelleyin. Kuyruk yöneticisini bir küme bırakması için zorlayın. Kümeler için TLS ' yi yapılandırırken dikkat edilmesi gereken bazı noktalar dikkate alın.

İzinsiz kuyruk yöneticilerinin ileti göndermesi durduruluyor

Yetkisiz kuyruk yöneticilerinin, kanal güvenliği çıkışı kullanarak kuyruk yöneticinize ileti göndermesini engelleyin.

Başlamadan önce

Kümelemenin güvenlik çıkışlarının çalışma yolunda bir etkisi yoktur. Dağıtılmış bir kuyruklama ortamında, bir kuyruk yöneticisine erişimi aynı şekilde kısıtlayabilirsiniz.

Bu görev hakkında

Seçilen kuyruk yöneticilerinin kuyruk yöneticinize ileti göndermesini engelle:

Yordam

1. CLUSTRVR kanal tanımında bir kanal güvenlik çıkış programı tanımlayın.
2. Kuyruk alıcı kanalınıza ileti göndermeye çalışan kuyruk yöneticilerini doğrulayan bir program yazın ve yetki verilmediyse, bu kanalların erişimini reddeder.

Sonraki adım

Kanal güvenlik çıkış programları MCA başlatma ve sonlandırma ile çağrılır.

İzinsiz kuyruk yöneticilerinin kuyruklarınıza ileti yerleştirmesini durdurma

Yetkisiz kuyruk yöneticilerinin kuyruklarınıza ileti koymasını durdurmak için, küme alıcı kanalındaki kanal put authority özniteliğini kullanın. Authorize a remote queue manager by checking the user ID in the message using RACF on z/OS, or the OAM on other platforms.

Bu görev hakkında

Kuyruklara erişimi denetlemek için bir platformun güvenlik olanaklarını ve IBM MQ içindeki erişim denetimi mekanizmasını kullanın.

Yordam

1. Belirli kuyruk yöneticilerinin bir kuyruğa ileti yerleştirmesini önlemek için, platformunuzda bulunan güvenlik olanaklarını kullanın.

   Örneğin:

   - IBM MQ for z/OSüzerindekiRACF ya da diğer dış güvenlik yöneticileri
   - Diğer platformlardaki nesne yetkisi yöneticisi (OAM).
2. Use the put authority, PUTAUT, attribute on the CLUSRCVR channel definition.

   PUTAUT özniteliği, bir kuyruğa ileti koyma yetkisi oluşturmak için hangi kullanıcı tanıtıcılarının kullanılacağını belirtmenize olanak tanır.

   PUTUUT öznitelideki seçenekler şunlardır:

   DEF
   Varsayılan kullanıcı kimliğini kullanın. On z/OS, the check might involve using both the user ID received from the network and that derived from MCAUSER.

   CTX
   İletiyle ilişkilendirilen bağlam bilgilerinde kullanıcı kimliğini kullanın. On z/OS the check might involve using either the user ID received from the network, or that derived from MCAUSER, or both. Bağlantı güvenilir ve doğrulanmışsa bu seçeneği kullanın.

   ONLYMCA (yalnızca z/OS)
   DEF ' ye göre, ancak ağdan alınan herhangi bir kullanıcı kimliği kullanılmaz. Bağlantıya güvenilmiyorsa bu seçeneği kullanın. Yalnızca, üzerinde MCAUSERiçin tanımlanan belirli bir işlem kümesine izin vermek istiyorsunuz.

   ALTMCA (yalnızca z/OS)
   CTXiçin olduğu gibi, ağdan alınan herhangi bir kullanıcı kimliği kullanılmaz.

Uzak küme kuyruklarına ileti koyma yetkisi

On z/OS set up authorization to put to a cluster queue using RACF. Diğer platformlarda, kuyruk yöneticilerine bağlanma ve bu kuyruk yöneticilerindeki kuyruklara bağlanmak için erişim yetkisi verin.

Bu görev hakkında

Varsayılan davranış, SYSTEM.CLUSTER.TRANSMIT.QUEUE' a karşı erişim denetiminin gerçekleştirilmesine neden olur. Birden çok iletim kuyruğu kullansanız da, bu davranışın geçerli olduğunu unutmayın.

The specific behavior described in this topic applies only when you have configured the **ClusterQueueAccessControl** attribute in the qm.ini file to be *RQMAdı*, as described in the Güvenlik stanzası topic, and restarted the queue manager.

Yordam

- z/OSiçin aşağıdaki komutları verin:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- UNIX, Linux, and Windows sistemleri için aşağıdaki komutları verin:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

- IBM iiçin aşağıdaki komutları verin:

```
GRTMQMAUT OBJ(' QMgrName ') OBJTYPE(*MQM) USER(GroupName) AUT(*CONNECT)
GRTMQMAUT OBJ(' QueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

Kullanıcı iletileri yalnızca belirtilen küme kuyruğuna ve diğer küme kuyruklarına koyabilir.

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.

GroupName
Verilecek erişim izni verilecek grubun adı.

QueueName
Yetkilerin değiştirileceği kuyruğun ya da genel profilin adı.

Sonraki adım

Bir iletiyi bir küme kuyruğuna koyduğunuzda bir yanıt kuyruğu belirlerseniz, alıcı uygulamanın yanıtı göndermek için yetkisi olmalıdır. Bu yetkiyi, "İletileri uzak bir küme kuyruğuna koyma yetkisi verilmesi" sayfa 381içindeki yönergeleri izleyerek ayarlayın.

İlgili kavramlar
qm.iniiçindeki güvenlik stanzası

Bir kümeye katılan kuyruk yöneticilerinin engellenmesi

Bir düzenek kuyruk yöneticisi bir kümeye katılırsa, bir kümeyi almasını engellemenin zorlaştığı bir kümeye katılıyorsa, bu bir küme yöneticisi tarafından alınmasını engelleyebilir.

Yordam

Yalnızca belirli yetkili kuyruk yöneticilerinin bir kümeye katıldığınızdan emin olmak istiyorsanız, şu üç teknikten oluşan bir seçiminiz vardır:

- Kanal kimlik denetimi kayıtlarını kullanarak, küme kanalı bağlantısını, uzak IP adresini, uzak kuyruk yöneticisi adını ya da uzak sistem tarafından sağlanan TLS Ayırt Edici Adı 'nı temel alarak engelleyebilirsiniz.
- Yetkisiz kuyruk yöneticilerinin SYSTEM.CLUSTER.COMMAND.QUEUE' a yazmasını önlemek için bir çıkış programı yazın. Do not restrict access to SYSTEM.CLUSTER.COMMAND.QUEUE such that no queue manager can write to it, or you would prevent any queue manager from joining the cluster.
- CLUSRCVR kanal tanımlamasındaki bir güvenlik çıkış programı.

Küme kanallarındaki güvenlik çıkışları

Küme kanallarında güvenlik çıkışlarını kullanırken dikkat edilmesi gereken noktalar.

Bu görev hakkında

Bir küme gönderici kanalı ilk kez başlatıldığında, sistem yöneticisi tarafından el ile tanımlanan öznitelikleri kullanır. Kanal durdurulduğunda ve yeniden başlatıldığında, öznitelikleri karşılık gelen küme alıcı kanalı tanımlamasından alır. Özgün kümenin gönderici kanal tanımlamasının üzerine, SecurityExit özniteliği de dahil olmak üzere yeni öznitelikler yazılır.

Yordam

1. Bir kanal için hem küme gönderici ucunda hem de küme alıcı ucunun üzerinde bir güvenlik çıkışı tanımlamalısınız.

   Güvenlik çıkışı adı, küme alıcı tanımından gönderilse de, ilk bağlantı, bir güvenlik çıkışı tokalaşmasıyla yapılmalıdır.
2. Güvenlik çıkışındaki MQCXP yapısındaki `PartnerName` (PartnerName) öğesini doğrulayın.

   Çıkışta, kanal yalnızca iş ortağı kuyruk yöneticisi yetkilendirilmişse başlatılmasına izin vermelidir.
3. Günlük nesnesi tanımlamasındaki güvenlik çıkışını, günlük nesnesi tanımlanacak şekilde tasarlayın.
4. Bunu gönderen olarak tasarladığınızda, hiçbir güvenlik denetimi gerçekleştirilmediği için, güvenlik çıkışı olmayan yetkisiz bir kuyruk yöneticisi kümeye katılabilir.

   Not until the channel is stopped and restarted can the SCYEXIT name be sent over from the cluster-receiver definition and full security checks made.
5. Şu anda kullanımda olan küme gönderici kanal tanımlamasını görüntülemek için şu komutu kullanın:

   ```
   DISPLAY CLUSQMGR( queue manager ) ALL
   ```

   Komut, küme alıcı-alıcı tanımlamasından gönderilen öznitelikleri görüntüler.
6. Özgün tanımlamayı görüntülemek için şu komutu kullanın:

   ```
   DISPLAY CHANNEL( channel name ) ALL
   ```
7. Kuyruk yöneticileri farklı platformlarda yer alıyorsa, küme gönderen kuyruk yöneticisininde, bir kanal otomatik tanımlama çıkışı (CHADEXIT) tanımlamanız gerekebilir.

   Use the channel auto-definition exit to set the `SecurityExit` attribute to an appropriate format for the target platform.
8. Güvenlik çıkışını konuşlandırın ve yapılandırın.

   z/OS

   Güvenlik çıkışı yükleme modülünün, kanal başlatıcı adres alanı yordamında `CSQXLIB DD` deyiminde belirtilen veri kümesinde olması gerekir.

   Windows, UNIX and Linux sistemleri

   - Güvenlik çıkışı dinamik bağlantı kitaplığı, kanal tanımlamasının SCYEXIT özniteliğinde belirtilen yolda yer almalıdır.
   - Kanal otomatik tanımlama çıkışı dinamik bağlantı kitaplığı, kuyruk yöneticisi tanımlamasının CHADEXIT öznitelemesinde belirtilen yolda olmalıdır.

İstenmeyen kuyruk yöneticilerini kümeden ayrılmaya zorlama

İstenmeyen bir kuyruk yöneticisini, tam havuz kuyruğu yöneticisinde `RESET CLUSTER` komutunu vererek kümeden ayrılmaya zorlar.

Bu görev hakkında

İstenmeyen bir kuyruk yöneticisini kümeden ayrılmaya zorlayabilirsiniz. Örneğin, bir kuyruk yöneticisi silinir, ancak küme alıcı kanalları kümede tanımlanmaya devam eder. Toparlansan iyi olur.

Yalnızca tam havuz kuyruğu yöneticilerinin bir kümeden kuyruk yöneticisini çıkarma yetkisi vardır.

Not: RESET CLUSTER komutu kullanıldığında bir kuyruk yöneticisi kümeden zorla kaldırılmasına rağmen, RESET CLUSTER ' in tek başına kullanılması kuyruk yöneticisinin daha sonra kümeye yeniden katılmasını engellemez. Kuyruk yöneticisinin kümeye yeniden katılmamasını sağlamak için “Bir kümeye katılan kuyruk yöneticilerinin engellenmesi” sayfa 442içinde açıklanan adımları izleyin.

OSLO Kümeden NORWAYkuyruk yöneticisini çıkarmak için aşağıdaki yordamı izleyin:

Yordam

1. Tam havuz kuyruğu yöneticisinde şu komutu verin:

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. Diğer bir seçenek olarak, komutta QMNAME yerine QMID kullanın:

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

Not: QMID bir dizedir; bu nedenle qmid değeri tek tırnak işareti ile çevrelenmelidir; örneğin, QMID('FR01_2019-07-15_14.42.42').

Sonuçlar

Zorlamalı olarak kaldırılan kuyruk yöneticisi değişmez; yerel küme tanımlamaları kümede olduğunu gösterir. Diğer tüm kuyruk yöneticilerindeki tanımlamalar kümede gösterilmez.

Kuyruk yöneticilerinin ileti alma engellenmesi

Bir küme kuyruk yöneticisinin çıkış programlarını kullanarak, alma yetkisi olmayan iletileri almasını önleyebilirsiniz.

Bu görev hakkında

Kuyruk tanımlamasından kümenin üyesi olan bir kuyruk yöneticisini durdurmak zordur. Bir düzenbaz kuyruk yöneticisinin bir kümeye katıldığı ve kümedeki kuyruklardan birinin kendi eşgörünümünü tanımladığı bir tehlike vardır. Artık alma yetkisinin olmadığı iletiler alabilir. Kuyruk yöneticisinin ileti almasını önlemek için, yordamda belirtilen aşağıdaki seçeneklerden birini kullanın.

Yordam

- Her bir küme gönderici kanalına bir kanal çıkış programı. Çıkış programı, iletilerin gönderileceği hedef kuyruk yöneticisinin uygunluğundan emin olmak için bağlantı adını kullanır.
- Hedef kuyruğun ve kuyruk yöneticisinin iletilerin gönderileceği uygunluğun belirlenmesine ilişkin hedef kayıtları kullanan bir küme iş yükü çıkış programı.

SSL/TLS ve kümeler

Kümeler için TLS yapılandırılırken, bir CLUSRCVR kanal tanımının, otomatik olarak tanımlanmış bir CLUSSDR kanalı olarak diğer kuyruk yöneticilerine yayılırdığı dikkate alın. Bir CLUSTRVR kanalı TLS kullanıyorsa, kanalı kullanarak iletişim kuran tüm kuyruk yöneticilerindeki TLS ' yi yapılandırmanız gerekir.

TLS hakkında daha fazla bilgi için bkz. “IBM MQiçinde TLS güvenlik iletişim kuralları” sayfa 22. Bu öneri, genellikle küme kanallarına uygulanabilir, ancak aşağıdakine özel bir önem vermek isteyebilirsiniz:

Bir IBM MQ kümesinde, belirli bir CLUSRCVR kanalı tanımlaması sık sık, otomatik olarak tanımlanmış bir CLUSSDRiçine dönüştürüldüğü diğer kuyruk yöneticilerine yayılır. Daha sonra otomatik olarak tanımlanan CLUSSDR , CLUSRCVR' e bir kanal başlatmak için kullanılır. CLUSRCVR TLS bağlanırlığı için yapılandırılmışsa, aşağıdaki noktalar geçerlidir:

- Bu CLUSRCVR ile iletişim kurmak isteyen tüm kuyruk yöneticilerinin TLS desteğine erişimleri olmalıdır. Bu TLS hükmü, kanal için CipherSpec ' yi desteklemelidir.
- Otomatik olarak tanımlanan küme gönderen kanallarının geçirildiği farklı kuyruk yöneticilerinin her biri farklı bir ayırt edici ada sahip olacak. If distinguished name peer checking is to be used on the CLUSRCVR it must be set up so all of the distinguished names that can be received are successfully matched.

Örneğin, belirli bir CLUSRCVR' a bağlanacak, küme gönderen kanallarını barınabilecek tüm kuyruk yöneticilerinin sertifikalara sahip olduğunu varsayariz. Let us also assume that the distinguished names in all of these certificates define the country as UK, organization as IBM, the organization unit as IBM MQ Development, and all have common names in the form DEVT.QMnnn, where nnn is numeric.

Bu durumda, CLUSRCVR üzerindeki SSLPEER değeri C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM* , gerekli tüm küme gönderici kanallarının başarılı bir şekilde bağlanmasına izin verir, ancak istenmeyen küme gönderici kanallarının bağlanmasını önler.

- Özel CipherSpec dizgileri kullanılırsa, özel dizgi biçimlerinin tüm altyapılarda kullanılmasına izin verilmediğini unutmayın. Bunun bir örneği, CipherSpec dizgisi RC4_SHA_US ' in IBM i üzerinde 05 değerine sahip olması, ancak UNIX, Linux ya da Windows sistemlerinde geçerli bir belirtim olmamasıdır. Bir CLUSRCVRüzerinde özel SSLCIPH değiştirgeleri kullanılırsa, sonuçta elde edilen tüm otomatik tanımlı küme gönderen kanalları, temeldeki TLS desteğinin bu CipherSpec ' i uyguladığı ve özel değerle belirtilebilecek altyapılarda bulunmalıdır. Kümeniz boyunca anlaşılacak olan SSLCIPH parametresi için bir değer seçemezseniz, bu parametreyi, kullanılmakta olan platformların anlayacağı bir yere değiştirmek için bir kanal otomatik tanımlama çıkışa gereksinim dumanız gerekir. Mümkün olan yerlerde metinli CipherSpec dizgillerini kullanın (örneğin, TLS_RSA_WITH_AES_128_CBC_SHA).

Bir SSLCRLNL parametresi, tek bir kuyruk yöneticisine uygulanır ve bir küme içindeki diğer kuyruk yöneticilerine yayılmaz.

Kümelenmiş kuyruk yöneticilerinin ve kanalların SSL/TLS ' ye büyütülmesi

Upgrade the cluster channels one at a time, changing all the CLUSRCVR channels before the CLUSSDR channels.

Başlamadan önce

Aşağıdaki noktaları göz önünde bulundurun; bunlar, bir küme için CipherSpec seçiminizi etkileyebileceğinden aşağıdaki noktaları göz önünde bulundurun:

- Bazı CipherSpecs , tüm platformlarda kullanılamaz. Kümedeki tüm kuyruk yöneticileri tarafından desteklenen bir CipherSpec seçmeye özen gösteriniz.
- Bazı CipherSpecs , geçerli IBM MQ yayınında yeni olabilir ve daha eski yayınlarda desteklenmeyebilir. Farklı MQ yayınlarında çalışan kuyruk yöneticilerini içeren bir küme, her yayın düzeyinde desteklenen CipherSpecs ' i kullanabilecektir.

  Bir küme içinde yeni bir CipherSpec kullanmak için, önce tüm küme kuyruğu yöneticilerini yürürlükteki yayına geçirmeniz gerekir.
- Bazı CipherSpecs , özellikle Eliptik Eğri Şifrelemesi kullanan belirli bir sayısal sertifika tipinin kullanılmasını gerektirir.

Uyarı: Bir kümenin parçası olarak birlikte katılmak istediğiniz kuyruk yöneticilerindeki Eliptik Eğri imzalı sertifikalar ve RSA imzalı sertifikaların bir karışımının kullanılması mümkün değildir.

Bir kümedeki kuyruk yöneticilerinin tümü RSA onaylı sertifikalar kullanmalı ya da her ikisinin bir karışımının değil, tüm EC imzalı sertifikalarını kullanmalıdır.

Ek bilgi için “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42 başlıklı konuya bakın.

Kümedeki tüm kuyruk yöneticilerini IBM MQ V8 düzeyine ya da daha yüksek bir düzeye yükselt, bu düzeylerde değilse, daha yüksek bir değer elde edin. TLS ' nin her birinden çalışabilmesi için sertifikaları ve anahtarları dağıtın.

Tom 'u yükseltmek ya da ANY_TLS12 CipherSpecs'u kullanmak istiyorsanız, kümedeki tüm kuyruk yöneticilerini IBM MQ 9.1.2 ' e ya da daha yüksek bir sürüme yükseltmeniz gerekir.

Büyütme yapmak ya da diğer diğer adı CipherSpecs (ANY_TLS13, ANY_TLS12, ANY_TLS12_OR_HIGHERvb.) kullanmak istiyorsanız, kümedeki tüm kuyruk yöneticilerini IBM MQ 9.1.4 ya da daha yüksek bir sürüme yükseltmeniz gerekir.

Bu görev hakkında

CLUSSDR kanallarından önce CLUSRCVR kanallarını değiştirin.

Yordam

1. CLUSRCVR kanallarını istediğiniz sırayla TLS 'ye değiştirin, bir kerede bir CLUSRCVR ' yi değiştirin ve sonraki işlemi değiştirmeden önce kümeden geçebilmesini sağlayın.

   Önemli: Yürürlükteki kanal için yapılan değişiklikler küme boyunca dağıtılıncaya kadar, ters yolu değiştirmediğinizden emin olun.
2. İsteğe bağlı: Tüm el ile CLUSSDR kanallarını TLS ' ye değiştirin.

   REFRESH CLUSTER komutunu REPOS(YES) seçeneğiyle birlikte kullanmadığınız sürece, bu, kümenin işleyişi üzerinde herhangi bir etkiye sahip değildir.

   Not: Büyük kümeler için, **REFRESH CLUSTER** komutunun kullanımı devam ederken kümeyi kesintiye uğratabilir ve bundan sonra 27 gün aralıklarla küme nesneleri, ilgili tüm kuyruk yöneticilerine otomatik olarak durum güncellemeleri gönderdiğinde, bu işlem yine 27 gün aralıklarla kesintiye uğrayabilir. Bkz. Büyük bir kümede yenilenme, kümenin performansını ve kullanılabilirliğini etkileyebilir.
3. Yeni güvenlik yapılandırmasının küme boyunca yayıldığından emin olmak için DISPLAY CLAUQMGR komutunu kullanın.
4. TLS ' yi kullanmak için kanalları yeniden başlatın ve REFRESH SECURITY komutunu (SSL) çalıştırın.

İlgili kavramlar

“CipherSpecs' in etkinleştirilmesi” sayfa 402
Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

“IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42
Bu konuda, IBM MQiçinde CipherSpecs ile dijital sertifikalar arasındaki ilişkiyi özetleyerek güvenlik ilkeniz için uygun CipherSpecs ve dijital sertifikaların nasıl seçileceğine ilişkin bilgiler sağlanır.

İlgili bilgiler

Kümeleme: REFRESH CLUSTER en iyi uygulamaları kullanma

Kümelenmiş kuyruk yöneticileri ve kanallar üzerinde SSL/TLS devre dışı bırakılıyor

TLS ' yi kapatmak için, SSLCIPH parametresini ' ' olarak ayarlayın. Küme kanallarında TLS ' yi tek tek devre dışı bırakın, küme gönderen kanallarından önce tüm küme alıcı kanallarını değiştirin.

Bu görev hakkında

Bir defada bir küme günlük nesnesi kanalını değiştirin ve bir sonraki değiştirmeden önce kümedeki değişikliklerin küme üzerinden akmasına izin verin.

Önemli: Yürürlükteki kanala ilişkin değişiklikler küme boyunca dağıtılıncaya kadar, ters yolu değiştirmediğinizden emin olun.

Yordam

1. SSLCIPH parametresinin değerini ' ' olarak ayarlayın, tek tırnak işaretindeki boş bir dizgi

   IBM i ya da IBM i üzerinde *NONE .

   Küme alıcı kanallarında TLS ' yi istediğiniz herhangi bir sırayla kapatabilirsiniz.

   TLS ' yi etkin bıraktığınız kanallar üzerinde ters yönde yapılan değişikliklerin akışını not edin.
2. Yeni değerin, **DISPLAY CLUSQMGR(*)** ALLkomutunu kullanarak diğer tüm kuyruk yöneticilerine yansıtıldığını doğrulayın.
3. Tüm el ile küme gönderen kanallarında TLS ' yi kapatın.

REFRESH CLUSTER komutunu REPOS （YES）seçeneğiyle birlikte kullanmadığınız sürece, bu işlem kümenin işleyişi üzerinde herhangi bir etkiye sahip değildir.

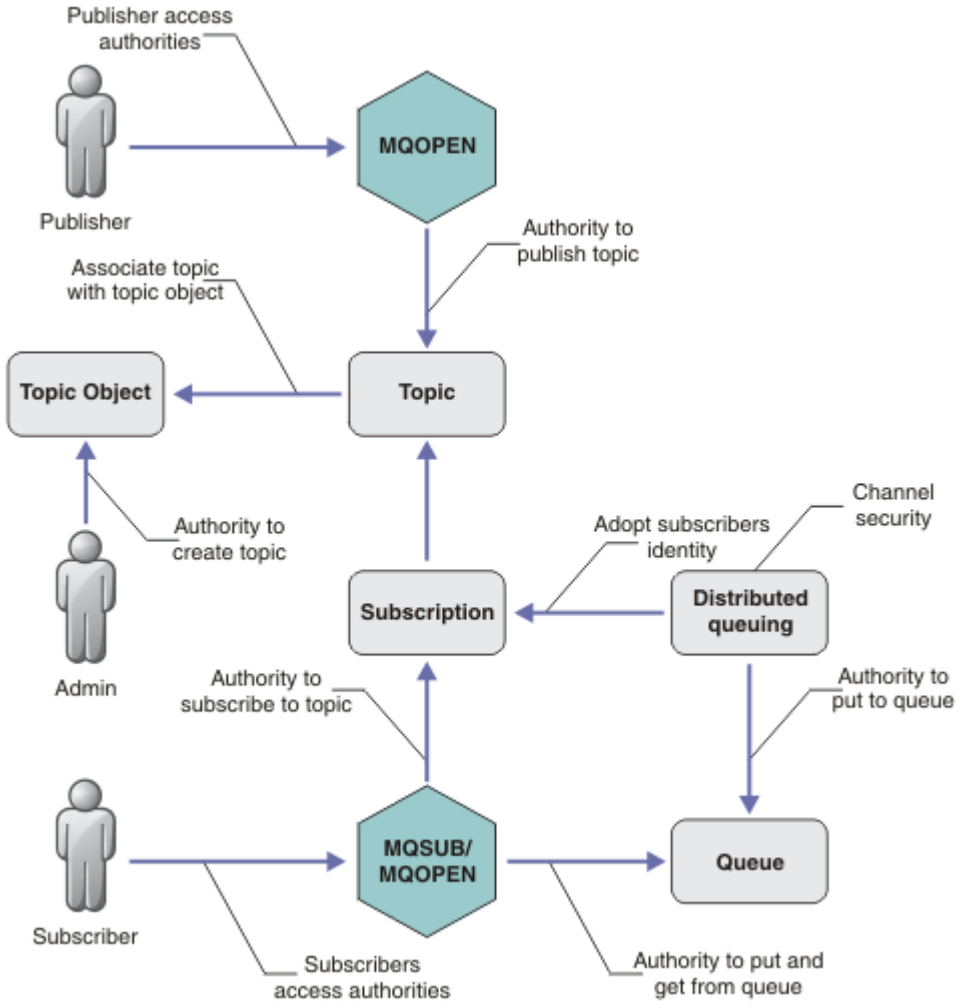
Büyük kümeler için, **REFRESH CLUSTER** komutunun kullanımı devam ederken kümeyi kesintiye uğratabilir ve bundan sonra düzenli aralıklarla küme nesneleri, ilgili tüm kuyruk yöneticilerine otomatik olarak durum güncellemeleri gönderdiğinde, bu işlemi düzenli aralıklarla yeniden yapabilirsiniz. Ek bilgi için Büyük bir kümede yenilenme, kümenin performansını ve kullanılabilirliğini olumsuz etkileyebilir konusuna bakın.

4. Küme gönderen kanallarını durdurun ve yeniden başlatın.

Güvenliği yayınla/abone ol

yayınlama/abone olma içinde yer alan bileşenler ve etkileşimler, takip eden daha ayrıntılı açıklamalara ve örneklere giriş olarak tanımlanır.

Bir konuya yayınlanırken ve bir konuya abone olmak için bir dizi bileşen vardır. Aralarındaki bazı güvenlik ilişkileri Şekil 22 sayfa 447 ' de gösterilir ve aşağıdaki örnekte anlatılır.



Şekil 22. Çeşitli bileşenler arasında güvenlik ilişkilerini yayınlama/abone olma

Konular

Konular konu dizgileriyle tanıtılır ve genellikle ağaçlara düzenlenir, bkz. Konu ağaçları. Konuya erişimi denetlemek için bir konuyu konu nesnesiyle ilişkilendirmeniz gerekir. “Konu güvenlik modeli” sayfa 449 , konuları konu nesnelerini kullanarak nasıl güvenli hale getirdiğinizi açıklar.

Denetim konusu nesneleri

You can control who has access to a topic, and for what purpose, by using the command **setmqaut** with a list of administrative topic objects. Örnekler, “Bir konuya abone olmak için kullanıcıya erişim izni ver” sayfa 454 ve “Bir konuyla ilgili olarak yayınlamak için kullanıcıya erişim izni ver” sayfa 461örneklerine bakın. z/OS z/OSüzerindeki konu nesnelerine erişimi denetlemek için bkz. Konu güvenliğine ilişkin tanıtımlar.

Abonelikler

Yayınların konu dizgileriyle eşleşmek üzere genel arama karakterleri içerebilen bir konu dizgisi sağlayan abonelik yaratarak bir ya da daha fazla konuya abone olun. Ek ayrıntılar için aşağıdaki başlara bakın:

Bir konu nesnesini kullanarak abone olma

“Konu nesnesi adı kullanılarak abone olunması” sayfa 450

Konu kullanarak abone olma

“Konu düğümünün var olmadığı bir konu dizesini kullanarak abone olma” sayfa 451

Genel arama karakterleri içeren bir konu kullanarak abone olma

“Genel arama karakterleri içeren bir konu dizesini kullanarak abone olma” sayfa 452

Abonelik, abonenin kimliği ve yayınların yerleştirileceği hedef kuyruğun kimliği hakkında bilgi içerir. Ayrıca, yayının hedef kuyruğa nasıl yerleştirileceği ile ilgili bilgiler de içerir.

Ayrıca, hangi abonelerin belirli konulara abone olma yetkisi olduğunu tanımlarken, abonelikleri tek bir abone tarafından sınırlandırabilirsiniz. Ayrıca, yayınlar hedef kuyruğa yerleştirildiğinde, kuyruk yöneticisi tarafından aboneye ilişkin bilgilerin ne olduğunu da denetleyebilirsiniz. Bkz. “Abonelik güvenliği” sayfa 467.

Kuyruklar

Hedef kuyruk, güvenli kılmak için önemli bir kuyruğdur. Bu, aboneye yereldir ve abonelikle eşleşen yayınların üzerine yerleştirilir. İki perspektiften hedef kuyruğa erişimi göz önünde bulunduramanız gerekir:

1. Hedef kuyruğa bir yayın yerleştiriyor.
2. Yayının hedef kuyruğundan çıkarılıyor.

Kuyruk yöneticisi, abonenin sağladığı bir kimliği kullanarak bir yayını hedef kuyruğa yerleştirir. Yayın alma görevi için yetkilendirilmiş olan abone ya da bir program, iletileri kuyruktan çıkarır. Bkz. “Hedef kuyruklara yetki” sayfa 452.

Herhangi bir konu nesnesi diğer adı yok, ancak bir konu nesnesinin diğer adı olarak bir diğer ad kuyruğu kullanabilirsiniz. Bunu yapmazsanız, yayınlama ya da abone olma konusunu kullanma yetkisini denetleyerek, kuyruk yöneticisi, kuyruğu kullanma yetkisini denetler.

“Kuyruk yöneticileri arasında güvenliği yayınla/abone ol” sayfa 468

Bir konuyu yayınlama ya da bir konuyu abone olma izniniz, yerel kimlikler ve yetkiler kullanılarak yerel kuyruk yöneticisininde denetlenir. Yetki, konunun tanımlanıp tanımlanmadığına ya da tanımlanıp tanımlanmadığına bağlı değildir. Sonuç olarak, kümelenmiş konular kullanıldığında bir kümedeki her kuyruk yöneticisinde konu yetkilendirmesi gerçekleştirmeniz gerekir.

Not: Konulara ilişkin güvenlik modeli, kuyruklar için güvenlik modelinden farklıdır. Her kümelenmiş kuyruk için yerel olarak bir kuyruk diğer adı tanımlayarak, kuyruklar için aynı sonucu elde edebilirsiniz.

Kuyruk yöneticileri, abonelikleri bir kümede değiş tokuş eder. Çoğu IBM MQ küme yapılandırmasında, kanallar, kanal işleminin yetkisini kullanarak iletileri hedef kuyruklara yerleştirmek için PUTAUT=DEF ile yapılandırılır. You can modify the channel configuration to use PUTAUT=CTX to require the subscribing user to have authority to propagate a subscription onto another queue manager in a cluster.

“Kuyruk yöneticileri arasında güvenliği yayınla/abone ol” sayfa 468 , abonelikleri kümedeki diğer sunuculara dağıtmaya kimlerin izin verildiğini denetlemek için kanal tanımlarınızın nasıl değiştirileceğini açıklar.

Yetkilendirme

Yalnızca kuyruklar ve diğer nesneler gibi konu nesnelerine yetkilendirme uygulayabilirsiniz. Yalnızca konulara uygulayabileceğiniz üç yetkilendirme işlemi vardır: `pub`, `subve resume` . Ayrıntılar, Farklı nesne tiplerine ilişkin yetkilerin belirtilmesibaşlıklı konu altında açıklanmıştır.

İşlev çağrıları

Yayınlama ve abone olma programlarında, kuyruğa alınmış programlardaki gibi, nesneler açıldığında, yaratıldığında, değiştirildiğinde ya da silindiğinde yetkilendirme denetimleri yapılır. Yayınları koymak ve almak için `MQPUT` ya da `MQGET` MQI çağrıları yapıldığında denetimler yapılmaz.

Bir konuyu yayınlamak için, konu üzerinde bir `MQOPEN` işlemi gerçekleştirin; bu işlem, yetkilendirme denetimlerini gerçekleştirir. Hiçbir yetki denetimi yapılmayan `MQPUT` komutunu kullanarak, iletileri konu tanıtıcısında yayınlayın.

Bir konuya abone olmak için, genellikle aboneliği yaratmak ya da sürdürmek için bir `MQSUB` komutu, ayrıca yayınları almak için hedef kuyruğu da açabilirsiniz. Diğer bir seçenek olarak, hedef kuyruğu açmak için ayrı bir `MQOPEN` işlemi gerçekleştirin ve daha sonra, aboneliği yaratmak ya da sürdürmek için `MQSUB` işlemini gerçekleştirin.

Hangi arama kullanırsanız kullanın, kuyruk yöneticisi konuya abone olabileceğiniz ve sonuçtaki yayınları hedef kuyruktan alabileceğiniz denetimlerini denetler. Hedef kuyruk yönetilmeyen ise, yetki denetimleri de kuyruk yöneticisinin hedef kuyruğun yayınlarını yerleştirebilmesini sağlar. Bu, eşleşen bir abonelikten benimsediği kimliği kullanır. Kuyruk yöneticisinin, yayınları her zaman yönetilen hedef kuyruklara yerleştirebildiğinden emin olun.

Roller

Kullanıcılar, yayınlama/abone olma uygulamalarının çalıştırılmasındaki dört rolde yer almaklardır:

1. Yayıncı
2. Abone
3. Konu yöneticisi
4. IBM MQ Administrator - member of group `mqm`

Yayınlama, abone olma ve konu yönetimi rollerine karşılık gelen uygun yetkiler içeren grupları tanımlayın. Daha sonra, belirli yayınlama ve abone olma görevlerini gerçekleştirmek için bu gruplara birincil kullanıcıları yetkilendirebilirsiniz.

Ayrıca, yayınları ve abonelikleri taşımaktan sorumlu olan kuyrukların ve kanalların yöneticisine yönetimle ilgili operasyon yetkilerini de genişletmeniz gerekir.

Konu güvenlik modeli

Yalnızca tanımlanmış konu nesnelerinin ilişkili güvenlik öznitelikleri olabilir. Konu nesnelerine ilişkin açıklamalar için Denetim konusu nesneleribaşlıklı konuya bakın. Güvenlik öznitelikleri, her bir konu nesnesinde bir abone olma ya da yayınlama işlemi gerçekleştirme yetkisine sahip bir kullanıcı kimliği ya da güvenlik grubunun izin verilip verilmediğini belirler.

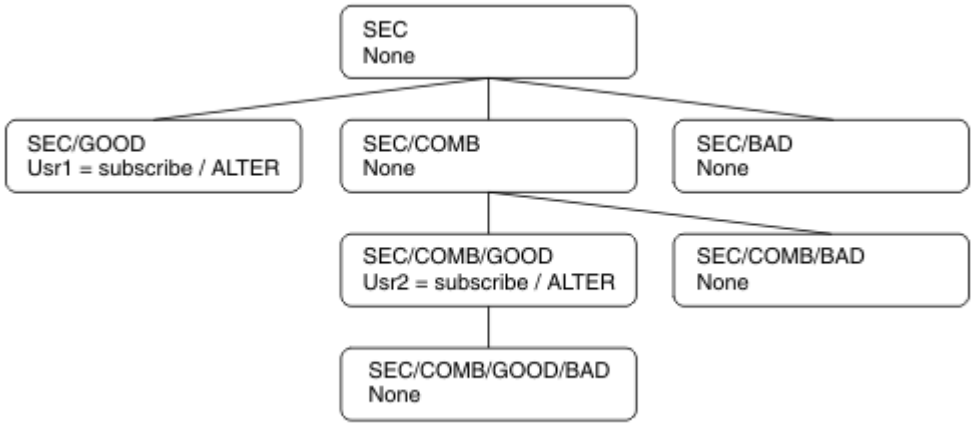
Güvenlik öznitelikleri, konu ağacındaki uygun denetim düğüyle ilişkilendirilir. Bir abonelik ya da yayınlama işlemi sırasında belirli bir kullanıcı kimliği için bir yetki denetimi yapıldığında, verilen yetki, ilişkili konu ağacı düğümünün güvenlik özniteliklerine dayanır.

Güvenlik öznitelikleri, belirli bir işletim sistemi kullanıcı kimliğinin ya da güvenlik grubunun konu nesnesine hangi yetki vereceğini gösteren bir erişim denetleme listedir.

Aşağıdaki örnekte, konu nesnelerinin güvenlik öznitelikleriyle tanımlanmış olduğu ya da gösterilen yetkilerin olduğu bir örnek olarak göz önünde bulundurun:

Çizelge 80. Örnek konu nesnesi yetkileri			
Konu adı	**Konu dizesi**	**Yetkiler- z/ OSdeğil**	**z/OS yetkileri**
SECROOT	SEC	Yok	Yok
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Yok	Yok HLQ.SUBSCRIBE.SECBAD
SECCOMB	SEC/COMB	Yok	Yok HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	Yok	Yok HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	Yok	Yok HLQ.SUBSCRIBE.SECCOMBN

Her düğümde ilişkili güvenlik özniteliklerine sahip olan konu ağacı aşağıdaki gibi gösterilebilir:



Listelenen örnekler, aşağıdaki yetkiler sağlar:

- /SECağacının kök düğümünde, hiçbir kullanıcının o düğümde yetkisi yok.
- usr1 nesnesine, /SEC/GOODnesnesine abone olma yetkisi verildi.
- usr2 nesnesine, /SEC/COMB/GOODnesnesine abone olma yetkisi verildi.

Konu nesnesi adı kullanılarak abone olunması

MQCHAR48 adını belirterek bir konu nesnesine abone olduğunda, konu ağacındaki ilgili düğüm yer alır. Düğümle ilişkili güvenlik öznitelikleri, kullanıcının abone olma yetkisine sahip olduğunu gösteriyorsa, erişim verilir.

Kullanıcıya erişim izni verilmediyse, ağaçtaki üst düğüm, kullanıcının üst düğüm düzeyine abone olma yetkisinin olup olmadığını belirler. Böyle bir durumda, erişim verilir. Değilse, düğümün üst öğesi dikkate alınır. Kullanıcı için abone olma yetkisi veren bir düğüm bulununcaya kadar özyineleme devam eder. Kök

düğüm, yetki verilmeden kök düğüme göz önünde bulundurulduğunda, yineleme durur. İkinci durumda erişim reddedilir.

Kısaca, yoldaki herhangi bir düğüm söz konusu kullanıcıya ya da uygulamaya abone olma yetkisi veriyorsa, abonenin o düğümde ya da konu ağacında o düğümün altındaki herhangi bir yerinde abone olmasına izin verilir.

Örnekteki kök düğüm SEC' dir.

Erişim denetimi listesi, kullanıcı kimliğinin kendisinin yetkisi olduğunu ya da kullanıcı kimliğinin üyesi olduğu bir işletim sistemi güvenlik grubunun yetkisi olduğunu gösteriyorsa, kullanıcıya abone olma yetkisi verilir.

Örneğin:

- usr1 abone olmaya çalışırsa, SEC/GOODkonu dizgisini kullanarak, kullanıcı kimliğinin o konu ile ilişkili düğüme erişimi olması için abonelik kullanılabilir. Ancak usr1 , SEC/COMB/GOOD konu dizgisini kullanarak abone olmaya çalıştıysa, kullanıcı kimliğinin kendisiyle ilişkili düğüme erişimi olmadığından, aboneliğe izin verilemez.
- If usr2 tries to subscribe, using a topic string of SEC/COMB/GOOD the subscription would be allowed to as the user ID has access to the node associated with the topic. Ancak usr2 , SEC/GOOD ' a abone olmaya çalıştıysa, kullanıcı kimliğinin kendisiyle ilişkili düğüme erişimi olmadığı için aboneliğe izin verilemez.
- If usr2 tries to subscribe using a topic string of SEC/COMB/GOOD/BAD the subscription would be allowed to because the user ID has access to the parent node SEC/COMB/GOOD.
- usr1 ya da usr2 ,topickonu dizesini kullanarak abone olmaya çalışırsa, bununla ilişkilendirilmiş konu düğümüne ya da o konunun üst düğümlerine erişimleri olmadığı için, /SEC/COMB/BAD' un bir konu dizesini kullanarak abone olmaya çalışırlar.

Var olmayan bir konu nesnesinin adını belirten bir abone olma işlemi, bir MQRC_UNKNOWN_OBJECT_NAME hatasına neden olur.

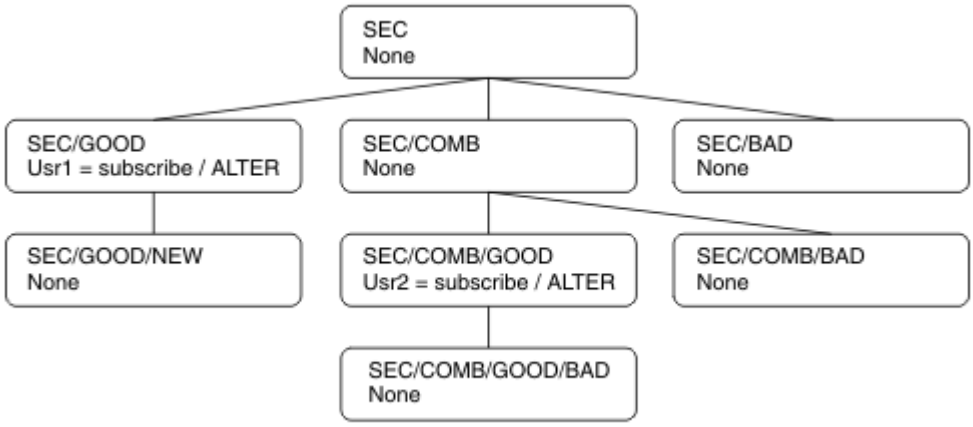
Konu düğümünün var olduğu bir konu dizesini kullanarak abone olma

Bu davranış, konuyu MQCHAR48 nesne adına göre belirtmesiyle aynıdır.

Konu düğümünün var olmadığı bir konu dizesini kullanarak abone olma

Şu anda konu ağacında var olmayan bir konu düğümünü temsil eden bir konu dizgisi belirterek, bir uygulamanın abone olma ihtimalini göz önünde bulundurun. Yetki denetimi, önceki bölümde belirtildiği şekilde gerçekleştirilir. Bu denetim öğesi, konu dizgisinin temsil ettiği üst düğümle başlar. Yetki verilirse, konu ağacında konu dizesini temsil eden yeni bir düğüm, konu ağacında yaratılır.

Örneğin, usr1 bir konuya abone olmayı dener SEC/GOOD/NEW. Authority is granted as usr1 has access to the parent node SEC/GOOD. Aşağıdaki çizge gösterilerinde, ağaçta yeni bir konu düğümü yaratılır. Yeni konu düğümü, doğrudan ilişkilendirilmiş güvenlik özniteliklerine sahip olmadığı bir konu nesnesi değil; öznitelikler üst öğesinden devralınır.



Genel arama karakterleri içeren bir konu dizesini kullanarak abone olma

Genel arama karakteri içeren bir konu dizesini kullanarak abone olma ihtimalini göz önünde bulundurun. Konu ağacında, konu dizgisinin tam olarak nitelenmiş bölüşüyle eşleşen düğüm için yetki denetimi yapılır.

Bu nedenle, bir uygulama SEC/COMB/GOOD/*' e abone olursa, konu ağacında SEC/COMB/GOOD düğümündeki önceki iki bölümde belirtildiği şekilde bir yetki denetimi gerçekleştirilir.

Similarly, if an application needs to subscribe to SEC/COMB/*/GOOD, an authority check is carried out on the node SEC/COMB.

Hedef kuyruklara yetki

Bir konuya abone olurken, değiştirgelerden biri, yayınları almak üzere çıkış için açılmış bir kuyruğun hobj işlecidir.

hobj belirtilmemişse, ancak boşsa, aşağıdaki koşullar geçerli olursa, yönetilen bir kuyruk oluşturulur:

- MQSO_MANAGED seçeneği belirtildi.
- Abonelik yok.
- Yaratma işlemi belirtildi.

hobj boşsa ve var olan bir aboneliği değiştiriyorsanız ya da devam ettiriyorsanız, önceden sağlanan hedef kuyruk yönetilebilir ya da yönetilmeyen olabilir.

MQSUB isteğini yapan uygulama ya da kullanıcı, iletileri hedef kuyruğa koyma yetkisine sahip olmalıdır; bu durumda, yayınlanan iletilerin o kuyruğa konması için etki yetkisi vardır. Yetki denetimi, kuyruk güvenliği denetimi için var olan kuralları izler.

Güvenlik denetimi, gereken yerlerde diğer kullanıcı kimliği ve bağlam güvenliği denetimlerini içerir. To be able to set any of the Identity context fields you must specify the MQSO_SET_IDENTITY_CONTEXT option as well as the MQSO_CREATE or MQSO_ALTER option. Bir MQSO_RESUME isteğindeki Kimlik bağlamı alanlarından hiçbirini ayarlayamazsınız.

Hedef yönetilen bir kuyruksa, yönetilen hedef için hiçbir güvenlik denetimi gerçekleştirilmez. Bir konuya abone olmanız için izin verdiyseniz, yönetilen hedefleri kullanabileceğiniz varsayılır.

Konu düğümünün bulunduğu konu ya da konu dizesini kullanarak yayınlama

Yayınlamaya ilişkin güvenlik modeli, abone olmak için kullanılan genel arama karakterleriyle aynıdır. Yayınların genel arama karakterleri yoktur; bu nedenle dikkate alınacak genel arama karakteri içeren bir konu dizgisine ilişkin bir vaka yoktur.

Yayımlama ve abone olma yetkileri ayrı. Bir kullanıcı ya da grup, diğer bir kullanıcı ya da grubun, diğerini yapması gerekmeden bir tane yapma yetkisine sahip olabilir.

Bir konu nesnesine, MQCHAR48 adını ya da konu dizgisini belirterek yayınlama sırasında, konu ağacındaki ilgili düğüm yer alır. Konu düğmesiyle ilişkilendirilmiş güvenlik öznitelikleri, kullanıcının yayınlama yetkisi olduğunu gösteriyorsa, erişim verilir.

Erişim verilmezse, ağaçtaki üst düğüm, kullanıcının o düzeyde yayınlama yetkisinin olup olmadığını belirler. Böyle bir durumda, erişim verilir. Yoksa, kullanıcı için yayınlama yetkisi veren bir düğüm bulununcaya kadar özyineleme devam eder. Kök düğüm, yetki verilmeden kök düğüme göz önünde bulundurulduğunda, yineleme durur. İkinci durumda erişim reddedilir.

Kısaca, yoldaki herhangi bir düğüm söz konusu kullanıcıya ya da uygulamaya yayınlama yetkisi veriyorsa, yayınlayıcının o düğümde ya da konu ağacında o düğümün altındaki herhangi bir yerinde yayınlayacağı izin verilir.

Konu düğümünün var olmadığı konu adı ya da konu dizesi kullanılarak yayınlama

Abone olma işlemindeki gibi, bir uygulama yayınlandığında, konu ağacında şu anda var olmayan bir konu düğümünü temsil eden bir konu dizgisi belirterek, yetki denetimi, konu dizgisinin temsil ettiği düğümün üst öğesiyle başlayarak gerçekleştirilir. Yetki verilirse, konu ağacında konu dizesini temsil eden yeni bir düğüm, konu ağacında yaratılır.

Bir konu nesnesine çözülen bir diğer ad kuyruğu kullanılarak yayınlama

Bir konu nesnesine çözülen bir diğer ad kuyruğunu kullanarak yayınlarsanız, güvenlik denetimi hem diğer ad kuyruğunda, hem de çözümleyicisinin temelindeki konuda gerçekleşir.

Diğer ad kuyruğunda bulunan güvenlik denetimi, kullanıcının o diğer ad kuyruğuna ileti koyma yetkisi olduğunu doğrular ve konu üzerindeki güvenlik denetimi, kullanıcının o konuya yayınlayabileceğini doğrular. Bir diğer ad kuyruğu başka bir kuyruğa çözüldüğünde, denetim altında yatan kuyruklar üzerinde denetim yapılmaz. Konular ve kuyruklar için yetki denetimi farklı bir şekilde gerçekleştirilir.

Aboneliğin kapatılması

Aboneliği bu tanıtıcı altında yaratmadıysanız, MQCO_REMOVE_SUB seçeneğini kullanarak aboneliği kapadığınızda ek güvenlik denetimi vardır.

Aboneliğin kaldırımında işlem sonuçları olarak bunu yapmak için doğru yetkiye sahip olmanız için bir güvenlik denetimi gerçekleştirilir. Konu düğmesiyle ilişkilendirilmiş güvenlik öznitelikleri, kullanıcının yetkisinin olduğunu gösteriyorsa, erişim verilir. Yoksa, ağaçtaki üst düğüm, kullanıcının aboneliği kapatma yetkisinin olup olmadığını belirlemek için dikkate alınır. Yetki verilinceye ya da kök düğüme ulaşılıncaya kadar özyineleme devam eder.

Aboneliğin tanımlanması, değiştirilmesi ve silinmesi

Bir abonelik, MQSUB API isteğini kullanmak yerine, yönetimsel olarak oluşturulduğunda, herhangi bir abone olma güvenlik denetimi gerçekleştirilmez. Yönetici, bu yetkiyi komuta yoluyla zaten verdi.

Yayınların, abonelikle ilişkili hedef kuyruğa konulabilmelerini sağlamak için güvenlik denetimleri gerçekleştirilir. Denetimler, MQSUB isteği ile aynı şekilde gerçekleştirilir.

Bu güvenlik denetimleri için kullanılan kullanıcı kimliği, verilmekte olan komutun uygulanmasının üzerine bağlıdır. If the **SUBUSER** parameter is specified it affects the way the check is performed, as shown in Çizelge 81 sayfa 454:

Çizelge 81. Komutlar için güvenlik denetimleri için kullanılan kullanıcı kimlikleri			
Komut	**SUBUSER belirlendi ve boş**	**SUBUSR belirlendi ve tamamlandı**	**SUBUSR belirtilmedi**
	Yönetici kimliğini kullan		LIKE aboneliklerinden kullanıcı kimliğini kullan
	Yönetici kimliğini kullan		SYSTEM.DEFAULT.SUB aboneliği-boşsa, yönetici kimliğini kullanın
	Yönetici kimliğini kullan		Var olan abonelikten kullanıcı kimliğini kullan

Yalnızca DELETE SUB komutunu kullanarak abonelikleri silerken gerçekleştirilen tek güvenlik denetimi komut güvenliği denetimidir.

Örnek yayınlama/abone olma güvenlik ayarı

Bu bölümde, güvenlik denetiminin gerektiği şekilde uygulanmasına olanak tanıyan bir şekilde, konularda erişim denetimi ayarlanmış bir senaryo açıklanmaktadır.

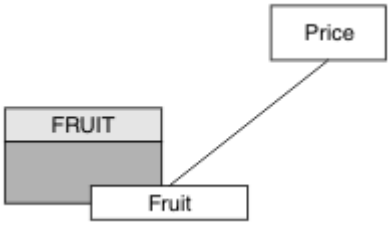
Bir konuya abone olmak için kullanıcıya erişim izni ver

Bu konu, birden çok kullanıcıya göre konulara nasıl erişim verileceğini bildiren bir görev listesinde yer alan ilk konudur.

Bu görev hakkında

Bu görev, hiçbir denetim konusu nesnesinin varolmadığını ve abonelik ya da yayın için tanımlanmış bir profilin bulunmadığını varsayar. Uygulamalar, var olan olanları sürdürme yerine yeni abonelikler oluşturuyor ve bunu yalnızca konu dizesini kullanarak yapıyor.

Bir uygulama, bir konu nesnesi ya da bir konu dizgisi ya da her ikisinin birleşimi sağlayarak abonelik yapabilir. Uygulamanın seçeceği şekilde, etki, konu ağacındaki belirli bir noktada abonelik yapmak olur. Konu ağacındaki bu nokta bir denetim konusu nesnesiyle gösteriliyorsa, o konu nesnesinin adına dayalı olarak bir güvenlik tanıtımı denetlenir.



Şekil 23. Konu nesne erişimi örneği

Çizelge 82. Örnek konu nesnesi erişimi		
Konu	**Abone olma erişimi gerekiyor**	**Konu nesnesi**
Fiyat	Kullanıcı yok	Yok
Fiyat/Fruit	USER1	MEYVE

Yeni bir konu nesnesini aşağıdaki gibi tanımlayın:

Yordam

1. Issue the MQSC command `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`.
2. Erişim izni aşağıdaki gibi olur:
   - z/OS **z/OS** :

     `hlq.SUBSCRIBE.FRUIT` profiline kullanıcı erişimi vererek `"Price/Fruit"` konusuna abone olmak için USER1 olanağına erişim izni verin. Bunu yapmak için aşağıdaki RACF komutlarını kullanın:

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
     PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     ```

   - Diğer platformlar:

     Grant access to USER1 to subscribe to topic `"Price/Fruit"` by granting the user access to the FRUIT object. Bu işlemi, altyapıya ilişkin yetki komutunu kullanarak yapın:

     ULW **Windows, UNIX and Linux sistemleri**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +sub
     ```

     IBM i **IBM i**

     ```
     GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
     ```

Sonuçlar

USER1 , `"Price/Fruit"` konusuna abone olmayı denediğinde sonuç başarılı olur.

When USER2 attempts to subscribe to topic `"Price/Fruit"` the result is failure with an `MQRC_NOT_AUTHORIZED` message, together with:

- z/OS z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ULW Diğer platformlarda, aşağıdaki yetki olayı:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  ```

```
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- IBM i IBMi üzerinde, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Bunun gördüğünün bir şekli olduğunu unutmayın; tüm alanları değil.

Bir kullanıcıya ağaç içinde daha derin bir konuya abone olmak için erişim izni ver

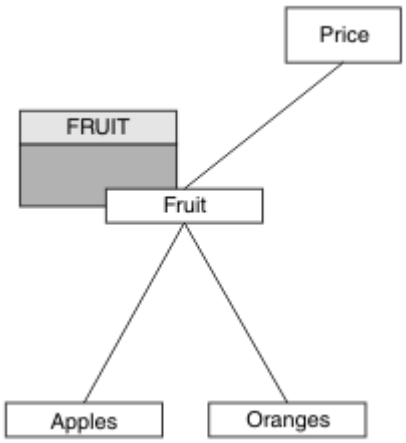
Bu konu, birden çok kullanıcı tarafından konulara nasıl erişim verileceğini size bildiren görevler listesinde ikinci sıradır.

Başlamadan önce

Bu konu, "Bir konuya abone olmak için kullanıcıya erişim izni ver" sayfa 454içinde açıklanan kurulumları kullanır.

Bu görev hakkında

Konu ağacındaki nokta, uygulamanın abonelik yaptığı yerde bir denetim konusu nesnesi tarafından gösterilmiyorsa, en yakın üst denetim konusu nesnesi bulununcaya kadar ağacı yukarı doğru taşıyın. Güvenlik profili, o konu nesnesinin adına dayalı olarak denetlenir.



Şekil 24. Bir konu ağacındaki bir konuya erişim verme örneği

Çizelge 83. Örnek konular ve konu nesnelerine ilişkin erişim gereksinmeleri

Konu	Abone olma erişimi gerekiyor	Konu nesnesi
Fiyat	Kullanıcı yok	Yok
Fiyat/Fruit	USER1	MEYVE
Fiyat/Meyve/Elma	USER1	

Çizelge 83. Örnek konular ve konu nesnelerine ilişkin erişim gereksinmeleri (devamı var)		
Konu	**Abone olma erişimi gerekiyor**	**Konu nesnesi**
Fiyat/Meyve/ Portakal	USER1	

In the previous task USER1 was granted access to subscribe to topic `"Price/Fruit"` by granting it access to the `hlq.SUBSCRIBE.FRUIT` profile on z/OS and subscribe access to the FRUIT profile on other platforms. Bu tek profil, `"Price/Fruit/Apples"`, `"Price/Fruit/Oranges"` ve `"Price/Fruit/#"'` ye abone olmak için de USER1 erişimi verir.

USER1 , `"Price/Fruit/Apples"` konusuna abone olmayı denediğinde sonuç başarılı olur.

When USER2 attempts to subscribe to topic `"Price/Fruit/Apples"` the result is failure with an `MQRC_NOT_AUTHORIZED` message, together with:

- z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Diğer platformlarda, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Apples"
```

Aşağıdakileri unutmayın:

- z/OS üzerinde aldığınız iletiler, aynı konu nesneleri ve tanıtımların erişimleri denetlediğinden, önceki görevdeki alınanlar ile aynıdır.
- Diğer platformlarda aldığınız olay iletisi, önceki görevdeki alınana benzer, ancak gerçek konu dizgisi farklıdır.

Başka bir kullanıcıya, ağaç içindeki daha derinlere abone olmak için başka bir kullanıcı erişimi verin

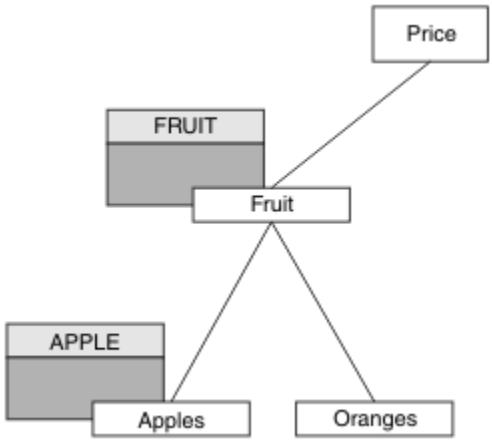
Bu konu, birden çok kullanıcı tarafından konulara abone olmak için nasıl erişim verileceğini size bildiren görevler listesinde üçüncü konudur.

Başlamadan önce

Bu konu, “Bir kullanıcıya ağaç içinde daha derin bir konuya abone olmak için erişim izni ver” sayfa 456içinde açıklanan kurulumları kullanır.

Bu görev hakkında

In the previous task USER2 was refused access to topic `"Price/Fruit/Apples"`. Bu konu, size bu konuya nasıl erişim verileceğini, ancak diğer konuların nasıl verileceğini belirtir.



Şekil 25. Bir konu ağacındaki belirli konulara erişim verilmesi

Çizelge 84. Örnek konular ve konu nesnelerine ilişkin erişim gereksinmeleri

Konu	Abone olma erişimi gerekiyor	Konu nesnesi
Fiyat	Kullanıcı yok	Yok
Fiyat/Fruit	USER1	MEYVE
Fiyat/Meyve/Elma	USER1 ve USER2	Apple
Fiyat/Meyve/Portakal	USER1	

Yeni bir konu nesnesini aşağıdaki gibi tanımlayın:

Yordam

1. Issue the MQSC command `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.
2. Erişim izni aşağıdaki gibi olur:

- z/OS **z/OS** :

  In the previous task USER1 was granted access to subscribe to topic `"Price/Fruit/Apples"` by granting the user access to the `hlq.SUBSCRIBE.FRUIT` profile.

  Bu tek profil, `"Price/Fruit/Oranges"` `"Price/Fruit/#"` ' a abone olmak için USER1 erişimi de verdi ve bu erişim, yeni konu nesnesinin ve onunla ilişkili profillerin eklenmesiyle birlikte olmaya devam ediyor.

  `hlq.SUBSCRIBE.APPLE` profiline kullanıcı erişimi vererek `"Price/Fruit/Apples"` konusuna abone olmak için USER2 olanağına erişim izni verin. Bunu yapmak için aşağıdaki RACF komutlarını kullanın:

  ```
  RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
  PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
  ```

- Diğer platformlar:

  In the previous task USER1 was granted access to subscribe to topic `"Price/Fruit/Apples"` by granting the user subscribe access to the `FRUIT` profile.

Bu tek profil, "Price/Fruit/Oranges" ve "Price/Fruit/#"' a abone olmak için USER1 erişimi de vermiştir ve bu erişim, yeni konu nesnesinin ve onunla ilişkili profillerin eklenmesiyle birlikte kalır.

Kullanıcıya APPLE profiline abone olma erişimi vererek "Price/Fruit/Apples" olanağına abone olmak için USER2 olanağına erişim verin. Bu işlemi, altyapıya ilişkin yetki komutunu kullanarak yapın:

ULW **Windows, UNIX and Linux sistemleri**

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

IBM i **IBM i**

```
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER2) AUT(*SUB)
```

Sonuçlar

On z/OS, when USER1 attempts to subscribe to topic "Price/Fruit/Apples" the first security check on the hlq.SUBSCRIBE.APPLE profile fails, but on moving up the tree the hlq.SUBSCRIBE.FRUIT profile allows USER1 to subscribe, so the subscription succeeds and no return code is sent to the MQSUB call. Ancak, ilk denetim için bir RACF ICH iletisi oluşturulur:

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

When USER2 attempts to subscribe to topic "Price/Fruit/Apples" the result is success because the security check passes on the first profile.

When USER2 attempts to subscribe to topic "Price/Fruit/Oranges" the result is failure with an MQRC_NOT_AUTHORIZED message, together with:

- z/OS z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ULW Windowsplatformlarında, UNIX and Linux altyapılarında aşağıdaki yetki olayı:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

- IBM i IBMi üzerinde, aşağıdaki yetki olayı:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

Bu kurulumın dezavantajı, z/OSüzerinde, konsolda ek ICH iletileri almanıza neden olur. Konu ağacını farklı bir şekilde sabitlediğinizde bundan kaçınabilirsiniz.

Ek iletileri önlemek için erişim denetimini değiştir

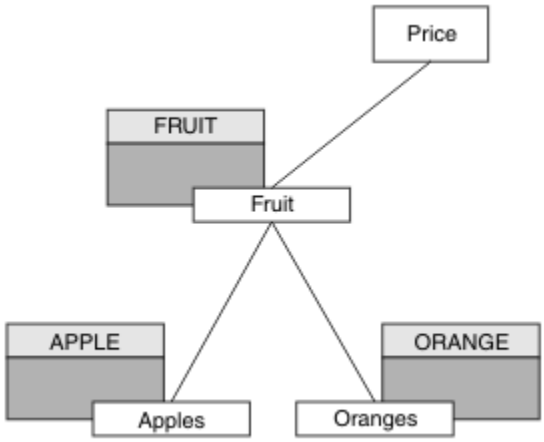
Bu konu, birden çok kullanıcıya göre konulara abone olma ve z/OSüzerindeki ek RACF ICH408I iletilerinden kaçınmak için erişim verilmesine nasıl izin verileceğini bildiren görevler listesinde dördüncü sırada yer alıyor.

Başlamadan önce

Bu konu, ek hata iletilerini önlemenizi önlemek için "Başka bir kullanıcıya, ağaç içindeki daha derinlere abone olmak için başka bir kullanıcı erişimi verin" sayfa 457 içinde açıklanan kurulumu iyileştirir.

Bu görev hakkında

Bu konuda, ağaçta daha derin konulara nasıl erişim verileceği ve kullanıcı gerektirmediği zaman ağacın aşağıya doğru nasıl erişileceği anlatılıyor.



Şekil 26. Ek iletileri önlemek için erişim denetimi verilmesine örnek olarak verilebilir.

Yeni bir konu nesnesini aşağıdaki gibi tanımlayın:

Yordam

1. Issue the MQSC command `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Erişim izni aşağıdaki gibi olur:

- z/OS **z/OS** :

  Yeni bir profil tanımlayın ve bu tanıtıma ve var olan tanıtımlara erişim ekleyin. Bunu yapmak için aşağıdaki RACF komutlarını kullanın:

```
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)
```

- Diğer platformlar:

  Altyapıya ilişkin yetki komutlarını kullanarak eşdeğer erişimi ayarlayın:

  ULW **Windows, UNIX and Linux sistemleri**

```
setmqaut -t topic -n ORANGE -p USER1 +sub
setmqaut -t topic -n APPLE -p USER1 +sub
```

IBM i

```
GRTMQAUT OBJ(ORANGE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
```

Sonuçlar

On z/OS, when USER1 attempts to subscribe to topic `"Price/Fruit/Apples"` the first security check on the `hlq.SUBSCRIBE.APPLE` profile succeeds.

Benzer şekilde, USER2 konuya abone olma girişiminde bulunduğunda `"Price/Fruit/Apples"` , güvenlik denetimi ilk tanıtıma geçtiği için sonuç başarılıdır.

When USER2 attempts to subscribe to topic `"Price/Fruit/Oranges"` the result is failure with an `MQRC_NOT_AUTHORIZED` message, together with:

- z/OS z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ULW Diğer platformlarda, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

- IBM i IBMi üzerinde, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

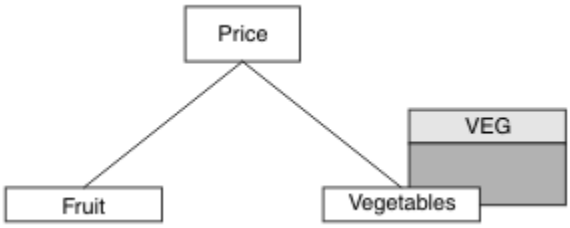
Bir konuyla ilgili olarak yayınlamak için kullanıcıya erişim izni ver

Bu konu, bir kullanıcıya birden çok kullanıcı tarafından yayınlama erişimi verilmesine nasıl izin verileceğini bildiren ilk görevler listesinde yer alan ilk konudur.

Bu görev hakkında

Bu görev, konu ağacının sağ tarafında herhangi bir denetim konusu nesnesi olmadığını ya da yayın için herhangi bir profilin tanımlandığını varsayar. Kullanılan varsayım, yayıncıların yalnızca konu dizesini kullanmaktadır.

Bir uygulama, bir konu nesnesini ya da bir konu dizgisini ya da her ikisinin birleşimini sağlayarak bir konuya yayınlanabilir. Uygulamanın seçeceği şekilde, etki, konu ağacındaki belirli bir noktada yayınlamalıdır. Konu ağacındaki bu nokta bir denetim konusu nesnesiyle gösteriliyorsa, o konu nesnesinin adına dayalı olarak bir güvenlik tanıtımı denetlenir. Örneğin:



Şekil 27. Bir konuya yayınlama erişimi verilmesi

Çizelge 85. Örnek yayınlama erişim gereksinimleri		
Konu	**Yayınlama erişimi gerekli**	**Konu nesnesi**
Fiyat	Kullanıcı yok	Yok
Fiyat/Sebzeler	USER1	VEG

Yeni bir konu nesnesini aşağıdaki gibi tanımlayın:

Yordam

1. Issue the MQSC command `DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
2. Erişim izni aşağıdaki gibi olur:

- z/OS **z/OS** :

  Grant access to USER1 to publish to topic `"Price/Vegetables"` by granting the user access to the `hlq.PUBLISH.VEG` profile. Bunu yapmak için aşağıdaki RACF komutlarını kullanın:

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
  PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
  ```

- Diğer platformlar:

  Grant access to USER1 to publish to topic `"Price/Vegetables"` by granting the user access to the VEG profile. Bu işlemi, altyapıya ilişkin yetki komutunu kullanarak yapın:

  ULW **Windows, UNIX and Linux sistemleri**

  ```
  setmqaut -t topic -n VEG -p USER1 +pub
  ```

  IBM i **IBM i**

  ```
  GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
  ```

Sonuçlar

USER1 , `"Price/Vegetables"` konusuna yayınlamayı denediğinde sonuç başarılı olur; yani, MQOPEN çağrısı başarılı olur.

When USER2 attempts to publish to topic `"Price/Vegetables"` the MQOPEN call fails with an `MQRC_NOT_AUTHORIZED` message, together with:

- z/OS z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- ULW Diğer platformlarda, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

- IBM i IBMi üzerinde, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

Bunun gördüğünün bir şekli olduğunu unutmayın; tüm alanları değil.

Bir kullanıcıya ağaç içinde daha derin bir konu yayınlamak için erişim izni ver

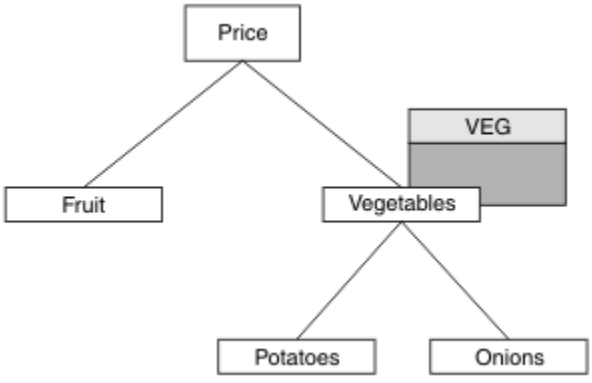
Bu konu, birden çok kullanıcıya göre konu başlıklarına nasıl erişilmesine ilişkin erişim verileceğini size bildiren görevler listesinde ikinci sıradır.

Başlamadan önce

Bu konu, “Bir konuyla ilgili olarak yayınlamak için kullanıcıya erişim izni ver” sayfa 461içinde açıklanan kurulumları kullanır.

Bu görev hakkında

Konu ağacında uygulamanın yayınlandığı nokta bir yönetici konu nesnesiyle gösterilmiyorsa, en yakın üst denetim konusu nesnesinin bulunduğu ağacı yukarı taşıyın. Güvenlik profili, o konu nesnesinin adına dayalı olarak denetlenir.



Şekil 28. Bir konu ağacındaki bir konuya yayınlama erişimi verilmesi

Çizelge 86. Örnek yayınlama erişim gereksinimleri		
Konu	**Abone olma erişimi gerekiyor**	**Konu nesnesi**
Fiyat	Kullanıcı yok	Yok
Fiyat/Sebzeler	USER1	VEG
Fiyat/Sebzeler/Patates	USER1	
Fiyat/Sebzeler/Soğan	USER1	

In the previous task USER1 was granted access to publish topic `"Price/Vegetables/Potatoes"` by granting it access to the `hlq.PUBLISH.VEG` profile on z/OS or publish access to the VEG profile on other platforms. This single profile also grants USER1 access to publish at `"Price/Vegetables/Onions"`.

USER1 , `"Price/Vegetables/Potatoes"` konusunda yayınlama girişiminde bulunduğunda, sonuç başarılı olur; MQOPEN çağrısının başarılı olması gerekir.

USER2 , `"Price/Vegetables/Potatoes"` konusuna abone olmayı denediğinde, sonuç başarısız olur; yani, MQOPEN çağrısı bir `MQRC_NOT_AUTHORIZED` iletisiyle başarısız olur ve aşağıdakilerle birlikte başarısız olur:

- z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Diğer platformlarda, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables/Potatoes"
```

Aşağıdakileri unutmayın:

- z/OS üzerinde aldığınız iletiler, aynı konu nesneleri ve tanıtımların erişimleri denetlediğinden, önceki görevdeki alınanlar ile aynıdır.
- Diğer platformlarda aldığınız olay iletisi, önceki görevdeki alınana benzer, ancak gerçek konu dizgisi farklıdır.

Yayınlama ve abone olma için erişim izni ver

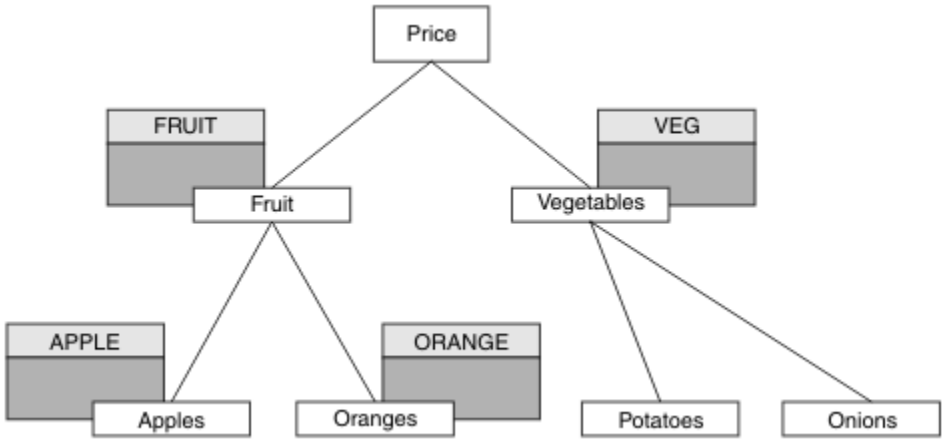
Bu konu, bir kullanıcıya birden çok kullanıcı tarafından yayınlama ve konuya abone olma erişim izni verileceğini bildiren görevler listesinin en sonuncunda yer alıyor.

Başlamadan önce

Bu konu, “Bir kullanıcıya ağaç içinde daha derin bir konu yayınlamak için erişim izni ver” sayfa 463içinde açıklanan kurulumları kullanır.

Bu görev hakkında

In a previous task USER1 was given access to subscribe to the topic `"Price/Fruit"`. Bu konuda, o kullanıcıya yayınlayabilmek için o kullanıcıya nasıl erişim verileceği açıklanır.



Şekil 29. Yayınlama ve abone olma için erişim verilmesi

Çizelge 87. Erişim gereksinmelerini yayınlama ve abone olma örneği

Konu	Abone olma erişimi gerekiyor	Yayınlama erişimi gerekli	Konu nesnesi
Fiyat	Kullanıcı yok	Kullanıcı yok	Yok
Fiyat/Fruit	USER1	USER1	MEYVE
Fiyat/Meyve/Elma	USER1 ve USER2		Apple
Fiyat/Meyve/Portakal	USER1		Turuncu

Yordam

Erişim izni aşağıdaki gibi olur:

- z/OS **z/OS** :

  In an earlier task USER1 was granted access to subscribe to topic `"Price/Fruit"` by granting the user access to the `hlq.SUBSCRIBE.FRUIT` profile.

  `"Price/Fruit"` konusuna yayınlayabilmek için `hlq.PUBLISH.FRUIT` profiline USER1 erişimine izin verin. Bunu yapmak için aşağıdaki RACF komutlarını kullanın:

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
  PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
  ```

- Diğer platformlar:

  Grant access to USER1 to publish to topic `"Price/Fruit"` by granting the user publish access to the `FRUIT` profile. Bu işlemi, altyapıya ilişkin yetki komutunu kullanarak yapın:

  ULW **Windows, UNIX and Linux sistemleri**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

IBM i

```
GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

Sonuçlar

On z/OS, when USER1 attempts to publish to topic `"Price/Fruit"` the security check on the MQOPEN call passes.

When USER2 attempts to publish at topic `"Price/Fruit"` the result is failure with an `MQRC_NOT_AUTHORIZED` message, together with:

- z/OS' ta, konsolda, denenen konu ağacında tam güvenlik yolunu gösteren aşağıdaki iletiler gösterilir:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Windows, UNIXve Linux platformlarında aşağıdaki yetkilendirme olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- IBMi üzerinde, aşağıdaki yetki olayı:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Bu görevlerin tam olarak belirlenmesinin ardından, USER1 ve USER2 ' a yayınlama ve listelenen konulara abone olmak için aşağıdaki erişim yetkilerini verir:

Çizelge 88. Güvenlik örneklerinden kaynaklanan erişim yetkilerinin tam listesi

Konu	Abone olma erişimi gerekiyor	Yayınlama erişimi gerekli	Konu nesnesi
Fiyat	Kullanıcı yok	Kullanıcı yok	Yok
Fiyat/Fruit	USER1	USER1	MEYVE
Fiyat/Meyve/Elma	USER1 ve USER2		Apple
Fiyat/Meyve/Portakal	USER1		Turuncu
Fiyat/Sebzeler		USER1	VEG
Fiyat/Sebzeler/Patates			

Çizelge 88. Güvenlik örneklerinden kaynaklanan erişim yetkilerinin tam listesi (devamı var)			
Konu	**Abone olma erişimi gerekiyor**	**Yayınlama erişimi gerekli**	**Konu nesnesi**
Fiyat/ Sebzeler/ Soğan			

Konu ağacındaki farklı düzeylerde güvenlik erişimi için farklı gereksinimlere sahip olduğunuz yerlerde dikkatli planlama, z/OS konsol günlüğüne dış güvenlik uyarıları almamanızı sağlar. Ağaç içindeki doğru düzeyde güvenlik ayarlanması, güvenlik iletilerini yanıltmalarından kaçınabiliyor.

Abonelik güvenliği

MQSO_ALTERNATE_USER_AUTHORITY

AlternateUserTanıtıcısı alanı, bu MQSUB çağrısını doğrulamak için kullanılacak bir kullanıcı kimliği içerir. The call can succeed only if this AlternateUserId is authorized to subscribe to the topic with the specified access options, regardless of whether the user identifier under which the application is running is authorized to do so.

MQSO_SET_IDENTITY_CONTEXT

Abonelik, PubAccountingSimgesi ve PubApplIdentityData alanlarında sağlanan muhasebe belirteci ve uygulama kimliği verilerini kullanmaktadır.

Bu seçenek belirlenirse, aynı yetki denetimi, MQOO_SET_IDENTITY_CONTEXT ile hedef kuyruğa bir MQSO_set_identifity_context kullanılarak erişildiği gibi yürütülür. Bu durumda, hedef kuyrukta bir yetki denetimi yapılmadığı durumlarda, MQSO_MANAGED seçeneğinin de kullanıldığı durumlar dışında.

Bu seçenek belirlenmezse, bu aboneye gönderilen yayınların varsayılan bağlam bilgileri aşağıdaki gibi olur:

Çizelge 89. Varsayılan yayın bağlamı bilgileri	
MQMD ' de alan	**Kullanılan değer**
UserIdentifier	Yayının yapıldığı sırada, abonelikle ilişkili kullanıcı kimliği (DISPLAY SBSTATUS ' ta SUBUSER alanına bakın).
AccountingToken	Olanaklıysa, ortamdan saptanır; tersi durumda MQACT_NONE değerine ayarlanır.
ApplIdentityVerileri	Boşluklara ayarlayın.

Bu seçenek yalnızca MQSO_CREATE ve MQSO_ALTER ile geçerlidir. MQSO_RESUME ile kullanılırsa, PubAccountingSimgesi ve PubApplIdentityData alanları yoksayılır, bu nedenle bu seçeneğin herhangi bir etkisi yoktur.

Bir abonelik, önceden aboneliğin sağladığı kimlik bağlamı bilgilerini içeren bu seçenek kullanılmadan değiştirilirse, değiştirilen abonelik için varsayılan bağlam bilgileri oluşturulur.

Farklı kullanıcı kimlikleri için MQSO_ANY_USERID seçeneği ile farklı kullanıcı kimliklerinin kullanılmasına izin veren bir abonelik farklı bir kullanıcı kimliği tarafından sürdürülürse, artık abonelik sahibi olan yeni kullanıcı kimliği için varsayılan kimlik bağlamı oluşturulur ve sonraki yayınlar yeni kimlik bağlamını içeren teslim edilir.

AlternateSecurityTanıtıcısı

Bu, uygun yetki denetimlerinin gerçekleştirilmesine izin vermek için yetki hizmetine AlternateUserTanıtıcısı ile geçirilen bir güvenlik tanıtıcısıdır. AlternateSecuritytanıtıcısı yalnızca MQSO_ALTERNATE_USER_AUTHORITY belirtildiyse kullanılır ve AlternateUserId alanı, ilk boş karakter ya da alanın sonuna kadar tam olarak boş bırakılmaz.

MQSO_ANY_USERID abonelik seçeneği

MQSO_ANY_USERID belirtildiğinde, abonenin kimliği tek bir kullanıcı kimliğiyle sınırlı değildir. Bu, herhangi bir kullanıcının uygun yetkiye sahip olduğunda aboneliği değiştirmesine ya da sürdürmesine olanak sağlar. Aboneliğin herhangi bir zamanda yalnızca tek bir kullanıcı tarafından olması gerekir. Şu anda başka bir uygulama tarafından kullanılmakta olan bir aboneliğin kullanımını sürdürme girişimi, çağrıya MQRC_XX_ENCODE_CASE_ONE subscription_in_use ile başarısız olmasına neden olur.

Bu seçeneği var olan bir aboneliğe eklemek için, MQSOB çağrısının (MQSO_ALTER kullanılarak) özgün abonelikle aynı kullanıcı kimliğiyle gelmeleri gerekir.

Bir MQSUB çağrısı, MQSO_ANY_USERID ayarına sahip var olan bir aboneliğe başvuruyorsa ve kullanıcı kimliği özgün abonelikten farklıysa, çağrı yalnızca yeni kullanıcı kimliğinin konuya abone olma yetkisi varsa başarılı olur. İşlem başarıyla tamamlandıktan sonra, bu aboneye gelecek yayınlar, yayındaki yeni kullanıcı kimliği ayarlarıyla abonenin kuyruğuna konabilr.

MQSO_FIXED_USERID

MQSO_FIXED_USERID değeri belirtildiğinde, abonelik yalnızca sahibi olan tek bir kullanıcı kimliği tarafından değiştirilebilir ya da sürdürülür. Bu kullanıcı kimliği, bu seçeneği ayarlayan aboneliği değiştirmek için son kullanıcı kimliğidir; dolayısıyla, MQSO_ANY_USERID seçeneğini kaldırın ya da hiçbir alter işlemi gerçekleşmediyse, aboneliği yaratan kullanıcı kimliğidir.

Bir MQSUB komutu MQSO_ANY_USERID kümesiyle var olan bir aboneliği ifade eder ve MQSO_FIXED_USERID seçeneğini kullanmak için aboneliği (MQSO_ALTER kullanarak) değiştirirse, aboneliğin kullanıcı kimliği şu anda bu yeni kullanıcı kimlide düzeltilir. Bu çağrı, yalnızca yeni kullanıcı kimliğinin konuya abone olma yetkisi varsa başarılı olur.

Bir MQSO_FIXED_USERID aboneliğini sürdürmek ya da bir MQSO_FIXED_USERID aboneliğini değiştirmek için sahip olduğu kaydedilen bir kullanıcı kimliği dışında bir kullanıcı kimliği MQRC_IDENTITY_MISMATCH ile başarısız olur. Bir aboneliğin sahibi olan kullanıcı kimliği, DISPLAY SBSTATUS komutu kullanılarak görüntülenebilir.

Ne MQSO_ANY_USERID ya da MQSO_FIXED_USERID belirtilirse, varsayılan değer MQSO_FIXED_USERID olur.

Kuyruk yöneticileri arasında güvenliği yayınla/abone ol

Yetkili abonelik abonelikleri ve yayınlar gibi iç iletileri yayınlama/abone olma, olağan kanal güvenlik kurallarını kullanarak sistem kuyruklarını yayınlamaya/abone olma konumuna getirmektedir. Bu konudaki bilgi ve çizgeler, bu iletilerin tesliminde yer alan çeşitli süreçleri ve kullanıcı kimliklerini vurgular.

Yerel erişim denetimi

Yayın ve aboneliklere ilişkin konulara erişim, Yayınlama/abone olma güvenliğindeaçıklanan yerel güvenlik tanımlarıyla ve kurallarıyla yönetilir. z/OS' ta, erişim denetimi oluşturmak için herhangi bir yerel konu nesnesi gerekmez. Diğer altyapılarda da erişim denetimi için yerel bir konu gerekmez. Yöneticiler, kümede var olup olmamaları bağımsız olarak, kümelenmiş konu nesnelerine erişim denetimi uygulamayı tercih edebilir.

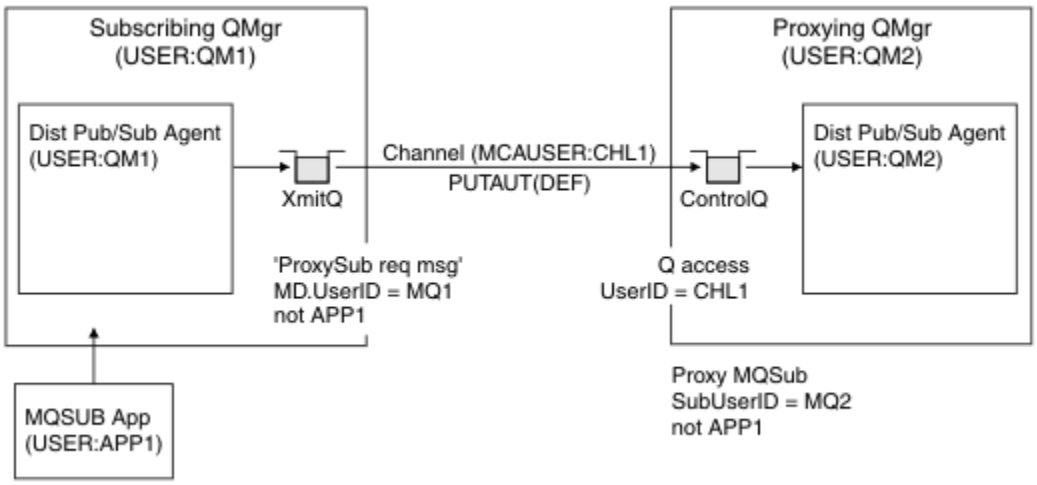
Sistem yöneticileri, yerel sistemlerindeki erişim denetiminden sorumludur. Erişim denetimi ilkesinden sorumlu olmak için, sıradüzeninin diğer üyelerinin yöneticilerine ya da küme kolektiflerine güvenmeleri gerekir. Erişim denetimi her bir ayrı makine için tanımlandığından, yüksek düzeyde denetime gerek duyulması durumunda da bu denetim öğesi büyük olasılıkla gömüledir. Erişim denetimi uygulanması

gerekli olmayabilir ya da erişim denetimi, konu ağacındaki üst düzey nesneler üzerinde tanımlanabilir. Önemli düzey erişim denetimi, konu ad alanının her bir alt bölümü için tanımlanabilir.

Yetkili abonelik oluşturma

Bir kuruluşun kuyruk yöneticisini kuyruk yöneticinize bağlayacak bir kuruluş için güven, olağan kanal kimlik doğrulaması tarafından onaylanır. Bu güvenilir kuruluşun dağıtımlı yayınlama/abone olma izni de veriliyorsa, bir yetki denetimi yapılır. Bu denetim, kanal, dağıtılmış yayınlama/abone olma kuyruğuna bir ileti yerleştirdiğinde yapılır. Örneğin, SYSTEM.INTER.QMGR.CONTROL kuyruğuna bir ileti konursa. Kuyruk yetkisi denetiminin kullanıcı kimliği, alan kanalının PUTAUT değerlerine bağlıdır. Örneğin, kanalın kullanıcı kimliği (MCAUSER), değer ve altyapıya bağlı olarak ileti bağlamı. Kanal güvenliğiyle ilgili ek bilgi için Kanal güvenliğibaşlıklı konuya bakın.

Yetkili sunucu abonelikleri, uzak kuyruk yöneticilikteki dağıtılmış yayınlama/abone olma aracısının kullanıcı kimliğiyle yapılır. Örneğin, Şekil 30 sayfa 469in QM2 . Kullanıcı kimliği sistemde tanımlı olduğundan ve dolayısıyla etki alanı çakışmaları olmadığından, kullanıcı daha sonra yerel konu nesne profillerine kolayca erişim izni verilir.



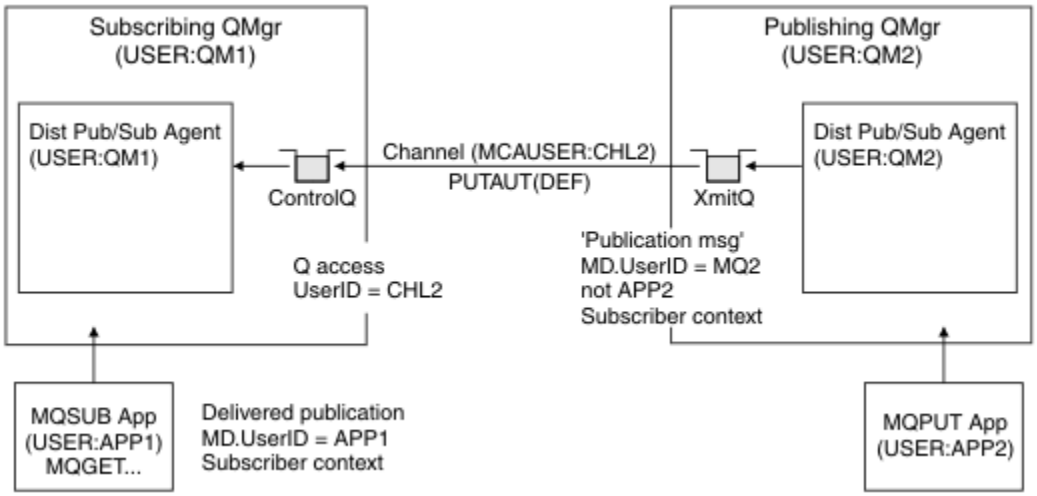
Şekil 30. Yetkili abonelik güvenliği, abonelik yapma

Uzak yayınları gönderme

Yayınlama kuyruk yöneticisince bir yayın oluşturulduğunda, herhangi bir yetkili abonelik için yayının bir kopyası oluşturulur. Kopyalanan yayının bağlamı, aboneliği yapan kullanıcı kimliğinin bağlamını (Şekil 31 sayfa 470içinde QM2) içerir. Yetkili abonelik, uzak kuyruk olan bir hedef kuyrukla yaratılır; bu nedenle, yayın iletisi bir iletim kuyruğuna çözülür.

Bir kuruluşun kuyruk yöneticisini (QM2), başka bir kuyruk yöneticisine (QM1) bağlamak için güvenli bir kuruluşa güven, normal kanal kimlik doğrulaması tarafından onaylanır. Bu güvenilir kuruluşun dağıtımlı yayınlama/abone olma izni verilmesine izin verilirse, kanal, yayın iletisini dağıtılmış yayınlama/abone olma yayın kuyruğuna SYSTEM.INTER.QMGR.PUBS' ye koyduğunda bir yetki denetimi yapılır. Kuyruk yetkisi denetiminin kullanıcı kimliği, giriş kanalının PUTAUT değerine bağlıdır (örneğin, kanala ilişkin kullanıcı kimliği, MCAUSER, ileti bağlamı ve diğerleri, değere ve platforma bağlı olarak). Kanal güvenliğiyle ilgili ek bilgi için Kanal güvenliğibaşlıklı konuya bakın.

Yayın iletisi abone olunan kuyruk yöneticisine ulaştığında, konuya ilişkin başka bir MQPUT o kuyruk yöneticisinin yetkisi altında yapılır ve iletiyle bağlam, her bir yerel abonenin her biri ileti verilen her bir yerel abonenin bağlamıyla değiştirilir.



Şekil 31. Yetkili abonelik güvenliği, yayın yayınları

Güvenlikle ilgili olarak küçük sayılan bir sistemde, dağıtılmış yayınlama/abone olma işlemlerinin büyük olasılıkla `mqm` grubundaki bir kullanıcı kimliği altında çalıştırılması, bir kanaldaki `MCAUSER` parametresinin boş olması (varsayılan değer) ve iletilerin gerektiği şekilde çeşitli sistem kuyruklarına teslim edilmeleri olabilir. Güvenli olmayan sistem, dağıtımlı yayınlama/abone olma/abone olma gibi bir kavramın kanıtını ortaya koymayı kolaylaştırıyor.

güvenliğin daha ciddi olarak düşünüldüğü bir sistemde, bu iç mesajlar, kanaldan geçen herhangi bir mesajla aynı güvenlik denetimlerine tabi olur.

If the channel is set up with a non-blank `MCAUSER` and a `PUTAUT` value specifying that `MCAUSER` must be checked, then the `MCAUSER` in question must be granted access to `SYSTEM.INTER.QMGR.*` queues. Farklı `MCAUSER` kimlikleri altında çalışan kanallarla birden çok farklı uzak kuyruk yöneticisi varsa, tüm bu kullanıcı kimliklerinin `SYSTEM.INTER.QMGR.*` kuyruklarına erişim izni verilmesi gerekir. Farklı `MCAUSER` tanıtıcıları altında çalışan kanallar olabilir; örneğin, tek bir kuyruk yöneticiside birden çok sıradüzensel bağlantı yapılandırıldığında.

Kanal, ileti bağlamının kullanıldığını belirten bir `PUTAUT` değeriyle ayarlandıysa, iç iletinin içindeki kullanıcı kimliğine dayalı olarak `SYSTEM.INTER.QMGR.*` kuyruklarına erişim denetlenir. Tüm bu iletiler, iç iletiyi ya da yayın iletisini gönderen kuyruk yöneticisinden dağıtılmış yayınlama/abone olma aracısının kullanıcı kimliği ile konduğu için (bkz. Şekil 31 sayfa 470), dağıtımlı yayınlama/abone olma güvenliğinizi bu şekilde ayarlamak istiyorsanız, çeşitli sistem kuyruklarına (uzak kuyruk yöneticisi başına bir tanesi) erişim izni vermek için çok büyük bir kullanıcı kimliği kümesi değil. Kanal bağlamı güvenliğinin her zaman her zaman sahip olduğu tüm sorunlar vardır; farklı kullanıcı kimliği etki alanları ve iletteki kullanıcı kimliğinin, giriş sisteminde tanımlanmaması gerekir. Ancak gerekirse, bu, gerektiğinde çalıştırılabilmenin son derece kabul edilebilir bir yoludur.

z/OS Sistem kuyruğu güvenliği , kuyrukların listesini ve dağıtılmış yayınlama/abone olma ortamınızı güvenli bir şekilde ayarlamak için gereken erişimi sağlar. Güvenlik ihlalleri nedeniyle herhangi bir iç ileti ya da yayının gönderilememesi durumunda, kanal, günlüğe olağan biçimde bir ileti yazar ve iletiler, olağan kanal hatası işlenmesine göre ölü-mektup kuyruğuna yollanabilir.

Olağan kanal güvenliği kullanılarak, dağıtılmış yayınlama/abone olma amaçları için tüm kuyruk yöneticisi ileti alışverişi yürütülür.

Konu düzeyinde yayınları ve yetkili sunucu aboneliklerini kısıtlamakla ilgili bilgi edinmek için Yayınlama/abone olma güvenliğikonusuna bakın.

Kuyruk yöneticisi sıradüzeniyle varsayılan kullanıcı kimliklerini kullanma

Farklı platformlarda çalışan ve varsayılan kullanıcı kimliklerini kullanan bir kuyruk yöneticisi sıradüzeniniz varsa, bu varsayılan kullanıcı kimliklerinin altyapılar arasında farklılık gösterdiğine ve hedef altyapıda bilinmeyebileceğinin unutulmamasını unutmayın. Sonuç olarak, bir platformda çalışan bir kuyruk

yöneticisi, kuyruk yöneticilerinden alınan iletileri, MQRC_NOT_AUTHORIZEDneden koduyla birlikte diğer platformlarda reddeder.

Reddedilmekte olan iletileri minimum olarak önlemek için, aşağıdaki yetkilerin diğer platformlarda kullanılan varsayılan kullanıcı kimliklerine eklenmesi gerekir:

- *PUT *GET yetkisi SYSTEM.BROKER. Kuyruklar
- *PUB *SUB authority on the SYSTEM.BROKER. Konular
- *ADMCRT *ADMDLT *ADMCHG authority on the SYSTEM.BROKER.CONTROL.QUEUE queue.

Kuyruk yöneticisi sıradüzenine sahip varsayılan kullanıcı kimlikleri aşağıdaki gibidir:

Platform	**Varsayılan kullanıcı kimliği**
Windows	MUSR_MQADMIN
UNIX and Linux sistemleri	mqm
IBM i	QMQM
z/OS	Kanal başlatıcı adres alanı kullanıcı kimliği

Windows, UNIX, Linuxve z/OS platformlarında Kuyruk Yöneticileri için IBM i 'de bir kuyruk yöneticisine hierarchyel olarak eklenirse,' qmqm ' kullanıcı kimliği için erişim yaratın ve bu kullanıcı kimliğine erişim verin.

IBM i ve z/OS platformlarındaki Kuyruk Yöneticileri için Windows, UNIXya da Linux for Queue Manager 'da bir kuyruk yöneticisine hierarchy bağlıysa, 'mqm' kullanıcı kimliği yaratın ve bu tanıtıma erişim izni verin.

Windows, UNIX, Linuxve IBM i platformlarında Kuyruk Yöneticileri için z/OS üzerinde bir kuyruk yöneticisine hierarchyel olarak eklendiyse, z/OS kanal başlatıcı adres alanı kullanıcı kimliğine kullanıcı erişimi yaratın ve bu kullanıcı için kullanıcı erişimi atayın.

Kullanıcı kimlikleri büyük ve küçük harfe duyarlı olabilir. Kaynak kuyruk yöneticisi (IBM i, Windows, UNIXya da Linux sistemleri ise), kullanıcı kimliğini tüm büyük harflere sahip olacak şekilde zorlar. Alıcı kuyruk yöneticisi (Windows, UNIX ya da Linux sistemleri ise), kullanıcı kimliğini tüm küçük harfli olacak şekilde zorlar. Bu nedenle, UNIX and Linux sistemlerinde yaratılan tüm kullanıcı kimlikleri küçük harfli biçimlerinde yaratılmalıdır. Bir ileti çıkışı kurulduysa, kullanıcı kimliğini büyük harfli ya da küçük harfe zorlamak yerine getirmez. İleti çıkışısının kullanıcı kimliğini nasıl işlediğini anlamak için dikkatli olmanız gerekir.

Kullanıcı kimliklerinin dönüştürülmesiyle ilgili olası sorunları önlemek için:

- UNIX, Linux, and Windows sistemlerinde kullanıcı kimliklerinin küçük harfli olarak belirtildiğinden emin olun.
- IBM i ve z/OS' da kullanıcı kimliklerinin büyük harfle belirtildiğinden emin olun.

V 9.1.0 IBM MQ Console ve REST API güvenliği

IBM MQ Console ve REST API güvenliği, mqwebuser.xml dosyasında mqweb sunucusu yapılandırması düzenlenerek yapılandırılır.

Bu görev hakkında

mqweb sunucusunun günlük dosyalarını inceleyerek kullanıcı eylemlerini izleyebilir ve IBM MQ Console ve REST API ' nin kullanımını denetleyebilirsiniz.

IBM MQ Console ve REST API kullanıcılarının kimlikleri doğrulanarak doğrulanabilir:

- Temel kayıt dosyası
- LDAP kaydı
- Yerel İşletim Sistemi Kayıt Dosyası

- SAF on z/OS
- WebSphere Libertytarafından desteklenen başka herhangi bir kayıt dosyası tipi

Roles can be assigned to IBM MQ Console users, and to REST API users to determine what level of access they are granted to IBM MQ objects. Örneğin, ileti sistemini gerçekleştirmek için kullanıcılara `MQWebUser` rolü atanmış olmalıdır. Kullanılabilecek rollerle ilgili daha fazla bilgi için bkz. “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.

Bir kullanıcı bir role atandıktan sonra, kullanıcının kimliğini doğrulamak için kullanılabilecek birçok yöntem vardır. IBM MQ Consoleile kullanıcılar, bir kullanıcı adı ve parolayla oturum açabilir ya da istemci sertifikası kimlik doğrulamasını kullanabilir. REST APIile kullanıcılar temel HTTP kimlik doğrulaması, belirteç tabanlı kimlik doğrulama ya da istemci sertifikası kimlik doğrulaması kullanabilir.

Yordam

1. Define the user registry to authenticate users, and assign each user or group a role to authorize the users and groups to use the IBM MQ Console or REST API. Daha fazla bilg için bkz. “Kullanıcıların ve rollerin yapılandırılması” sayfa 473
2. IBM MQ Console kullanıcısının mqweb sunucusu ile nasıl kimlik doğrulaması gerçekleştireceğini seçin. Tüm kullanıcılar için aynı yöntemi kullanmanıza gerek yoktur:
   - Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. In this case, a user enters a user ID and password at the IBM MQ Console log in screen. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Bu kimlik doğrulama seçeneğini kullanmak için başka bir yapılandırma gerekmez, ancak isteğe bağlı olarak LTPA belirteci için süre bitimi yapılandırabilirsiniz. Daha fazla bilgi için LTPA belirteci süre bitimi aralığının yapılandırılmasıbaşlıklı konuya bakın.
   - İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı IBM MQ Console' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.
3. REST API kullanıcısının mqweb sunucusu ile nasıl kimlik doğrulaması gerçekleştireceğini seçin. Tüm kullanıcılar için aynı yöntemi kullanmanıza gerek yoktur:
   - HTTP temel kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, bir kullanıcı adı ve parola şifrelenir, ancak şifrelenmez ve her bir REST API isteği ile kullanıcıya bu istek için kimlik doğrulaması yapmak ve kullanıcıyı yetkilendirmek için gönderilir. Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Daha fazla bilgi için bkz “Using HTTP basic authentication with the REST API” sayfa 488.
   - Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı, HTTP POST yöntemiyle REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlar. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Daha fazla bilgi için bkz “REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma” sayfa 489.

     Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Ancak HTTP bağlantılarını etkinleştirdiyseniz, HTTP bağlantısı için HTTPS bağlantısı için verilen bir LTPA belirtecinin kullanılmasına izin verebilirsiniz. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
   - İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı REST API' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.
4. İsteğe bağlı: REST APIiçin Cross Origin Resource Sharing 'i yapılandırın.

   Varsayılan olarak bir web tarayıcısı, komut dosyası REST APIile aynı kaynak noktasından değilse, JavaScriptgibi komut dosyalarının REST API ' i çağırmasına izin vermez. Yani, çapraz başlangıç istekleri

etkinleştirilmez. Belirtilen URL ' lerden gelen çapraz kaynak isteklerine izin vermek için Çapraz Kaynak Paylaşımı Paylaşımını (CORS) yapılandırabilirsiniz. Daha fazla bilgi için bkz “Configuring CORS for the REST API” sayfa 492.

5. İsteğe bağlı: IBM MQ Console ve REST APIiçin anasistem üstbilgisi doğrulamasını yapılandırın.

   Yalnızca belirli anasistem üstbilgileri içeren isteklerin IBM MQ Console ve REST APItarafından işlenmesini sağlamak için anasistem üstbilgisi doğrulamasını yapılandırabilir ve anasistem adları ve bağlantı noktalarından oluşan bir allowlist (allowlist) yaratabilirsiniz. Daha fazla bilgi için bkz “IBM MQ Console ve REST APIiçin anasistem üstbilgisi geçerlilik denetiminin yapılandırılması” sayfa 493.

V 9.1.0 Kullanıcıların ve rollerin yapılandırılması

IBM MQ Console ya da REST APIdosyasını kullanabilmek için, kullanıcıların mqweb sunucusu için tanımlanmış bir kullanıcı kayıt defterine karşı kimlik doğrulaması yapması gerekir.

Bu görev hakkında

Kimliği doğrulanmış kullanıcıların, IBM MQ Console ve REST API' in yeteneklerine erişmeye yetki veren gruplardan birinin üyesi olması gerekir. Varsayılan olarak, kullanıcı kaydı herhangi bir kullanıcı içermiyor; bu, `mqwebuser.xml` dosyasının düzenlenmesiyle eklenmelidir.

Kullanıcıları ve grupları yapılandırdığınızda, kullanıcıların ve grupların kimliğini doğrulamak için ilk olarak bir kullanıcı kaydı yapılandırmanızı sağlar. Bu kullanıcı kaydı, IBM MQ Console ile REST APIarasında paylaşılır. Kullanıcılarınız ve gruplarınız için rolleri yapılandırdığınızda, kullanıcıların ve grupların IBM MQ Console, REST APIya da her ikisine erişip erişmediğini denetleyebilirsiniz.

Kullanıcı kaydını yapılandırdıktan sonra, kullanıcılara ve gruplara yetki vermeleri için roller yapılandırırsınız. There are several roles available, including roles specific to using the REST API for Managed File Transfer. Her bir rol farklı bir erişim düzeyi verir. Daha fazla bilgi için bkz “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.

Kullanıcıların ve grupların yapılandırmasını daha basit hale getirmek için mqweb sunucusuyla birlikte bir dizi örnek XML dosyası sağlanır. WebSphere Liberty (WLP) içinde güvenliği yapılandırma konusunda bilgi sahibi olan kullanıcılar, örnekleri kullanmamayı tercih edebilir. WLP, burada belgelenenlerin yanı sıra diğer yetki yetenekleri de sağlar.

Yordam

- Configure users and groups with a basic registry by using the `basic_registry.xml` file.

  Kayıttaki kullanıcı adları ve parolalar, IBM MQ Console ve REST APIkullanıcılarını doğrulamak ve yetkilendirmek için kullanılan kayıttaki kullanıcı adları ve parolalardır.

  To configure a basic registry by using the `basic_registry.xml` sample file, see “IBM MQ Console ve REST APIiçin temel bir kayıt dosyası yapılandırma” sayfa 474.

- `ldap_registry.xml` dosyasını kullanarak, kullanıcıları ve grupları LDAP kayıt defteriyle yapılandırın.

  LDAP kaydındaki kullanıcı adları ve parolalar, IBM MQ Console ve REST APIkullanımını doğrulamak ve bu kullanım için yetkilendirmek için kullanılır.

  To configure an LDAP registry by using the `ldap_registry.xml` sample file, see “IBM MQ Console ve REST APIiçin bir LDAP kaydı yapılandırma” sayfa 478.

- ULW

  `local_os_registry.xml` dosyasını kullanarak yerel bir işletim sistemi kayıt dosyası olan kullanıcıları ve grupları yapılandırın.

  İşletim sistemi kaydındaki kullanıcı adları ve parolalar, IBM MQ Console ve REST APIkullanıcılarını doğrulamak ve yetkilendirmek için kullanılır.

  To configure a local OS registry by using the `local_os_registry.xml` sample file, see “IBM MQ Console ve REST APIiçin yerel işletim sistemi kayıt dosyası yapılandırılması” sayfa 477.

- z/OS
  Configure users and groups with the System authorization facility (SAF) interface on z/OS by using the `zos_saf_registry.xml` file.

  RACF ya da diğer güvenlik ürünü, kullanıcılara ve gruplara rollere erişim vermek için profiller kullanılır. RACF veritabanındaki kullanıcı adları ve parolalar, IBM MQ Console ve REST APIkullanıcılarına kimlik doğrulamak ve kullanıcıları yetkilendirmek için kullanılır.

  SAF arabirimini `zos_saf_registry.xml` örnek dosyasını kullanarak yapılandırmak için bkz. “IBM MQ Console ve REST API için SAF kaydının yapılandırılması” sayfa 480.
- Disable security, including the ability to access the IBM MQ Console, or the REST API, using HTTPS, by using the `no_security.xml` file.

Sonraki adım

Kullanıcıların kimliklerini nasıl doğrulayacağını seçin:

IBM MQ Console Kimlik Doğrulaması Seçenekleri

- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. In this case, a user enters a user ID and password at the IBM MQ Console log in screen. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Bu kimlik doğrulama seçeneğini kullanmak için başka bir yapılandırma gerekmez, ancak isteğe bağlı olarak LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Ek bilgi için LTPA simgesi süre bitimi aralığının yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı IBM MQ Console' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

REST API Kimlik Doğrulaması Seçenekleri

- HTTP temel kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, bir kullanıcı adı ve parola şifrelenir, ancak şifrelenmez ve her bir REST API isteği ile kullanıcıya bu istek için kimlik doğrulaması yapmak ve kullanıcıyı yetkilendirmek için gönderilir. Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Daha fazla bilgi için bkz “Using HTTP basic authentication with the REST API” sayfa 488.
- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı, HTTP POST yöntemiyle REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlar. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Daha fazla bilgi için bkz “REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma” sayfa 489. LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı REST API' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

V 9.1.0 IBM MQ Console ve REST APIiçin temel bir kayıt dosyası yapılandırma

`mqwebuser.xml` dosyası içinde temel bir kayıt dosyası yapılandırabilirsiniz. Xml dosyasındaki kullanıcı adları, parolalar ve roller, IBM MQ Console ve REST APIkullanıcılarının kimliklerini doğrulamak ve kullanıcıları yetkilendirmek için kullanılır.

Başlamadan önce

- Temel kayıt dosyası içinde kullanıcıları yapılandırdığınızda, her kullanıcıya bir rol atamanız gerekir. Her bir rol, IBM MQ Console ve REST API' a erişmek için farklı ayrıcalık düzeyleri sağlar ve izin verilen bir işlem denendiğinde kullanılan güvenlik bağlamını belirler. Temel kayıt defterini yapılandırmadan önce bu rolleri anlamanız gerekir. Rollerin her biri hakkında daha fazla bilgi için bkz. "IBM MQ Console ve REST APIüzerinde roller" sayfa 483.
- Bu görevi tamamlamak için, `mqwebuser.xml` dosyasını düzenlemek için yeterli ayrıcalıklara sahip bir kullanıcı olmanız gerekir:
  - z/OS z/OS' ta, `mqwebuser.xml` dosyasına yazma erişiminiz olmalıdır.
  - Multi Diğer tüm işletim sistemlerinde, ayrıcalıklı bir kullanıcıolmanız gerekir.

Yordam

1. Copy the sample XML file `basic_registry.xml` from one of the following paths:
   - ULW UNIX, Linux, and Windowsüzerinde: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
   - z/OS z/OSüzerinde: `PathPrefix /web/mq/samp/configuration`

   Burada `PathPrefix` , IBM MQ Unix System Services Components kuruluş yoludur.
2. Örnek dosyayı uygun dizine yerleştirin:
   - ULW

     UNIX, Linux, and Windowsüzerinde: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     z/OSüzerinde: *WLP_user_directory*`/servers/mqweb`

     Burada *WLP_user_directory* , mqweb sunucusu tanımlamasını yaratmak için **crtmqweb** komut dosyası çalıştırıldığında belirtilen dizindir.
3. İsteğe bağlı: `mqwebuser.xml`' ta herhangi bir yapılandırma ayarını değiştirdiyseniz, bunları örnek dosyaya kopyalayın.
4. Var olan `mqwebuser.xml` dosyasını silin ve örnek dosyayı `mqwebuser.xml`olarak yeniden adlandırın.
5. **basicRegistry** etiketleri içinde kullanıcılar ve gruplar eklemek için yeni `mqwebuser.xml` dosyasını düzenleyin.

   Be aware that any user with the `MQWebUser` role can perform only the operations that the user ID is granted to perform on the queue manager. Therefore, the user ID defined in the registry must have an identical user ID on the system on which IBM MQ is installed. Bu kullanıcı kimlikleri aynı durumda olmalı ya da kullanıcı kimlikleriyle arasındaki eşleme başarısız olabilir.

   Temel kullanıcı kayıtlarının yapılandırılmasıyla ilgili ek bilgi için, WebSphere Liberty belgelerinde Configuring a basic user registry for Liberty başlıklı konuya bakın.
6. Rolleri kullanıcılara ve gruplara atamak için `mqwebuser.xml` dosyasını düzenleyin:

   Kullanıcıların ve grupların IBM MQ Consoleve REST API' yi kullanması için yetki veren çeşitli roller vardır. Her bir rol farklı bir erişim düzeyi verir. Daha fazla bilgi için bkz "IBM MQ Console ve REST APIüzerinde roller" sayfa 483.
   - Rolleri atamak ve IBM MQ Console' a erişim vermek için kullanıcılarınızı ve gruplarınızı **<enterpriseApplication id="com.ibm.mq.console">** etiketleri içinde uygun **security-role** etiketleri arasında ekleyin.

- Rolleri atamak ve REST API' a erişim vermek için kullanıcılarınızı ve gruplarınızı **<enterpriseApplication id="com.ibm.mq.rest">** etiketleri içinde uygun **security-role** etiketleri arasında ekleyin.

security-role etiketleri içindeki kullanıcı ve grup bilgilerinin biçimine ilişkin yardım almak için örnekler' e bakın.

7. mqwebuser.xml' ta kullanıcılar için parola sağladıysanız, WebSphere Libertytarafından sağlanan **securityUtility encoding** komutunu kullanarak bu parolaları daha güvenli hale getirmek için kodlamalısınız. Ek bilgi için, WebSphere Liberty ürün belgelerindeki Liberty:securityUtility command başlıklı konuya bakın.

Örnek

In the following example, the group MQWebAdminGroup is granted access to the IBM MQ Console with the role MQWebAdmin. The user, reader, is granted access with the role MQWebAdminRO, and the user guest is granted access with the role MQWebUser:

```
<enterpriseApplication id="com.ibm.mq.console">
        <application-bnd>
            <security-role name="MQWebAdmin">
                <group name="MQWebAdminGroup" realm="defaultRealm"/>
            </security-role>
            <security-role name="MQWebAdminRO">
                <user name="reader" realm="defaultRealm"/>
            </security-role>
            <security-role name="MQWebUser">
                <user name="guest" realm="defaultRealm"/>
            </security-role>
        </application-bnd>
    </enterpriseApplication>
```

Aşağıdaki örnekte, reader ve guest kullanıcılarına IBM MQ Consoleerişim yetkisi verilir. The user user is granted access to the REST API, and any users within the MQAdmin group are granted access to the IBM MQ Console and the REST API. mftadmin kullanıcısına MFT için REST API erişim yetkisi verilir:

```
<enterpriseApplication id="com.ibm.mq.console">
    <application-bnd>
        <security-role name="MQWebAdmin">
            <group name="MQAdmin" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebAdminRO">
            <user name="reader" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebUser">
            <user name="guest" realm="defaultRealm"/>
        </security-role>
    </application-bnd>
</enterpriseApplication>

<enterpriseApplication id="com.ibm.mq.rest">
    <application-bnd>
        <security-role name="MQWebAdmin">
            <group name="MQAdmin" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebUser">
            <user name="user" realm="defaultRealm"/>
        </security-role>
        <security-role name="MFTWebAdmin">
            <user name="mftadmin" realm="defaultRealm"/>
        </security-role>
     </application-bnd>
</enterpriseApplication>
```

Sonraki adım

Kullanıcıların kimliklerini nasıl doğrulayacağını seçin:

IBM MQ Console Kimlik Doğrulaması Seçenekleri

- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. In this case, a user enters a user ID and password at the IBM MQ Console log in screen. Kullanıcının

oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Bu kimlik doğrulama seçeneğini kullanmak için başka bir yapılandırma gerekmez, ancak isteğe bağlı olarak LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Ek bilgi için LTPA simgesi süre bitimi aralığının yapılandırılmasıbaşlıklı konuya bakın.

- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı IBM MQ Console' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

REST API Kimlik Doğrulaması Seçenekleri

- HTTP temel kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, bir kullanıcı adı ve parola şifrelenir, ancak şifrelenmez ve her bir REST API isteği ile kullanıcıya bu istek için kimlik doğrulaması yapmak ve kullanıcıyı yetkilendirmek için gönderilir. Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Daha fazla bilgi için bkz “Using HTTP basic authentication with the REST API” sayfa 488.
- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı, HTTP POST yöntemiyle REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlar. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Daha fazla bilgi için bkz “REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma” sayfa 489. LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı REST API' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

ULW V 9.1.0 IBM MQ Console ve REST APIiçin yerel işletim sistemi kayıt dosyası yapılandırılması

`mqwebuser.xml` dosyası içinde yerel bir işletim sistemi kayıt dosyası yapılandırabilirsiniz. Yerel işletim sistemindeki kullanıcı adları ve parolalar, IBM MQ Console ve REST APIkullanıcılarını doğrulamak ve yetkilendirmek için kullanılır.

Başlamadan önce

- Yerel işletim sistemi kimlik doğrulama özelliğiyle istemci sertifikası kimlik doğrulaması için, kullanıcı kimliği istemci sertifikasının ayırt edici adından (DN) ortak addır (CN). Kullanıcı kimliği bir işletim sistemi kullanıcısı olarak yoksa, istemci sertifikası oturum açma işlemi başarısız olur ve parola tabanlı kimlik doğrulamasına geri dönüş yapar.
- Bu görevi tamamlamak için, ayrıcalıklı bir kullanıcıolmanız gerekir.

Bu görev hakkında

Yerel bir işletim sistemi kayıt defteriyle, kullanıcılar ve gruplar otomatik olarak bir role atanır:

- 'mqm' grubunun bir parçası olan ya da IBM iüzerindeki 'QMQMADM' grubunun bir parçası olan herhangi bir kullanıcı MQWebAdmin ve MFTWebAdmin rolleri için verilir.
- Diğer tüm kullanıcılara MQWebUser rolü verilir.

Bu rollerle ilgili daha fazla bilgi için bkz. “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.

Yerel bir işletim sistemi kaydı yalnızca UNIX, Linux, and Windowsüzerinde kullanılabilir. Eşdeğer işlev, bir SAF kayıt dosyası yapılandırılarak z/OS ' ta sağlanır. Daha fazla bilgi için bkz “IBM MQ Console ve REST API için SAF kaydının yapılandırılması” sayfa 480.

Yordam

1. Copy the sample XML file `local_os_registry.xml` from the following path:
   MQ_INSTALLATION_PATH`/web/mq/samp/configuration`
2. Örnek dosyayı aşağıdaki dizine yerleştirin:
   MQ_DATA_PATH`/web/installations/`*installationName*`/servers/mqweb`
3. İsteğe bağlı: `mqwebuser.xml`' ta herhangi bir yapılandırma ayarını değiştirdiyseniz, bunları örnek dosyaya kopyalayın.
4. Var olan `mqwebuser.xml` dosyasını silin ve örnek dosyayı `mqwebuser.xml`olarak yeniden adlandırın.

Sonraki adım

Kullanıcıların kimliklerini nasıl doğrulayacağını seçin:

IBM MQ Console Kimlik Doğrulaması Seçenekleri

- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. In this case, a user enters a user ID and password at the IBM MQ Console log in screen. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Bu kimlik doğrulama seçeneğini kullanmak için başka bir yapılandırma gerekmez, ancak isteğe bağlı olarak LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Ek bilgi için LTPA simgesi süre bitimi aralığının yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı IBM MQ Console' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

REST API Kimlik Doğrulaması Seçenekleri

- HTTP temel kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, bir kullanıcı adı ve parola şifrelenir, ancak şifrelenmez ve her bir REST API isteği ile kullanıcıya bu istek için kimlik doğrulaması yapmak ve kullanıcıyı yetkilendirmek için gönderilir. Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Daha fazla bilgi için bkz “Using HTTP basic authentication with the REST API” sayfa 488.
- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı, HTTP POST yöntemiyle REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlar. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Daha fazla bilgi için bkz “REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma” sayfa 489. LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı REST API' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

V 9.1.0 IBM MQ Console ve REST APIiçin bir LDAP kaydı yapılandırma

`mqwebuser.xml` dosyası içinde bir LDAP kaydı yapılandırabilirsiniz. LDAP kaydındaki kullanıcı adları ve parolalar, IBM MQ Console ve REST APIkullanıcılarının kimliklerini doğrulamak ve kullanıcıları yetkilendirmek için kullanılır.

Başlamadan önce

- Bir LDAP kayıt dosyasını yapılandırdığınızda, her kullanıcıya bir rol atamanız gerekir. Her bir rol, IBM MQ Console ve REST API' a erişmek için farklı ayrıcalık düzeyleri sağlar ve izin verilen bir işlem denendiğinde kullanılan güvenlik bağlamını belirler. Kaydı yapılandırmadan önce bu rolleri anlamanız

gerekir. Rollerin her biri hakkında daha fazla bilgi için bkz. “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.

Be aware that any user with the `MQWebUser` role can perform only the operations that the user ID is granted to perform on the queue manager. Therefore, the user ID defined on the LDAP server must have an identical user ID on the system on which IBM MQ is installed. Bu kullanıcı kimlikleri aynı durumda olmalı ya da kullanıcı kimlikleriyle arasındaki eşleme başarısız olabilir.

- Bu görevi tamamlamak için, `mqwebuser.xml` dosyasını düzenlemek için yeterli ayrıcalıklara sahip bir kullanıcı olmanız gerekir:
  - z/OS z/OS' ta, `mqwebuser.xml` dosyasına yazma erişiminiz olmalıdır.
  - Multi Diğer tüm işletim sistemlerinde, ayrıcalıklı bir kullanıcıolmanız gerekir.

Yordam

1. Copy the sample XML file `ldap_registry.xml` from one of the following paths:
   - ULW UNIX, Linux, and Windowsüzerinde: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
   - z/OS z/OSüzerinde: `PathPrefix /web/mq/samp/configuration`

     Burada `PathPrefix` , IBM MQ Unix System Services Components kuruluş yoludur.
2. Örnek dosyayı uygun dizine yerleştirin:
   - ULW

     UNIX, Linux, and Windowsüzerinde: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     z/OSüzerinde: *WLP_user_directory*`/servers/mqweb`

     Burada *WLP_user_directory* , mqweb sunucusu tanımlamasını yaratmak için **crtmqweb** komut dosyası çalıştırıldığında belirtilen dizindir.
3. İsteğe bağlı: `mqwebuser.xml` ' ta herhangi bir yapılandırma ayarını değiştirdiyseniz, bunları örnek dosyaya kopyalayın.
4. Var olan `mqwebuser.xml` dosyasını silin ve örnek dosyayı `mqwebuser.xml`olarak yeniden adlandırın.
5. **ldapRegistry** ve **idsLdapFilterProperties** etiketlerinde LDAP kayıt ayarlarını değiştirmek için yeni `mqwebuser.xml` dosyasını düzenleyin.

   LDAP kayıt dosyalarını yapılandırma hakkında daha fazla bilgi için, WebSphere Liberty belgelerinde Configuring LDAP user siclars in Liberty başlıklı konuya bakın.
6. Rolleri kullanıcılara ve gruplara atamak için `mqwebuser.xml` dosyasını düzenleyin:

   Kullanıcıların ve grupların IBM MQ Consoleve REST API' yi kullanması için yetki veren çeşitli roller vardır. Her bir rol farklı bir erişim düzeyi verir. Daha fazla bilgi için bkz “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.
   - Rolleri atamak ve IBM MQ Console' a erişim vermek için kullanıcılarınızı ve gruplarınızı **<enterpriseApplication id="com.ibm.mq.console">** etiketleri içinde uygun **security-role** etiketleri arasında ekleyin.
   - Rolleri atamak ve REST API' a erişim vermek için kullanıcılarınızı ve gruplarınızı **<enterpriseApplication id="com.ibm.mq.rest">** etiketleri içinde uygun **security-role** etiketleri arasında ekleyin.

Sonraki adım

Kullanıcıların kimliklerini nasıl doğrulayacağını seçin:

IBM MQ Console Kimlik Doğrulaması Seçenekleri

- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. In this case, a user enters a user ID and password at the IBM MQ Console log in screen. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Bu kimlik doğrulama seçeneğini kullanmak için başka bir yapılandırma gerekmez, ancak isteğe bağlı olarak LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Ek bilgi için LTPA simgesi süre bitimi aralığının yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı IBM MQ Console' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

REST API Kimlik Doğrulaması Seçenekleri

- HTTP temel kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, bir kullanıcı adı ve parola şifrelenir, ancak şifrelenmez ve her bir REST API isteği ile kullanıcıya bu istek için kimlik doğrulaması yapmak ve kullanıcıyı yetkilendirmek için gönderilir. Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Daha fazla bilgi için bkz “Using HTTP basic authentication with the REST API” sayfa 488.
- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı, HTTP POST yöntemiyle REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlar. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Daha fazla bilgi için bkz “REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma” sayfa 489. LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı REST API' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

z/OS V 9.1.0 IBM MQ Console ve REST API için SAF kaydının yapılandırılması

Sistem Yetkilendirme Olanağı (SAF) arabirimi, mqweb sunucusunun kimlik doğrulama ve yetkilendirme denetimi için dış güvenlik yöneticisini çağırmasına olanak sağlar. Daha sonra bir kullanıcı, z/OS kullanıcı kimliği ve parolasıyla IBM MQ Console ve REST API içinde oturum açabilir.

Başlamadan önce

- Bir SAF kaydını yapılandırdığınızda, kullanıcılara bir rol atamanız gerekir. Her rol, IBM MQ Console ve REST API' e erişmek için farklı ayrıcalık düzeyleri sağlar ve izin verilen bir işlem denendiğinde kullanılan güvenlik bağlamını belirler. Kaydı yapılandırmadan önce bu rolleri anlamanız gerekir. Rollerin her biri hakkında daha fazla bilgi için bkz. “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.
- SSF ' ye ilişkin yetkili arabirimi kullanmak için çalışan WebSphere Liberty Angel işlemi gerekir. Ek bilgi için bkz. Liberty üzerinde z/OS yetkili hizmetlerinin z/OS için etkinleştirilmesi .
- Bu görevi tamamlamak için, `mqwebuser.xml` kütüğüne yazma erişiminiz ve güvenlik yöneticisi tanıtımlarını tanımlama yetkinizin olması gerekir.

Not: V 9.1.0.20 IBM MQ 9.1.0 Fix Pack 20olanağından, örnek yapılanış kütüğü `zos_saf_registry.xml` yinelenen bir safAuthorization girişini kaldıracak şekilde güncellenmiştir.

Bu güncelleme, ICH408I hatasının MQ Console on z/OS , WebSphere Liberty Profile 22.0.0.12 ya da sonraki bir yayın düzeyine yükseltildiğinde ortaya çıkabileceği bir sorunu düzeltir: IBM MQ 9.1.0 Fix Pack 15. Birden çok safAuthorization deyiminin olması desteklenmez ve MQWebAdmin ya da MQWebAdminRO rollerinde olmayan kullanıcılar MQ Consolearacılığıyla z/OS kuyruk yöneticisine erişmeye çalıştığında bir ICH408I hatasına neden olabilir.

Günlüğe kaydetme girişimi tiplerini belirten **racRouteLog**için varsayılan değer NONE' dır. Güvenlik denetimi için ek bir rapora ya da kayda gereksinim duyarsanız, daha fazla bilgi için SAF Yetkisi (safAuthorization) başlıklı konuya bakın.

Bu görev hakkında

SAF arabirimi, mqweb sunucusunun IBM MQ Console ve REST APIiçin kimlik doğrulama ve yetkilendirme denetimi için dış güvenlik yöneticisini çağırmasına olanak sağlar.

Yordam

1. mqweb sunucunuza z/OS yetkili hizmetlerini kullanma yetkisi vermek için Liberty üzerinde z/OS yetkili hizmetlerinin z/OS için etkinleştirilmesi içindeki adımları izleyin.

   Melek işlemini başlatmak için örnek JCL USS_ROOT/web/templates/zos/procs/bbgzangl.jcldizininde bulunur; burada USS_ROOT, Unix Sistem Hizmetlerinde IBM MQ for z/OS USS bileşenlerinin kurulu olduğu yoldur.

   bbgzangl.jcliçinde, SET ROOT deyimini USS_ROOT/webdeğerini gösterecek şekilde değiştirin; örneğin, /usr/lpp/mqm/V9R1M0/web.

   Melek sürecini durdurma ve başlatma hakkında daha fazla bilgi için bkz. Administering Liberty on z/OS .
2. Libertyiçin gerekli olan kimliği doğrulanmamış kullanıcıyı oluşturmak için Liberty: System Authorization Facility (SAF) kimliği doğrulanmamış kullanıcısını ayarlama başlıklı konudaki adımları izleyin.
3. zos_saf_registry.xml dosyasını şu yoldan kopyalayın: PathPrefix /web/mq/samp/configuration ; burada PathPrefix , IBM MQ Unix System Services Components kuruluş yoludur.
4. Örnek dosyayı *WLP_user_directory*/servers/mqweb dizinine yerleştirin; burada *WLP_user_directory* , **crtmqweb** komut dosyası mqweb sunucusu tanımlamasını oluşturmak için çalıştırıldığında belirtilen dizindir.
5. İsteğe bağlı: Daha önce mqwebuser.xmliçinde herhangi bir yapılandırma ayarını değiştirdiyseniz, bunları örnek dosyaya kopyalayın.
6. Var olan mqwebuser.xml dosyasını silin ve örnek dosyayı mqwebuser.xmlolarak yeniden adlandırın.
7. mqwebuser.xmliçindeki **safCredentials** öğesini özelleştirin.
   a. **profilePrefix** ' ı Liberty sunucunuz için benzersiz bir ada ayarlayın. Tek bir sistemde çalışan birden çok mqweb sunucunuz varsa, her sunucu için farklı bir ad seçmeniz gerekir; örneğin, MQWEB910 ve MQWEB905.
   b. **unauthenticatedUser** ayarını, “2” sayfa 481. adımda oluşturulan kimliği doğrulanmamış kullanıcının adına ayarlayın.
8. mqweb sunucusu APPLID değerini RACFolarak tanımlayın.

   APPLID kaynak adı, “7” sayfa 481. adımda **profilePrefix** özniteliğinde belirttiğiniz değerdir. Aşağıdaki örnek, RACFiçinde mqweb sunucusu APPLID değerini tanımlar:

   ```
   RDEFINE APPL profilePrefix UACC(NONE)
   ```
9. APPL sınıfındaki mqweb sunucusu APPLID için MQ Console ya da REST API okuma erişimi için kimliği doğrulanacak tüm kullanıcılara ya da gruplara yetki verin.

   Bunu, “2” sayfa 481. adımda tanımlanan kimliği doğrulanmamış kullanıcı için de yapmalısınız. Aşağıdaki örnek, RACFiçinde bir kullanıcıya mqweb sunucusu APPLID 'sine okuma erişimi verir:

   ```
   PERMIT profilePrefix CLASS(APPL) ACCESS(READ) ID(userID)
   ```
10. Kullanıcılara MQ Console ve REST APIiçindeki rollere erişim vermek için gereken EJBROLE sınıfındaki tanıtımları tanımlayın.

Aşağıdaki örnek, RACFiçindeki profilleri tanımlar; burada **profilePrefix** , “7” sayfa 481adımında **profilePrefix** özniteliği için belirtilen değerdir.

```
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdminRO UACC(NONE)
```

11. Kullanıcılara MQ Console ve REST APIiçindeki rollere erişim yetkisi verin.

    Bunu yapmak için, kullanıcılara ya da gruplara “10” sayfa 481. adımda oluşturulan EBJROLE sınıfındaki bir ya da daha fazla tanıtıma okuma erişimi verin. Roller hakkında daha fazla bilgi için bkz. “IBM MQ Console ve REST APIüzerinde roller” sayfa 483.

    Aşağıdaki örnek, RACFiçinde REST API için MQWebAdmin rolüne kullanıcı erişimi verir; burada **profilePrefix** , “7” sayfa 481adımında **profilePrefix** özniteliği için belirtilen değerdir.

```
PERMIT profilePrefix.com.ibm.mq.rest.MQWebAdmin CLASS(EJBROLE) ACCESS(READ) ID(userID)
```

Sonuçlar

IBM MQ Console ve REST APIiçin SAF kimlik doğrulamasını ayarladınız.

Sonraki adım

Kullanıcıların kimliklerini nasıl doğrulayacağını seçin:

IBM MQ Console Kimlik Doğrulaması Seçenekleri

- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. In this case, a user enters a user ID and password at the IBM MQ Console log in screen. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Bu kimlik doğrulama seçeneğini kullanmak için başka bir yapılandırma gerekmez, ancak isteğe bağlı olarak LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Ek bilgi için LTPA simgesi süre bitimi aralığının yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı IBM MQ Console' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

REST API Kimlik Doğrulaması Seçenekleri

- HTTP temel kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, bir kullanıcı adı ve parola şifrelenir, ancak şifrelenmez ve her bir REST API isteği ile kullanıcıya bu istek için kimlik doğrulaması yapmak ve kullanıcıyı yetkilendirmek için gönderilir. Bu kimlik doğrulamasının güvenli olması için güvenli bir bağlantı kullanmanız gerekir. Yani, HTTPS kullanmanız gerekir. Daha fazla bilgi için bkz “Using HTTP basic authentication with the REST API” sayfa 488.
- Belirteç kimlik doğrulamasını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı, HTTP POST yöntemiyle REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlar. Kullanıcının oturum açmış durumda kalmasını ve belirli bir süre için yetkilendirilmesini sağlayan bir LTPA belirteci oluşturulur. Daha fazla bilgi için bkz “REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma” sayfa 489. LTPA belirteci için süre bitimi aralığını yapılandırabilirsiniz. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- İstemci sertifikalarını kullanarak kullanıcıların kimliklerini doğrulamasına izin verin. Bu durumda, kullanıcı REST API' ta oturum açmak için kullanıcı kimliği ya da parola kullanmaz, ancak istemci sertifikasını kullanır. Daha fazla bilgi için bkz “REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması” sayfa 484.

V 9.1.0 IBM MQ Console ve REST APIüzerinde roller

Kullanıcıları ve grupları IBM MQ Console ya da REST API' ı kullanmak üzere yetkilendirdiğinizde, kullanıcıları ve grupları şu rollerden birine atamanız gerekir: **MQWebAdmin**, **MQWebAdminRO**, **MQWebUser**, **MFTWebAdmin**ve **MFTWebAdminRO**. Her bir rol, IBM MQ Console ve REST API' a erişmek için farklı ayrıcalık düzeyleri sağlar ve izin verilen bir işlem denendiğinde kullanılan güvenlik bağlamını belirler.

Not: MQWebUser rolü dışında, kullanıcı kimliği büyük/küçük harfe duyarlı değildir. Bu role ilişkin belirli gereksinimler için “MQWebUser” sayfa 483 ' e bakın.

MQWebAdmin
Bu role atanmış bir kullanıcı ya da grup, tüm denetim işlemlerini gerçekleştirebilir ve mqweb sunucusunu başlatmak için kullanılan işletim sistemi kullanıcı kimliğinin güvenlik bağlamı altında çalışır.

Bu role sahip bir kullanıcı ya da grup şu REST hizmetlerine erişimi yok:

- MFTiçin REST API . Bu hizmetleri kullanmak için, kullanıcı ya da gruba **MFTWebAdmin** ya da **MFTWebAdminRO** rolü atanmış olmalıdır.
- messaging REST API. messaging REST API' ı kullanmak için kullanıcıya **MQWebUser** rolü atanmış olmalıdır.

MQWebAdminRO
This role gives read only access to the IBM MQ Console or REST API. Bu role atanan bir kullanıcı ya da grup aşağıdaki işlemleri gerçekleştirebilir:

- Kuyruklar ve kanallar gibi IBM MQ nesnelerine ilişkin işlemleri görüntüleyin ve sorgulayın.
- Kuyruklardaki iletilere göz atın.

Bu role atanan bir kullanıcı ya da grup, mqweb sunucusunu başlatmak için kullanılan işletim sistemi kullanıcı kimliğinin güvenlik bağlamı altında çalışır.

Bu role sahip bir kullanıcı ya da grup şu REST hizmetlerine erişimi yok:

- MFTiçin REST API . Bu hizmetleri kullanmak için, kullanıcı ya da gruba **MFTWebAdmin** ya da **MFTWebAdminRO** rolü atanmış olmalıdır.
- messaging REST API. messaging REST API' ı kullanmak için kullanıcıya **MQWebUser** rolü atanmış olmalıdır.

MQWebUser
Bu role atanan bir kullanıcı ya da grup, kullanıcı kimliğinin kuyruk yöneticisi üzerinde gerçekleştirmesi için verdiği tüm işlemleri gerçekleştirebilir. Örneğin:

- Kanallar gibi IBM MQ nesnelerine ilişkin işlemleri başlatın ve durdurun.
- IBM MQ nesneleri üzerinde, kuyruklar ve kanallar gibi işlemler tanımlayın ve bunları ayarlayın.
- Kuyruklar ve kanallar gibi IBM MQ nesnelerine ilişkin işlemleri görüntüleyin ve sorgulayın.
- messaging REST APIkomutunu kullanarak ileti alın ve alın.

Bu role atanan bir kullanıcı ya da grup, asıl adın güvenlik bağlamı altında çalışır ve yalnızca kuyruk yöneticisi üzerinde gerçekleştirmek için kullanıcı kimliğinin verildiği işlemleri gerçekleştirebilir.

Bu nedenle, kullanıcının herhangi bir işlem gerçekleştirebilmesi için önce, mqweb kullanıcı kayıt dosyasında tanımlı olan kullanıcı ya da grubun IBM MQ içinde yetki verilmesi gerekir. Bu rolü kullanarak, IBM MQ Console ve REST API' yi kullanırken belirli IBM MQ kaynaklarına hangi kullanıcıların hangi erişim erişimi türünü kullanabileceğini göz altına altabilirsiniz.

Not:

- Bu role atanan kullanıcı kimliği uzunluğu üst sınırı 12 karakterdir.
- Kullanıcı kimliğinin büyük/küçük harf durumu, mqweb kullanıcı kayıt dosyasında ve IBM MQ sisteminde aynı olmalıdır. Kullanıcı kimliğinin durumu farklıysa, kullanıcının kimliği IBM MQ Console ve REST API tarafından doğrulanabilir, ancak IBM MQ kaynaklarını kullanma yetkisi verilmeyebilir.

A user or group with this role does not have access to any of the REST API for MFT services. Bu hizmetleri kullanmak için, kullanıcı ya da gruba **MFTWebAdmin** ya da **MFTWebAdminRO** rolü atanmış olmalıdır.

MFTWebAdmin
Bu role atanan bir kullanıcı ya da grup, tüm MFT REST işlemlerini gerçekleştirebilir ve mqweb sunucusunu başlatmak için kullanılan işletim sistemi kullanıcı kimliğinin güvenlik bağlamı altında çalışır.

Bu role sahip bir kullanıcı ya da grup, IBM MQ REST API hizmetlerinin hiçbirine erişimi yok. Bu hizmetleri kullanmak için, kullanıcı ya da grubun **MQWebAdmin**, **MQWebAdminRO**ya da **MQWebUser** rolü atanmış olması gerekir.

MFTWebAdminRO
This role gives read only access to the REST API for MFT . Bu role atanan bir kullanıcı ya da grup, liste aktarma ve liste aracıları gibi yalnızca okuma işlemleri (GET istekleri) gerçekleştirebilir.

Bu role atanan bir kullanıcı ya da grup, mqweb sunucusunu başlatmak için kullanılan işletim sistemi kullanıcı kimliğinin güvenlik bağlamı altında çalışır.

Bu role sahip bir kullanıcı ya da grup, IBM MQ REST API hizmetlerinin hiçbirine erişimi yok. Bu hizmetleri kullanmak için, kullanıcı ya da grubun **MQWebAdmin**, **MQWebAdminRO**ya da **MQWebUser** rolü atanmış olması gerekir.

Kullanıcıları ve grupları bu rolleri kullanacak şekilde yapılandırmayla ilgili daha fazla bilgi için bkz. “Kullanıcıların ve rollerin yapılandırılması” sayfa 473.

Çakışan roller

Bir kullanıcı ya da gruba birden çok rol atanabilir. Bir kullanıcı bu durumda bir işlem gerçekleştirdiğinde, işlem için geçerli olan en yüksek ayrıcalık rolü kullanılır. Örneğin, **MQWebAdminRO** ve **MQWebUser** rollerine sahip bir kullanıcı bir sorgu kuyruğu işlemi gerçekleştiriyorsa, **MQWebAdminRO** rolü kullanılır ve işlem, web sunucusunu başlatan sistem kullanıcı kimliği bağlamı altında denenir. Aynı kullanıcı bir tanımlama işlemi gerçekleştirirse, **MQWebUser** rolü kullanılır ve işlem, birincil kullanıcı bağlamı altında denenir.

ULW V 9.1.0 REST API ve IBM MQ Consoleile istemci sertifikası kimlik doğrulaması kullanılması

You can map client certificates to principals to authenticate IBM MQ Console and REST API users.

Başlamadan önce

- Configure users, groups, and roles to be authorized to use the IBM MQ Console and REST API. Daha fazla bilgi için bkz “Kullanıcıların ve rollerin yapılandırılması” sayfa 473.
- REST API' ı kullandığınızda, `login` kaynağındaki HTTP GET yöntemini kullanarak geçerli kullanıcının kimlik bilgilerini sorgulayabilir ve isteğin kimlik doğrulaması için istemci sertifikası sağlayabilirsiniz. Bu istek, kullanıcı adına ve kullanıcının atandığı rollere ilişkin bilgileri döndürür. Daha fazla bilgi için bkz. GET `/login`.
- İstemci sertifikalarını kullanıcıların kimliğini doğrulamak üzere birincil kullanıcılar ile eşlediğinizde, yapılandırılan kullanıcı kaydındaki kullanıcılarla eşleştirmek için istemci sertifikasının ayırt edici adı kullanılır:
  - Temel bir kayıt dosyası için, Ortak Ad (CN), kullanıcı ile eşleştirilir. For example, `CN=Fred, O=IBM, C=GB` is matched against a user name of `Fred`.
  - LDAP kayıt dosyası için, varsayılan olarak tam ayırt edici ad LDAP ' a göre eşleştirilir. Eşleştirmeyi özelleştirmek için süzgeçleri ve eşlemeyi ayarlayabilirsiniz. Daha fazla bilgi için, WebSphere Liberty belgelerinde Liberty :LDAP certificate map mode başlıklı konuya bakın.

Bu görev hakkında

Bir kullanıcı istemci sertifikası kullanarak kimlik doğrulamasını gerçekleştirdiğinde, sertifika kullanıcı adı ve parola yerine kullanılır. REST APIiçin istemci sertifikası, kullanıcının kimliğini doğrulamak için her REST isteğiyle birlikte sağlanır. IBM MQ Consoleiçin, bir kullanıcı sertifikayla oturum açtığında, kullanıcı oturumu kapatılamaz.

Yordama göre aşağıdaki bilgiler yer alır:

- `mqwebuser.xml` dosyanızın aşağıdaki örneklerden birine dayalı olduğunu:
  - `basic_registry.xml`
  - `local_os_registry.xml`
  - `ldap_registry.xml`
- UNIX, Linuxya da Windows sistemini kullandığınızı.
- Ayrıcalıklı bir kullanıcısınız.

İstemci sertifikası kimlik doğrulamasını z/OSüzerindeki bir RACF anahtar halkasıyla yapılandırmak için, “Configuring TLS for the REST API and IBM MQ Console on z/OS” sayfa 497içindeki yordamı izleyin.

Not: Aşağıdaki yordam, istemci sertifikalarını IBM MQ Console ve REST APIile kullanmak için gereken adımları özetlemektedir. Geliştirici kolaylığı için, adımlarda kendinden imzalı sertifikaların nasıl oluşturulacağı ve kullanılacağı ayrıntılı bilgiler yer aldı. Ancak, üretim için, bir sertifika yetkilisinden alınan sertifikaları kullanın.

Yordam

1. Komut satırındaki **strmqweb** komutunu girerek mqweb sunucusunu başlatın.
2. İstemci sertifikası yarat:
   a) Bir PKCS#12 anahtar deposu yaratın:
      i) Komut satırına **strmqikm** komutunu girerek IBM Key Management (Anahtar Yönetimi) aracını açın.
      ii) IBM Key Management (Anahtar Yönetimi) aracındaki **Key Database File** (Anahtar Veri Tabanı Dosyası) menüsünden **New**(Yeni) seçeneğini tıklatın.
      iii) **Anahtar veritabanı tipi** listesinden **PKCS12** öğesini seçin.
      iv) Anahtar deposunu kaydetmek için bir yer seçin ve **Dosya Adı** alanına uygun bir ad girin. Örneğin, `user.p12`
      v) İstendiğinde bir parola ayarlayın.
   b) Sertifikayı kendi kendine imzalanmış bir sertifika oluşturarak ya da bir sertifika yetkilisinden bir sertifika edinerek yaratın:
      - Kendinden onaylı sertifika yarat:
        i) **Yeni Kendinden Onaylı**seçeneğini tıklatın.
        ii) **Key Label** (Anahtar Etiketi) alanına `user` girin.
        iii) Temel bir kullanıcı kayıt dosyası kullanıyorsanız, **Ortak Ad** alanına kullanıcı kaydınızdan bir kullanıcı adı girin. Örneğin, `mqadmin`. LDAP kullanıcı kaydı için, sertifikana ilişkin ayırt edici adın LDAP kaydındaki ayırt edici adla eşleştiğinden emin olun.
        iv) **Tamam**'ı tıklatın.
      - Sertifika yetkilisinden bir sertifika alın. CA sertifikası, ayırt edici ad (DN) alanına ilişkin ortak ad (CN) içinde uygun kullanıcı adını içermelidir:
        i) Yeni bir sertifika isteyin. **Yarat** menüsünden **Yeni Sertifika İsteği**öğesini tıklatın.
        ii) **Key Label** (Anahtar Etiketi) alanına sertifika etiketini girin.
        iii) Temel bir kullanıcı kayıt dosyası kullanıyorsanız, **Ortak Ad** alanına sertifikana ilişkin kullanıcının kullanıcı adını girin.

Yerel bir OS kayıt dosyası kullanıyorsanız, **Ortak Ad** alanının yerel işletim sistemi kullanıcı kimliğiyle eşleşmesi gerekir.

LDAP kullanıcı kaydı için, sertifikana ilişkin ayırt edici adın LDAP kaydındaki ayırt edici adla eşleştiğinden emin olun.

iv) Diğer alanlar için geçerli olduğu şekilde, değerleri yazın ya da seçin.

v) Sertifika isteğinin kaydedileceği yeri ve sertifika isteği için dosya adını seçin ve **Tamam**düğmesini tıklatın.

vi) Sertifika isteği dosyasını bir sertifika yetkilisine (CA) gönderin.

vii) Sertifika kuruluşundan sertifikana sahip olduğunda, komut satırına **strmqikm** komutunu girerek IBM Key Management aracını açın.

viii) IBM Key Management (Anahtar Yönetimi) aracındaki **Key Database File** (Anahtar Veri Tabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın.

ix) İstemci sertifikasının bulunduğu PKCS#12 anahtar deposunu seçin. Örneğin, `user.p12`

x) **Al**'ı tıklatın, uygun sertifikayı seçin ve **Tamam**' ı tıklatın.

3. İstemci sertifikasının genel kısmını çıkarın:
   a) Komut satırına **strmqikm** komutunu girerek IBM Key Management (Anahtar Yönetimi) aracını açın.
   b) IBM Key Management (Anahtar Yönetimi) aracındaki **Key Database File** (Anahtar Veri Tabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın.
   c) İstemci sertifikasının bulunduğu PKCS#12 anahtar deposunu seçin. Örneğin, `user.p12`
   d) IBM Key Management aracındaki sertifika listesinden istemci sertifikasını seçin.
   e) **Sertifikayı Çek**düğmesini tıklatın.
   f) Sertifikayı kaydetmek için bir yer seçin ve **Sertifika dosyası adı** alanına uygun bir dosya adı girin. Örneğin, `user.arm`.
4. İstemci sertifikasının genel kısmını, sunucunun istemci sertifikasının geçerliliğini denetleyebilmesi için imzalayıcı sertifikası olarak mqweb sunucusu güven anahtar deposuna aktarın:
   a) Önceden yoksa, mqweb sunucusu tarafından kullanılmak üzere bir `trust.jks` anahtar deposu yaratın:
      i) IBM Key Management (Anahtar Yönetimi) aracındaki **Key Database File** (Anahtar Veri Tabanı Dosyası) menüsünden **New**(Yeni) seçeneğini tıklatın.
      ii) **Anahtar veritabanı tipi** listesinden **JKS** öğesini seçin.
      iii) **Göz At** ' ı tıklatın ve şu şekilde gidin: `MQ_DATA_DIRECTORY/web/installations/installationName/servers/mqweb/resources/security`.

      Bu dizin zaten bir `key.jks` dosyası içermelidir. Bir `trust.jks` dosyası önceden varsa, var olan bir dosyayı açmak yerine, var olan bir dosya açın.
      iv) **File Name** (Dosya Adı) alanına `trust.jks` girin.
      v) İstendiğinde bir parola ayarlayın.
   b) Açılan menüden **Signer Certificates**(İmzalayıcı Sertifikaları) öğesini seçin.
   c) **Ekle**'yi tıklatın.
   d) Uygun kol dosyasını seçin ve **Tamam**' ı tıklatın. Örneğin, `user.arm`seçeneğini belirleyin.
   e) Sertifika için bir etiket girin.
5. mqweb sunucusu anahtar deposuna ilişkin parolayı değiştirin:
   a) **Key Database File** (Anahtar Veritabanı Dosyası) menüsünden **Open**(Aç) seçeneğini tıklatın.
   b) **Anahtar veritabanı tipi** listesinden **JKS** öğesini seçin.
   c) **Göz At** 'ı tıklatın ve *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb/resources/security`' a gidin
   d) `key.jks` anahtar deposunu seçin ve **Aç**' ı tıklatın.

e) İstendiğinde parolayı girin. Varsayılan parola `password`' dir.

f) **Key Database File** (Anahtar Veri Tabanı Dosyası) menüsünden **Change Password**(Parolayı Değiştir) seçeneğini tıklatın.

g) Anahtar deposu için yeni bir parola girin.

6. `mqwebuser.xml` dosyasında istemci sertifikası kimlik doğrulamasını etkinleştir:

   `mqwebuser.xml` dosyası şu yolda bulunabilir: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`

   a) Uncomment the section in the `mqwebuser.xml` file that enables client certificate authentication. Bölüm aşağıdaki metni içerir:

   ```
   <keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
       <keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
       <ssl id="thisSSLConfig" clientAuthenticationSupported="true"
   keyStoreRef="defaultKeyStore"
              trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"
   serverKeyAlias="default"/>
       <sslDefault sslRef="thisSSLConfig"/>
   ```

   b) **serverKeyAlias** değerinin sunucu sertifikasının adıyla eşleşip eşleştiğini denetleyin. Varsayılan sunucu sertifikasını kullanıyorsanız, değer doğru olur.

   c) `defaultKeyStore` için **parola** değerini, `key.jks` anahtar deposu parolasının kodlanmış bir sürümüne çevirin:

      i) *MQ_INSTALLATION_PATH*`/web/bin` dizininden, komut satırına aşağıdaki komutu girin:

      ```
      securityUtility encode password
      ```

      ii) Bu komutun çıktısını, `defaultKeyStore`için **parola** alanına yerleştirin.

   d) Change the value for **parola** for the `defaultTrustStore` to match the password for the `trust.jks` keystore:

      i) *MQ_INSTALLATION_PATH*`/web/bin` dizininden, komut satırına aşağıdaki komutu girin:

      ```
      securityUtility encode password
      ```

      ii) Bu komutun çıktısını, `defaultTrustStore`için **parola** alanına yerleştirin.

   e) `mqwebuser.xml` kütüğünden aşağıdaki satırı kaldırın ya da kaldırın:

   ```
   <sslDefault sslRef="mqDefaultSSLConfig"/>
   ```

7. Komut satırındaki **endmqweb** komutunu girerek mqweb sunucusunu durdurun.
8. Komut satırındaki **strmqweb** komutunu girerek mqweb sunucusunu başlatın.
9. Kimlik doğrulamak için istemci sertifikasını kullan:

   - İstemci sertifikasını IBM MQ Consoleile kullanmak için istemci sertifikasını, IBM MQ Console' a erişmek için kullanılan web tarayıcısına kurun. Örneğin, `user.p12` istemci sertifikasını kişisel sertifika olarak kurun.
   - İstemci sertifikasını REST APIile kullanmak için, her bir REST isteğiyle istemci sertifikasını sağlayın. HTTP POST, PATCH ya da DELETE yöntemleri kullanırken, siteler arası istek sahteciliği saldırılarını önlemek için istemci sertifikasıyla ek kimlik doğrulaması sağlamanız gerekir. Yani, isteğin kimlik doğrulaması için kullanılan kimlik bilgilerinin, kimlik bilgilerinin sahibi tarafından kullanıldığını doğrulamak için ek kimlik doğrulaması kullanılır.

     Bu fazladan kimlik doğrulaması, `ibm-mq-rest-csrf-token` HTTP üstbilgisi tarafından sağlanır. Set the value of the `ibm-mq-csrf-token` header to anything including blank, then submit the request.

Örnek

Önemli: Örnekte, tüm cURL somutlamaları kendinden imzalı sertifikaları desteklemez, bu nedenle, ilgili bir cURL somutlaması kullanmanız gerekir.

Aşağıdaki cURL örneği, istemci sertifikası kimlik doğrulaması ile QM1kuyruk yöneticisi üzerinde Q1yeni bir kuyruğun nasıl yaratılacağı gösterilmektedir. Bu cURL komutunun tam yapılandırması, cURL tarafından oluşturulan kitaplıklara bağlıdır. The example is based on a Windows system, with cURL built against OpenSSL.

- Use the HTTP POST method with the queue resource, authenticating with the client certificate and including the `ibm-mq-rest-csrf-token` HTTP header with an arbitrary value. Bu değer, boşluk da içinde olmak üzere her şey olabilir. `--cert-type` işareti, sertifikanda bir PKCS#12 sertifikası olduğunu belirtir. `--cert` işareti sertifikana ilişkin konumu belirtir, ardından iki nokta üst üste işareti (:) ve sertifika için parolayı belirtir:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -
-cert-type P12 --cert c:\user.p12:password
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 Using HTTP basic authentication with the REST API

REST API kullanıcıları, bir HTTP üstbilgisinde kullanıcı kimliği ve parola sağlayarak kimlik doğrulaması yapabilir. Bu kimlik doğrulama yöntemini, POST, PATCH ve DELETE gibi HTTP yöntemleriyle kullanmak için, `ibm-mq-rest-csrf-token` HTTP üstbilgisinin yanı sıra bir kullanıcı kimliği ve parola da sağlanmalıdır.

Başlamadan önce

- Configure users, groups, and roles to be authorized to use the REST API. Daha fazla bilgi için bkz "Kullanıcıların ve rollerin yapılandırılması" sayfa 473.
- HTTP temel kimlik doğrulamasının etkinleştirildiğinden emin olun. Aşağıdaki XML ' in var olduğunu ve `mqwebuser.xml` dosyasında açıklama yapılmadığını denetleyin. Bu XML ' in `<featureManager>` etiketleri içinde olması gerekir:

```
<feature>basicAuthenticationMQ-1.0</feature>
```

z/OS z/OS'ta, bu dosyayı düzenlemek için `mqwebuser.xml` ' a yazma erişimi olan bir kullanıcı olmanız gerekir.

Multi Diğer tüm işletim sistemlerinde, `mqwebuser.xml` dosyasını düzenlemek için bir ayrıcalıklı kullanıcı olmanız gerekir.

- REST istekleri gönderirken güvenli bir bağlantı kullandığınızdan emin olun. Kullanıcı adı ve parola birleşimi kodlandığında, ancak şifrelenmemiş olarak, REST APIile HTTP temel kimlik doğrulaması kullandığınızda güvenli bir bağlantı (HTTPS) kullanmanız gerekir.
- You can query the credentials of the current user by using the HTTP GET method on the `login` resource, providing the basic authentication information to authenticate the request. Bu istek, kullanıcı adına ve kullanıcının atandığı rollere ilişkin bilgileri döndürür. Daha fazla bilgi için bkz. GET `/login`.

Yordam

1. Kullanıcı adını iki nokta üst üste ve parolayla bitiştirin. Kullanıcı adının büyük ve küçük harfe duyarlı olduğunu unutmayın.

   Örneğin, admin kullanıcı adı ve yönetici parolası aşağıdaki dizgi olur:

   ```
   admin:admin
   ```

2. Bu kullanıcı adı ve parola dizesini base64 kodlamasında kodlayın.

3. Bu kodlanmış kullanıcı adını ve parolayı bir HTTP `Authorization: Basic` üstbilgisinde ekleyin.
   Örneğin, bir kodlanmış kullanıcı admin ve admin parolasıyla aşağıdaki üstbilgi yaratılır:

   ```
   Authorization: Basic YWRtaW46YWRtaW4=
   ```

4. HTTP POST, PATCH ya da DELETE yöntemleri kullandığınızda, kullanıcı adı ve parola gibi ek kimlik doğrulamayı da sağlamanız gerekir.
   Bu fazladan kimlik doğrulaması, `ibm-mq-rest-csrf-token` HTTP üstbilgisi tarafından sağlanır. `ibm-mq-rest-csrf-token` HTTP üstbilgisi istekte var olmalıdır, ancak değeri boşluk da içinde olmak üzere herhangi bir şey olabilir.
5. REST isteğinizi uygun üstbilgilerle IBM MQ ' e gönderin.

Örnek

The following example shows how to create a new queue Q1, on queue manager QM1, with basic authentication, on Windows systems. Örnek, cURL' yi kullanır:

- HTTP POST yöntemini kuyruk kaynağıyla birlikte kullanarak, temel kimlik doğrulamasıyla ve isteğe bağlı bir değerle `ibm-mq-rest-csrf-token` HTTP üstbilgisi dahil olmak üzere kimlik doğrulamanız gerekir. Bu değer, boşluk da içinde olmak üzere her şey olabilir:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST
  -u mqadmin:mqadmin
  -H "ibm-mq-rest-csrf-token: value"
  -H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
  ```

V 9.1.0 REST API 'si ile simgeli tabanlı kimlik doğrulaması kullanma

REST API kullanıcıları, HTTP POST yöntemi ile REST API `login` kaynağına bir kullanıcı kimliği ve parola sağlayarak kimlik doğrulaması yapabilir. Kullanıcının gelecekteki istekleri doğrulamasına olanak sağlayan bir LTPA belirteci oluşturulur. Bu LTPA belirteci `LtpaToken2`önekine sahip. Kullanıcı, HTTP DELETE yöntemini kullanarak oturum açabilir ve HTTP GET yöntemiyle yürürlükteki kullanıcının oturum açma bilgilerini sorgulayabilir.

Başlamadan önce

- Configure users, groups, and roles to be authorized to use the REST API. Daha fazla bilgi için bkz “Kullanıcıların ve rollerin yapılandırılması” sayfa 473.
- Varsayılan olarak, LTPA belirtecini içeren tanımlama bilgisinin adı `LtpaToken2`ile başlar ve mqweb sunucusu yeniden başlatıldığında değiştirebilecek bir sonek içerir. Bu rasgele tanımlama bilgisi adı, birden çok mqweb sunucusunun aynı sistemde çalışmasına olanak sağlar. However, if you want the cookie name to remain a consistent value, you can specify the name that the cookie has by using the **setmqweb** command. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- Varsayılan olarak, LTPA belirteci tanımlama bilgisinin süresi 120 dakikadan sonra doluyor. You can configure the expiry time of the LTPA token cookie by using the **setmqweb** command. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- REST istekleri gönderirken güvenli bir bağlantı kullandığınızdan emin olun. `login` kaynağında HTTP POST yöntemini kullandığınızda, istekle birlikte gönderilen kullanıcı adı ve parola birleşimi şifrelenmez. Therefore, you must use a secure connection (HTTPS) when you use token based authentication with the REST API. Varsayılan olarak, LTPA belirteci kimlik doğrulamasıyla HTTP ' yi kullanamazsınız. You can enable the LTPA token to be used by insecure HTTP connections by setting **secureLTPA** to `False`. Daha fazla bilgi için LTPA simgesinin yapılandırılmasıbaşlıklı konuya bakın.
- You can query the credentials of the current user by using the HTTP GET method on the `login` resource, providing the LTPA token to authenticate the request. Bu istek, kullanıcı adına ve kullanıcının atandığı rollere ilişkin bilgileri döndürür. Daha fazla bilgi için bkz. GET `/login`.

Yordam

1. Bir kullanıcıda oturum açın:
   a) `login` kaynağı üzerinde HTTP POST yöntemini kullanın:

   ```
   https://host:port/ibmmq/rest/v1/login
   ```

   JSON isteğinin gövdesine kullanıcı adı ve parolayı aşağıdaki biçimde ekleyin:

   ```
   {
       "username" : name,
       "password" : password
   }
   ```

   b) Yerel çerez mağazasındaki istekten döndürülen LTPA belirtecini saklayın. Varsayılan olarak, bu LTPA belirteci `LtpaToken2`önekine sahiptir.
2. Saklanan LTPA belirteciyle REST isteklerini, her istekle birlikte bir tanımlama bilgisi olarak doğrulayın.
   HTTP PUT, PATCH ya da DELETE yöntemleri kullanan istekler için bir `ibm-mq-rest-csrf-token` üstbilgisi ekleyin. Bu üstbilginin değeri, boşluk da içinde olmak üzere herhangi bir şey olabilir.
3. Kullanıcı oturumunu kapatın:
   a) `login` kaynağıdaki HTTP DELETE yöntemini kullanın:

   ```
   https://host:9443/ibmmq/rest/v1/login
   ```

   İsteği doğrulamak için LTPA simgesini bir tanımlama bilgisi olarak sağlamalı ve bir `ibm-mq-rest-csrf-token` üstbilgisi içermelisiniz. Bu üstbilginin değeri boşluk da içinde olmak üzere her şey olabilir.

   b) Yönergeyi, LTPA simgesini yerel tanımlama bilgisi deposundan silme yönergesini işlet.

   Not: Yönerge işlenmezse ve LTPA simgesi yerel tanımlama bilgisi deposunda kaldıysa, gelecekteki REST isteklerinin kimliğini doğrulamak için LTPA simgesi kullanılabilir. Yani, kullanıcı oturum sona erdirildikten sonra LTPA belirteciyle kimlik doğrulaması gerçekleştirmeye çalıştığında, var olan simgeyi kullanan yeni bir oturum yaratılır.

Örnek

The following cURL example shows how to create a new queue Q1, on queue manager QM1, with token-based authentication, on Windows systems:

- Oturum açın ve LTPA belirtecini `LtpaToken2`önekiyle yerel tanımlama bilgisi deposuna ekleyin. Kullanıcı adı ve parola bilgileri JSON gövdesine dahil edilir. `-c` işareti, simgenin saklanacak dosyanın yerini belirtir:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/login -X POST
  -H "Content-Type: application/json" --data
  "{\"username\":\"mqadmin\",\"password\":\"mqadmin\"}"
  -c c:\cookiejar.txt
  ```

- Bir kuyruk yaratın. HTTP POST yöntemini, kuyruk kaynağı ile birlikte kullanarak, LTPA belirteciyle kimlik doğrulamanız gerekir. The LTPA token with the prefix `LtpaToken2` is retrieved from the `cookiejar.txt` file by using the `-b` flag. CSRF koruması, `ibm-mq-rest-csrf-token` HTTP üstbilgisinin varlığı tarafından sağlanır:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -b
  c:\cookiejar.txt -H "ibm-mq-rest-csrf-token: value" -H "Content-Type: application/json"
  --data "{\"name\":\"Q1\"}"
  ```

- Oturumu kapatın ve yerel tanımlama bilgisinden LTPA simgesini silin. LTPA simgesi, `-b` işaretiyle `cookiejar.txt` dosyasından alınır. CSRF koruması, `ibm-mq-rest-csrf-token` HTTP üstbilgisinin

varlığı tarafından sağlanır. The location of the `cookiejar.txt` file is specified by the `-c` flag so that the LTPA token is deleted from the file:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X DELETE
-H "ibm-mq-rest-csrf-token: value" -b c:\cookiejar.txt
-c c:\cookiejar.txt
```

İlgili başvurular

POST /login

GET /login

SİL /login

V 9.1.3 IBM MQ Console ' ı IFrame içine gömme

HTML < iframe> öğesi, bir Web sayfasını bir Inline Frame (IFrame) kullanarak başka bir web sayfasını başka bir yere yerleştirmek için kullanılabilir. Güvenlik nedeniyle, IBM MQ Console varsayılan olarak bir IFrame içine gömülemez. Ancak, bir IFrame 'i, mqweb sunucusundaki **mqConsoleFrameAncestors** configuration özelliğini kullanarak etkinleştirebilirsiniz.

Bu görev hakkında

The mqweb server maintains an allowlist of origins of web pages which can embed the IBM MQ Console using an IFrame. Başlangıç noktası, bir URL şemasının, etki alanının ve kapının birleşimidir, örneğin, `https://example.com:1234`.

Listedeki girdileri belirtmek için mqweb sunucusunda **mqConsoleFrameAncestors** yapılandırma özelliğini kullanabilirsiniz.

Varsayılan olarak **mqConsoleFrameAncestors** boştur; bu da IBM MQ Console ' nin bir IFrame 'e katılamayabileceği anlamına gelir.

Yordam

Specify a list of origins of web pages, that can embed the IBM MQ Console in an IFrame, by entering the following command:

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

Burada *allowedOrigins* , kökenlerin virgülle ayrılmış bir listesidir. Her bir başlangıç noktası şunlardan oluşmalıdır:

- Anasistem adı ya da IP adresi
- İsteğe bağlı bir URL şeması
- İsteğe bağlı kapı numarası

Anasistem adının genel arama karakteri (*) ile başlayabileceğini ve kapı numarasının genel arama karakteri (*) de kullanabileceğini unutmayın.

Örnek kökenler şunlardır:

```
https://example.com:1234
```

which allows any web page served from `https://example.com:1234` to embed the IBM MQ Console in an IFrame.

```
https://*.example.com:*
```

which allows any HTTPS web page with a hostname ending with `example.com`, and using any port, to embed the IBM MQ Console in an IFrame.

Örnek

Aşağıdaki örnek, IBM MQ Console 'un `https://site2.example.com:1234` ya da `https://site2.example.com:1235`' tan hizmet edilen web sayfalarından bir IFrame içine yerleştirilmesine olanak sağlar:

```
setmqweb properties -k mqConsoleFrameAncestors -v
https://site2.example.com:1234,https://site2.example.com:1235
```

V 9.1.0 Configuring CORS for the REST API

Varsayılan olarak bir web tarayıcısı, komut dosyası REST APIile aynı kaynak noktasından değilse, JavaScriptgibi komut dosyalarının REST API ' i çağırmasına izin vermez. Yani, çapraz başlangıç istekleri etkinleştirilmez. Çapraz köken istekleri belirtilen kökenlerden izin vermek için Çapraz Kaynak Paylaşımı Paylaşımını (CORS) yapılandırabilirsiniz.

Bu görev hakkında

REST API ' a bir web tarayıcısıyla (örneğin, bir komut dosyası aracılığıyla) erişebilirsiniz. Bu istekler farklı bir kaynaktan REST API' a geldikçe, web tarayıcısı çapraz kaynak isteği olduğu için isteği reddeder. Etki alanı, kapı ya da şema aynı değilse, kaynak farklı olur.

For example, if you have a script that is hosted at `http://localhost:1999/` you make a cross-origin request if you issue an HTTP GET on a website that is hosted at `https://localhost:9443/`. Kapı numaraları ve şema (HTTP) farklı olduğundan, bu istek bir çapraz başlangıç isteğidir.

CORS 'yi yapılandırarak ve REST API' a erişmesine izin verilen kökenleri belirterek, çapraz kökenli istekleri etkinleştirebilirsiniz.

CORS ile ilgili daha fazla bilgi için bkz. https://www.w3.org/TR/cors/ ve https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS.

Yordam

1. Aşağıdaki komutu girerek geçerli yapılandırmayı görüntüleyin:

   `dspmqweb properties -a`

   `mqRestCorsAllowedOrigins` girişi, izin verilen kökenleri belirtir. `mqRestCorsMaxAgeInSeconds` girdisi, web tarayıcısının herhangi bir CORS uçuş öncesi denetiminde sonuçları önbelleğe alabileceği süreyi saniye cinsinden belirtir.
2. Aşağıdaki komutu girerek REST API ' a erişmesine izin verilen kökenleri belirtin:

   `setmqweb properties -k mqRestCorsAllowedOrigins -v` *`allowedOrigins`*

   Burada *allowedOrigins* , çapraz kaynak isteklerine izin vermek istediğiniz başlangıç noktasını belirtir. Tüm çapraz kaynak isteklerine izin vermek için çift tırnak imi, "*" ile çevrili bir yıldız işareti kullanabilirsiniz. Virgülle ayrılmış bir listede, çift tırnak işaretiyle çevrelenmiş birden çok kaynak girebilirsiniz. Çapraz köken isteklerine izin vermek için, *allowedOrigins*değeri olarak boş tırnak işaretleri girin.
3. Aşağıdaki komutu girerek, bir Web tarayıcısına, CORS uçuş öncesi denetimlerinin sonuçlarını önbelleğe almak için izin vermek istediğiniz süreyi (saniye cinsinden) belirtin:

   `setmqweb properties -k mqRestCorsMaxAgeInSeconds -v` *`time`*

Örnek

Aşağıdaki örnek, `http://localhost:9883`, `https://localhost:1999`ve `https://localhost:9663`için etkinleştirilen çapraz başlangıç isteklerini göstermektedir. CORS uçuş öncesi denetimleri için önbelleğe alınan sonuç sayısı üst sınırı 90 saniyeye ayarlıdır:

```
setmqweb properties -k mqRestCorsAllowedOrigins -v "http://localhost:9883,https://
localhost:1999,https://localhost:9663"
setmqweb properties -k mqRestCorsMaxAgeInSeconds -v 90
```

IBM MQ Console ve REST APIiçin anasistem üstbilgisi geçerlilik denetiminin yapılandırılması

You can configure the mqweb server to restrict access to the IBM MQ Console and REST API such that only requests that are sent with a host header that matches a specified allowlist are processed. Allowlist 'te olmayan bir anasistem üstbilgi değeri kullanılırsa bir hata döndürülür.

Bu görev hakkında

mqweb sunucusu, kabul edilebilir anasistem üstbilgilerinin allowlist 'i tanımlamak için sanal anasistemleri kullanır. Sanal anasistemler hakkında daha fazla bilgi için, WebSphere Liberty belgelerine bakın: https://www.ibm.com/docs/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/cwlp_virtual_hosts.html

Bu görevi tamamlamak için, `mqwebuser.xml` dosyasını düzenlemek için yeterli ayrıcalıklara sahip bir kullanıcı olmanız gerekir:

- z/OS z/OS' ta, `mqwebuser.xml` dosyasına yazma erişiminiz olmalıdır.
- Multi Diğer tüm işletim sistemlerinde, ayrıcalıklı bir kullanıcıolmanız gerekir.

Yordam

1. `mqwebuser.xml` dosyasını açın. Bu dosya aşağıdaki konumlardan birinde yer alıyor:
   - ULW

     UNIX, Linux, and Windowsüzerinde: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     z/OSüzerinde: *WLP_user_directory*`/servers/mqweb`

     Burada *WLP_user_directory* , mqweb sunucusu tanımlamasını yaratmak için **crtmqweb** komut dosyası çalıştırıldığında belirtilen dizindir.
2. `mqwebuser.xml` dosyasına aşağıdaki kodu ekleyin ya da bu kodu açıklama satırı kaldırın:

   ```
   <virtualHost allowFromEndpointRef="defaultHttpEndpoint" id="default_host">
           <hostAlias>localhost:9080</hostAlias>
   </virtualHost>
   ```
3. Edit the **<hostAlias>** field, inserting the hostname and port combination that you want to allow.

   Bu birleşim, mqweb sunucusunun yapılanışında kullandığınız anasistem adı ve kapı adı olabilir. For example, if you use the default configuration of `localhost:9443`, you might want to use `localhost:9443` in the **<hostAlias>** field.

   Gerekirse, daha fazla anasistem adı ve kapı birleşimleri sağlamak için **<virtualHost>** etiketleri içinde birden çok **<hostAlias>** alanı ekleyebilirsiniz. Örneğin, HTTP kapısı kullanan anasistem üstbilgilerinin yanı sıra, HTTPS kapısını kullanan anasistem üstbilgilerine izin vermek için.

V 9.1.0 Denetleme

Audit records of operations performed in the IBM MQ Console and REST API can be produced by enabling queue manager command and configuration events, and on UNIX, Linux, and Windows significant state changes are recorded in the log files of the mqweb server.

Önemli durum değişiklikleri

ULW

UNIX, Linux, and Windows' ta, IBM MQ Console , önemli durum değişikliklerini mqweb sunucusunun günlüklerinde ileti olarak kaydeder. Her ileti, işlemi isteyen kimliği doğrulanan birincil kullanıcı adını belirtir.

Kuyruk yöneticilerinin oluşturulduğu, başlatıldığı, sona erdirildiği ya da silindiği gibi önemli durum değişiklikleri, mqweb sunucusu `messages.log` ve `console.log` dosyalarında [AUDIT] günlük kaydı düzeyinde günlüğe kaydedilir. Her bir günlük girişi, işlemi isteyen doğrulanmış birincil kullanıcı adını belirtir.

`messages.log` ve `console.log` dosyaları aşağıdaki konumda bulunabilir:

- ULW UNIX, Linux, and Windowsüzerinde: *MQ_DATA_PATH*\web\installations*installationName*\servers\mqweb\logs

mqweb sunucusu günlük kaydı düzeylerinin yapılandırılmasına ilişkin ek bilgi için Günlüğe kaydetme özelliğinin yapılandırılmasıbaşlıklı konuya bakın.

Komut ve yapılandırma olayları

İsteğe bağlı olarak, çoğu IBM MQ Console ve REST API etkinliği hakkında bilgi sağlamak için kuyruk yöneticilikteki komut ve yapılandırma olaylarını etkinleştirebilirsiniz. Örneğin, kanalların yaratılması ve kuyrukların sorgusu komut ve yapılandırma olayları oluşturur. Komut ve yapılandırma olaylarını etkinleştirme hakkında daha fazla bilgi için Yapılandırma, komut ve günlüğe kaydedici olaylarını denetlemebaşlıklı konuya bakın.

Bu komut ve yapılanış olayı iletileri için, MQIACF_EVENT_ORIGIN alanı MQEVO_REST olarak ayarlanır ve MQCACF_EVENT_APPL_IDENTITY alanı, kimliği doğrulanan birincil kullanıcı adının ilk 32 karakterini bildirir. Bir kullanıcının **MQWebAdmin** ya da **MQWebAdminRO** rolü varsa, MQCACF_EVENT_USER_ID alanı, komutu yayınlayan birincil kullanıcının kullanıcı adını değil, mqweb sunucusu kullanıcı kimliğini bildirir. Ancak, kullanıcının **MQWebUser** rolü varsa, MQCACF_EVENT_USER_ID komutu, komutu veren birincil kullanıcının adını bildirir.

İlgili kavramlar

“Denetleme” sayfa 440
Olay iletilerini kullanarak, güvenlik izinsiz girişlerinin ya da izinsiz girişlerin denenmesini denetleyebilirsiniz. Ayrıca, IBM MQ Explorerkomutunu kullanarak sisteminizin güvenliğini denetleyebilirsiniz.

Security considerations for the IBM MQ Console and REST API on z/OS

IBM MQ Console ve REST API , bir kullanıcının komutları yayınlayıp yayınlayamayacağını, görüntüleyebileceğini ya da değiştirebileceğini denetleyen güvenlik özelliklerine sahiptir. Daha sonra, komutlar kuyruk yöneticisine geçirilir ve kullanıcının bu belirli kuyruk yöneticisine komutu vermesine izin verilip verilmediğini denetlemek için kuyruk yöneticisi güvenliği kullanılır.

Yordam

1. Mqweb sunucusu başlatılmış görev kullanıcı kimliğinin, belirli PCF komutlarını vermek ve belirli kuyruklara erişmek için uygun yetkilerine sahip olduğundan emin olun. Daha fazla bilgi için bkz “Mqweb sunucusu tarafından gerekli olan yetki, görev kullanıcı kimliğini başlattı” sayfa 495.
2. `MQWebUser` rolüne sahip kullanıcıların uygun yetkilerine sahip olduğundan emin olun.

`MQWebUser` rolüne atananIBM MQ Console ve REST API kullanıcıları, asıl adın güvenlik bağlamı altında çalışır. Bu kullanıcı kimlikleri yalnızca, kullanıcı kimliğinin kuyruk yöneticisi üzerinde gerçekleştirmek için izin verdiği işlemleri gerçekleştirebilir ve mqweb sunucusu adres alanıyla aynı sistem kuyruklarına erişim izni verilmesi gerekir.

Mqweb sunucusu başlatılan görev kullanıcı kimliğine, `MQWebUser` rolüne atanan tüm kullanıcılara başka bir kullanıcı erişimi verilmelidir.

For more information about granting appropriate authorities for users with the `MQWebUser` role, see "MQ Console ya da REST APIolanağını kullanmak için gereken IBM MQ kaynaklarına erişim" sayfa 495.

3. İsteğe bağlı: Configure TLS for the IBM MQ Console and REST API. Daha fazla bilgi için bkz "Configuring TLS for the REST API and IBM MQ Console on z/OS" sayfa 497.

z/OS Mqweb sunucusu tarafından gerekli olan yetki, görev kullanıcı kimliğini başlattı

z/OSişletim sisteminde, mqweb sunucusu başlatılan görev kullanıcı kimliği için bazı yetkilerin PCF komutları yayınlanmasını ve sistem kaynaklarına erişmesini gerektirir.

mqweb sunucusu, görev kullanıcı kimliği gereksinmesini başlattı:

- z/OS UNIX System Services olanağını kullanabilecek bir z/OS UNIX kullanıcı kimliği (UID).
- IBM MQ kuruluşundaki `hlq.SCSQAUTH` ve `hlq.SCSQANL*` veri kümelerine erişim.
- z/OS UNIX System Services olanağında IBM MQ kuruluş dosyalarına okuma erişimi.
- **`crtmqweb`** komut dosyası tarafından oluşturulan Liberty kullanıcı dizinine okuma ve yazma erişimi.
- Kuyruk yöneticisine bağlanma yetkisi. Mqweb sunucusuna, MQCONN sınıfındaki `hlq.BATCH` tanıtımında *READ* (Okuma) erişimi başlatmış olarak görev kullanıcı kimliğini başlatmış olun.
- IBM MQ komutlarını verme ve belirli kuyruklara erişim yetkisi. Bu ayrıntılar, "IBM MQ Console -gerekli komut güvenliği profilleri" sayfa 218, "Sistem kuyruğu güvenliği" sayfa 196ve "Bağlam güvenliğine ilişkin profiller" sayfa 206içinde açıklanmıştır.
- MFTiçin REST API ' i kullanmak üzere SYSTEM.FTE konusuna abone olma yetkisi. Grant the mqweb server started task user ID *ALTER* access to the `hlq.SUBSCRIBE.SYSTEM.FTE` profile in the MXTOPIC class.
- Bir SAF kayıt dosyası yapılandırıyorsanız, çeşitli güvenlik profillerine erişin. Ek bilgi için "IBM MQ Console ve REST API için SAF kaydının yapılandırılması" sayfa 480 başlıklı konuya bakın.

Bağlantı kimlik doğrulaması

Kuyruk yöneticiniz, tüm toplu iş uygulamalarının geçerli bir kullanıcı kimliği ve parola sağlanmasını gerektirecek şekilde yapılandırıldıysa, CHKLOCL (REQUIREND) ayarlanarak, mqweb sunucusunu, MQCONN sınıfındaki `hlq.BATCH` tanıtımında *UPDATE* görev kullanıcı kimliği erişimi başlatmış olmanız gerekir.

Bu yetki, mqweb sunucusu için CHKLOCL (isteğe bağlı) kipinde bağlantı doğrulamasının çalışmasına neden olur.

Kuyruk yöneticisini tüm toplu iş uygulamalarının geçerli bir kullanıcı kimliği ve parola sağladığından emin olmak için yapılandırmadıysanız, mqweb sunucusu görevini *OKU* profiline başlatan kullanıcı kimliğini MQCONN sınıfındaki `hlq.BATCH` tanıtımında vermek yeterli olur.

CHCKLOCL hakkında daha fazla bilgi için bkz. "Yerel olarak bağlı uygulamalarda CHCKLOCL ' in kullanılması" sayfa 186.

MQ Console ya da REST APIolanağını kullanmak için gereken IBM MQ kaynaklarına erişim

MQ Consoleya da REST API' da gerçekleştirilen işlemler, `MQWebUser` rolündeki bir kullanıcı tarafından kullanıcının güvenlik bağlamı altında gerçekleşir.

Bu görev hakkında

See “IBM MQ Console ve REST APIüzerinde roller” sayfa 483 for more information on the roles in the MQ Console and REST API.

Bir kullanıcıya, `MQWebUser` rolünde, MQ Console ya da REST API' yi kullanmak için gereken kuyruk yöneticisi kaynaklarına erişim vermek için aşağıdaki yordamı kullanın.

Yordam

1. `mqweb server started task` kullanıcı kimliği diğer kullanıcı erişimini, `MQWebUser` rolündeki her bir kullanıcı kimliğine verin.

   Bunu, kullanıcıların MQ Console ya da REST APIaracılığıyla yöneteceği her kuyruk yöneticisininde yapın.

   `mqweb server started task` kullanıcı kimliği diğer kullanıcı erişimini, `MQWebUser` rolündeki bir kullanıcıya vermek için aşağıdaki örnek RACF komutlarını kullanabilirsiniz:

   ```
   RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
   PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
   SETROPTS RACLIST(MQADMIN) REFRESH
   ```

   Burada:

   `hlq`
   Tanıtım öneki, kuyruk yöneticisi adı ya da kuyruk paylaşım grubu adı olabilir.

   `userId`
   Kullanıcı `MQWebUser` rolünde mi?

   `mqwebUserId`
   `mqweb server started task` kullanıcı kimliği mi?

   Not: Karma büyük-büyük harf güvenliği kullanıyorsanız, MQADMIN sınıfı yerine MXADMIN sınıfını kullanın.
2. Grant each user in the `MQWebUser` role access to system queues that are necessary to use the MQ Console and REST API.

   Bunu yapmak için, hem SYSTEM.ADMIN.COMMAND.QUEUE hem de SYSTEM.REST.REPLY.QUEUEiçin, her kullanıcıya, karma durum güvenliğinin kullanımda olup olmadığına bağlı olarak, her kullanıcıya MQQUEUE ya da MXQUEUE sınıflarına erişim yetkisi verir.

   Bunu, kullanıcının administrative REST API ağ geçidiaracılığıyla yönetilen uzak kuyruk yöneticileri de dahil olmak üzere, REST APIaracılığıyla yöneteceği her kuyruk yöneticisine yapmanız gerekir.
3. `MQWebUser` rolündeki bir kullanıcının uzak kuyruk yöneticilerini yönetmesine izin vermek için, MQQUEUE ya da MXQUEUE sınıfındaki tanıtıma kullanıcı güncelleme erişimi verin ve uzak kuyruk yöneticisine komut göndermek için kullanılan iletim kuyruğunu korudur. Ağ geçidi kuyruk yöneticisine kullanıcı güncelleme erişimi vermeniz gerektiğini unutmayın.

   Uzak kuyruk yöneticisininde, aynı kullanıcı için, komut yanıt iletilerini ağ geçidi kuyruk yöneticisine geri göndermek için kullanılan iletim kuyruğuna konmak üzere erişim verin.
4. Grant the users in the `MQWebUser` role access to any other resources required to perform the operations supported by the MQ Console and REST API.

   Bu erişim için gereken erişim:

   - Perform operations in the REST API, is described in the *Güvenlik gereksinimleri* sections of the individual REST API kaynakları
   - MQ Console ile ilgili komut verme komutları “IBM MQ Console -gerekli komut güvenliği profilleri” sayfa 218içinde açıklanmıştır.

V 9.1.0 Configuring TLS for the REST API and IBM MQ Console on z/OS

z/OS' ta, mqweb sunucusunu, TLS ve istemci sertifikası kimlik doğrulamasıyla güvenli bağlantılar için sertifikaları saklamak üzere bir RACF anahtar halkası kullanacak şekilde yapılandırabilirsiniz.

Başlamadan önce

Bu yordamı tamamlamak için, `mqwebuser.xml` dosyasına yazma erişimi ve SAF anahtarı halkalarıyla çalışma yetkisi olan bir kullanıcı olmalısınız.

Bu görev hakkında

Varsayılan mqweb sunucusu yapılandırması, sunucu ve güvenilir sertifikalar için Java anahtar depolarını kullanır. z/OS' ta, mqweb sunucusunu Java anahtar deposu yerine RACF anahtar halkası kullanacak şekilde yapılandırabilirsiniz. Sunucu, kullanıcıların bir istemci sertifikası kullanarak kimlik doğrulaması gerçekleştirmesine izin verecek şekilde de yapılandırılabilir.

Libertyiçinde RACF anahtar halkaları kullanmaya ilişkin bilgi için bkz. Liberty: Anahtar depoları .

Bir RACF anahtar halkasını kullanacak şekilde mqweb sunucusunu yapılandırmak ve isteğe bağlı olarak istemci sertifikası kimlik doğrulamasını yapılandırmak için bu yordamı izleyin.

Yordam

1. Sunucu sertifikasını imzalamak için kullanılacak bir sertifika yetkilisi (CA) sertifikası oluşturun. Örneğin, aşağıdaki RACF komutunu girin:

```
RACDCERT GENCERT
  CERTAUTH
  SUBJECTSDN(CN('mqweb Certification Authority')
    O('IBM')
    OU('MQ'))
  SIZE(2048)
  WITHLABEL('mqwebCertauth')
```

2. Aşağıdaki komutu girerek, 1. adımda yaratılan CA sertifikasıyla imzalanmış bir sunucu sertifikası oluşturun:

```
RACDCERT ID(mqwebUserId) GENCERT
  SUBJECTSDN(CN('hostname')
   O('IBM')
   OU('MQ'))
   SIZE(2048)
   SIGNWITH (CERTAUTH LABEL('mqwebCertauth'))
  WITHLABEL('mqwebServerCert')
```

   Burada *mqwebUserId* , mqweb sunucusu tarafından başlatılan görev kullanıcı kimliği ve *anasistemadı* , mqweb sunucusunun anasistem adıdır.

3. CA sertifikasını ve sunucu sertifikasını, aşağıdaki komutları girerek SAF anahtar halkasına bağlayın:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebCertauth') CERTAUTH)
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebServerCert'))
```

   Burada *mqwebUserId* , mqweb sunucusu tarafından başlatılan görev kullanıcı kimliği ve *anahtarlık* , kullanmak istediğiniz anahtar halkasının adıdır.

4. Aşağıdaki komutu girerek CA sertifikasını bir CER dosyasına aktarın:

```
RACDCERT CERTAUTH EXPORT(LABEL('mqwebCertauth'))
        DSN('hlq.CERT.MQWEBCA')
        FORMAT(CERTDER)
        PASSWORD('password')
```

5. İkili olarak dışa aktarılan CA sertifikasını iş istasyonunuza FTP ' ye aktarın ve sertifika yetkilisi sertifikası olarak tarayıcınıza aktarın.
6. İsteğe bağlı: İstemci sertifikası kimlik doğrulamasını yapılandırmak istiyorsanız, bir istemci sertifikası yaratın ve dışa aktarın.
   a) İstemci sertifikasını imzalamak için kullanılacak bir sertifika yetkilisi (CA) sertifikası oluşturun. Örneğin, aşağıdaki RACF komutunu girin:

```
RACDCERT GENCERT
  CERTAUTH
  SUBJECTSDN(CN('mqweb User CA')
   O('IBM')
   OU('MQ'))
   SIZE(2048)
  WITHLABEL('mqwebUserCertauth')
```

   b) Aşağıdaki komutu girerek CA sertifikasını SAF anahtar halkasına bağlayın:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebUserCertauth') CERTAUTH)
```

   Burada *mqwebUserId* , mqweb sunucusu tarafından başlatılan görev kullanıcı kimliği ve *anahtarlık* , kullanmak istediğiniz anahtar halkasının adıdır.

   c) CA sertifikasıyla imzalanmış bir istemci sertifikası oluşturun. Örneğin, şu komutu girin.

```
RACDCERT ID(clientUserId) GENCERT
  SUBJECTSDN(CN('clientUserId')
     O('IBM')
     OU('MQ'))
   SIZE(2048)
   SIGNWITH (CERTAUTH LABEL('mqwebUserCertauth'))
  WITHLABEL('userCertLabel')
```

   Burada *clientUserId* kullanıcı adıdır.

   Bir sertifikayı bir birincil kullanıcı için eşlemek için kullanılan yöntem, yapılandırılan kullanıcı kayıt dosyası tipine bağlıdır:

   - Temel bir kayıt dosyası kullanıyorsanız, sertifikadaki Ortak Ad alanı, kayıt defterindeki kullanıcı ile eşleştirilir.
   - Bir SAF kayıt dosyası kullanıyorsanız ve sertifika RACF veritabanında varsa, sertifika yaratılırken **ID** değiştirgesiyle belirtilen sertifika sahibi kullanılır.
   - LDAP kayıt dosyası kullanıyorsanız, sertifikadaki tam ayırt edici ad, LDAP kayıt defterine göre eşleştirilir.

   d) Aşağıdaki komutu girerek istemci sertifikasını PKCS #12 dosyasına verin:

```
RACDCERT ID(mqwebUserId) EXPORT(LABEL('userCertLabel')) PASSWORD('password')
DSN('hlq.USER.CERT')
```

   e) Dışa aktarılan sertifikayı ikili olarak iş istasyonunuza FTP ' niz. İstemci sertifikasını IBM MQ Consoleile kullanmak için, bunu kişisel sertifika olarak IBM MQ Console ' a erişmek için kullanılan web tarayıcısına aktarın.
7. Edit the file *WLP_user_directory*/servers/mqweb/mqwebuser.xml, where *WLP_kullanıcı_dizini* is the directory that was specified when the **crtmqweb** script ran to create the mqweb server definition.

   Bir RACF anahtar halkası kullanacak şekilde mqweb sunucusunu yapılandırmak için aşağıdaki değişiklikleri yapın:

   a) Aşağıdaki satırı kaldırın ya da açıklama satırı yapın:

```
<sslDefault sslRef="mqDefaultSSLConfig"/>
```

b) Aşağıdaki deyimleri ekleyin:

```
<keyStore id="defaultKeyStore" filebased="false" location="safkeyring://mqwebUserId/
keyring"
          password="password" readOnly="true" type="JCERACFKS" />
<ssl id="thisSSLConfig" keyStoreRef="defaultKeyStore" sslProtocol="TLSv1.2"
          serverKeyAlias="mqwebServerCert" clientAuthenticationSupported="true" />
<sslDefault sslRef="thisSSLConfig"/>
```

Burada:

- *mqwebUsertnt* , mqweb sunucusu görev kullanıcı kimliğini başlattı.
- *anahtarlık* , RACF anahtar halkasının adıdır.
- *mqwebServerCert* , mqweb sunucusu sertifikasının etiketidir.

Notlar: `keyStore password` değeri yoksayılır.

8. mqweb sunucusunu durdurup yeniden başlatarak mqweb sunucusunu yeniden başlatın.
9. İsteğe bağlı: Kimlik doğrulamak için istemci sertifikasını kullan:
   - İstemci sertifikasını IBM MQ Consoleile kullanmak için, istemci sertifikasını kurduğunuz web tarayıcısındaki MQ Console URL adresini girin.
   - REST API 'si ile istemci sertifikasını kullanmak için, her bir REST isteğiyle istemci sertifikasını sağlayın.

   Notlar:

   a. Yalnızca IBM MQ Console' ta kimlik doğrulaması için sertifikalar kullanıyorsanız, tarayıcı içinden seçim yapmak için bir sertifika listesi görüntüleyebilir.

   b. Farklı bir sertifika kullanmak istiyorsanız, tarayıcınızı kapatıp yeniden başlatmanız gerekebilir.

   c. RACF veritabanında olmayan istemci sertifikalarını kullanıyorsanız, sertifika özniteliklerini bir kullanıcı kimliğiyle eşlemek için RACF sertifika adı süzme işlevini kullanabilirsiniz. Örneğin:

   ```
   RACDCERT ID(DEPT3USR) MAP SDNFILTER(OU=DEPT1.C=US)
   ```

   maps certificates with a subject distinguished name containing OU=DEPT1 and C=US to user ID DEPT3USR.

Sonuçlar

IBM MQ Console ve REST APIiçin TLS arabirimi ayarladınız.

ULW Managing keys and certificates on UNIX, Linux, and Windows

Anahtarları, sertifikaları ve sertifika isteklerini yönetmek için `runmqckm` komutunu (UNIX ve Windows) ve `runmqakm` komutunu (UNIX, Linux, and Windows) kullanın.

runmqckm komutu

`runmqckm` komutu UNIX ve Windowsüzerinde kullanılabilir.

`runmqckm` komutu, “güvenlikIBM MQ” sayfa 5içinde açıklanan iKeyman' a benzer işlevler sağlar.

To use the **`runmqckm`** command, ensure that the systems environment variables are correctly configured by running the **`setmqenv`** command.

V 9.1.0 **`runmqckm`** komutu, IBM MQ JRE bileşeninin kurulmasını gerektirir. Bu bileşen kurulmamışsa, **`runmqackm`** komutunu kullanabilirsiniz.

runmqakm komutu

`runmqakm` komutu, UNIX, Linuxve Windowsüzerinde kullanılabilir.

To use the **runmqaqm** command, ensure that the systems environment variables are correctly configured by running the **setmqenv** command.

TLS sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqckm** komutları yerine **runmqakm** komutunu kullanın. Bunun nedeni, **runmqakm** komutunun daha güçlü şifrelemeyi desteklemesinden kaynaklanır.

Aşağıdaki işlemi yapmak için `runmqckm` ve `runmqakm` komutlarını kullanın:

- IBM MQ ' in gerektirdiği CMS anahtar veritabanı dosyaları tipini yaratın
- Sertifika istekleri oluştur
- Kişisel sertifikaları içe aktar
- CA sertifikalarını içe aktar
- Kendinden onaylı sertifikaları yönet

İlgili bilgiler
Anahtar aracı

ULW UNIX, Linux, and Windows üzerinde runmqckm ve runmqakm komutları

Bu kısım, komutun nesnesine göre runmqckm ve runmqakm komutlarını açıklar.

İki komut arasındaki temel farklılıklar şunlardır:

- ULW **runmqakm**
  - UNIX, Linuxve Windowssistemlerinde kullanılabilir.
  - Sertifika ve sertifika isteklerinin Elliptic Curve ortak anahtarlarıyla oluşturulmasını desteklerken, **runmqckm** komutu oluşturulmaz.
  - Anahtar havuzu dosyasının, **-strong** parametresiyle **runmqckm** komutundan daha güçlü şifrelenmesini destekler.
  - FIPS 140-2 uyumlu olarak onaylanmıştır ve **runmqckm** komutunun aksine **-fips** parametresi kullanılarak FIPS uyumlu bir şekilde çalışacak şekilde yapılandırılabilir.
- Windows UNIX **runmqckm**
  - UNIX ve Windowsüzerinde kullanılabilir.
  - **runmqakm** komutu JKS ve JCEKS anahtar havuzu dosya biçimlerini desteklerken, JKS ve JCEKS anahtar havuzu dosya biçimlerini destekler.

Uyarı: V 9.1.0 **runmqckm** komutu, IBM MQ Java runtime environment (JRE) özelliğinin kurulmasını gerektirir.

Her komut en az bir *nesne*belirtir. PKCS #11 aygıt işlemlerine ilişkin komutlar ek nesneler belirtebilir. Anahtar veritabanı, sertifika ve sertifika isteği nesnelerine ilişkin komutlar bir *işlem*de belirtir. Nesne aşağıdakilerden biri olabilir:

-keydb
İşlemler bir anahtar veritabanı için geçerlidir

-cert
İşlemler bir sertifikaya uygulanır

-certreq.
İşlemler bir sertifika isteği için geçerlidir

-help
yardımı görüntüler

-version
Sürüm bilgilerini görüntüler

Aşağıdaki alt konularda, anahtar veritabanı, sertifika ve sertifika isteği nesneleri üzerinde gerçekleştirebileceğiniz işlemler açıklanır; bu komutlara ilişkin seçeneklerin açıklaması için bkz. “UNIX, Linux, and Windows üzerinde runmqckm ve runmqakm seçenekleri” sayfa 509 .

ULW Yalnızca UNIX, Linux, and Windows üzerinde CMS anahtar veritabanına ilişkin komutlar

CMS anahtar veritabanına ilişkin anahtarları ve sertifikaları yönetmek için **runmqckm**ve **runmqakm** komutlarını kullanabilirsiniz.

-keydb -changepw
CMS anahtar veritabanına ilişkin parolayı değiştirin:

```
-keydb -changepw -db filename -pw password -new_pw new_password


-stash
```

-keydb -create
CMS anahtar veritabanı yarat:

```
-keydb -create -db filename
-pw password -type cms -expire days -stash
```

-keydb -stashpw
CMS anahtar veritabanının parolasını bir dosyada saklamanızı sağlar:

```
-keydb -stashpw -db filename
-pw password
```

-cert -getdefault

Not: Varsayılan sertifika IBM MQ 8.0tarafından desteklenmez. “Dijital sertifika etiketleri, gereksinimleri anlama” sayfa 25içinde açıklandığı gibi sertifika etiketi yapılanışını kullanmalısınız.

Varsayılan kişisel sertifikayı al:

```
-cert -getdefault -db filename
-pw password
```

-cert-modify
Bir sertifikayı değiştirin.

Not: Şu anda değiştirilebilecek tek alan Sertifika Güven alanıdır.

```
-cert -modify -db filename
-pw password -label label
-trust enable|disable
```

-cert -setdefault

Not: Varsayılan sertifika IBM MQ 8.0 ya da üstü tarafından desteklenmez. “Dijital sertifika etiketleri, gereksinimleri anlama” sayfa 25içinde açıklandığı gibi sertifika etiketi yapılanışını kullanmalısınız.

Varsayılan kişisel sertifikayı ayarla:

```
-cert -setdefault -db filename
-pw password -label label
```

ULW UNIX, Linux, and Windows üzerinde CMS ya da PKCS #12 anahtar veritabanları için komut

Bir CMS anahtar veritabanına ya da PKCS #12 anahtar veritabanına ilişkin anahtarları ve sertifikaları yönetmek için runmqckm ve runmqakm komutlarını kullanabilirsiniz.

Not: IBM MQ , SHA-3 ya da SHA-5 algoritmalarını desteklemez. Her iki algoritma da SHA-2 ailesinin üyesi olduğundan, SHA384WithRSA ve SHA512WithRSA dijital imza algoritması adlarını kullanabilirsiniz.

Sayısal imza algoritması adları SHA3WithRSA ve SHA5WithRSA , sırasıyla SHA384WithRSA ve SHA512WithRSA kısaltması oldukları için kullanımdan kaldırılmıştır.

-keydb -changepw
Anahtar veritabanına ilişkin parolayı değiştirin:

```
-keydb -changepw -db filename -pw password -new_pw
new_password -expire days
```

-keydb -convert
anahtar veritabanını bir biçimden diğerine dönüştürün:

```
-keydb -convert -db filename -pw password
-old_format cms | pkcs12 -new_format cms
```

-keydb -create
Anahtar veritabanı yarat:

```
-keydb -create -db filename -pw password -type cms
| pkcs12
```

-keydb -delete
Anahtar veritabanını sil:

```
-keydb -delete -db filename -pw password
```

-keydb -list
Şu anda desteklenen anahtar veritabanı tiplerini listele:

```
-keydb -list
```

-cert -add
Anahtar veritabanına bir dosyadan sertifika ekleyin:

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

-cert -create
Kendinden onaylı sertifika yarat:

```
-cert -create -db filename -pw password -label label
-dn distinguished_name
-size 1024 | 512 -x509version 3 | 1
| 2
-expire days -sig_alg MD2_WITH_RSA | MD2WithRSA
|
MD5_WITH_RSA | MD5WithRSA
|
SHA1WithDSA | SHA1WithRSA
|
SHA256_WITH_RSA | SHA256WithRSA
|
```

```
SHA2WithRSA | SHA384_WITH_RSA
|
SHA384WithRSA | SHA512_WITH_RSA
|
SHA512WithRSA | SHA_WITH_DSA
|
SHA_WITH_RSA | SHAWithDSA
|
SHAWithRSA
```

-cert -delete
Bir sertifikayı sil:

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

-cert -details
Belirli bir sertifikaya ilişkin ayrıntılı bilgileri listeleyin:

```
-cert -details -db filename -pw password -label label
```

-cert -export
Kişisel sertifikayı ve ilişkili özel anahtarını bir anahtar veritabanından PKCS #12 dosyasına ya da başka bir anahtar veritabanına aktarın:

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

-cert -extract
Bir sertifikayı anahtar veritabanından çek:

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

-cert -import
Anahtar veritabanından kişisel sertifika al:

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

`-label` seçeneği gereklidir ve kaynak anahtar veritabanından içe aktarılacak sertifikanın etiketini belirtir.

`-new_label` seçeneği isteğe bağlıdır ve içe aktarılan sertifikaya, kaynak veritabanındaki etiketten hedef anahtar veritabanında farklı bir etiket verilmesini sağlar.

-cert -list
Bir anahtar veritabanındaki tüm sertifikaları listele:

```
-cert -list all | personal | CA
-db filename -pw password
```

-cert -receive
Dosyadan sertifika al:

```
-cert -receive -file filename -db filename -pw password
```

```
-format ascii | binary -default_cert yes |
no
```

-cert -sign

Bir sertifikayı imzala:

```
-cert -sign -db filename -file filename -pw password
-label label -target filename
-format ascii | binary -expire days
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA
|
MD5WithRSA | SHA1WithDSA | SHA1WithRSA
|
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

-certreq -create

Sertifika isteği yarat:

```
-certreq -create -db filename -pw password
-label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

-certreq -delete

Sertifika silme isteği:

```
-certreq -delete -db filename -pw password -label
label
```

-certreq -details

Belirli bir sertifika isteğine ilişkin ayrıntılı bilgileri listeleyin:

```
-certreq -details -db filename -pw password -label
label
```

Bir sertifika isteğiyle ilgili ayrıntılı bilgileri listeleyin ve tam sertifika isteğini gösterin:

```
-certreq -details -showOID -db filename
-pw password -label label
```

-certreq -extract

Sertifika isteği veritabanından bir sertifika isteğini bir dosyaya çek:

```
-certreq -extract -db filename -pw password
-label label -target filename
```

-certreq -list

Sertifika isteği veritabanındaki tüm sertifika isteklerini listele:

```
-certreq -list -db filename -pw password
```

-certreq -rekreate
Sertifika isteğini yeniden yarat:

```
-certreq -recreate -db filename -pw password
-label label -target filename
```

ULW UNIX, Linux, and Windows üzerinde şifreleme aygıtı işlemlerine ilişkin komutlar

Şifreleme aygıtı işlemlerine ilişkin anahtarları ve sertifikaları yönetmek için runmqckm ve runmqakm komutlarını kullanabilirsiniz.

Not: IBM MQ , SHA-3 ya da SHA-5 algoritmalarını desteklemez. Her iki algoritma da SHA-2 ailesinin üyesi olduğundan, SHA384WithRSA ve SHA512WithRSA dijital imza algoritması adlarını kullanabilirsiniz.

Sayısal imza algoritması adları SHA3WithRSA ve SHA5WithRSA , sırasıyla SHA384WithRSA ve SHA512WithRSA kısaltması oldukları için kullanımdan kaldırılmıştır.

-keydb -changepw
Şifreleme aygıtına ilişkin parolayı değiştirin:

```
-keydb -changepw -crypto module_name -tokenlabel token_label
-pw password -new_pw new_password
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-keydb -list
Şu anda desteklenen anahtar veritabanı tiplerini listele:

```
-keydb -list
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -add
Bir dosyadan şifreleme aygıtına sertifika ekleyin:

```
-cert -add -crypto module_name -tokenlabel token_label
-pw password -label label -file filename -format
ascii | binary
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -create
Şifreleme aygıtında kendinden onaylı bir sertifika yaratın:

```
-cert -create -crypto module_name -tokenlabel token_label

-pw password -label label -dn distinguished_name
```

```
-size 1024 | 512
-x509version 3 | 1 | 2 -default_cert no
| yes -expire days
-sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Not: Ayırt edici adda birden çok Kuruluş Birimi (kuruluş birimi) özniteliği içeren bir sertifikayı içe aktaramazsınız.

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -delete

Şifreleme aygıtındaki bir sertifikayı sil:

```
-cert -delete -crypto module_name -tokenlabel token_label
-pw password -label label
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -details

Şifreleme aygıtındaki belirli bir sertifikaya ilişkin ayrıntılı bilgileri listeleyin:

```
-cert -details -crypto module_name -tokenlabel token_label

-pw password -label label
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

Ayrıntılı bilgileri listeleyin ve bir şifreleme aygıtında belirli bir sertifikaya ilişkin tam sertifikayı gösterin:

```
-cert -details -showOID -crypto module_name -tokenlabel
token_label
-pw password -label label
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -extract

Bir sertifikayı anahtar veritabanından çek:

```
-cert -extract -crypto module_name -tokenlabel token_label
```

```
-pw password -label label -target filename
-format ascii | binary
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -import

İkincil anahtar veritabanı desteği olan bir şifreleme aygıtına sertifika alın:

```
-cert -import -db filename -pw password -label label
-type cms
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

```
-cert -import -db filename -pw password -label label
-type cms
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

Bir PKCS #12 sertifikasını ikincil anahtar veritabanı desteği olan bir şifreleme aygıtına aktar:

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

Not: Ayırt edici adda birden çok Kuruluş Birimi (kuruluş birimi) özniteliği içeren bir sertifikayı içe aktaramazsınız.

-cert -list

Bir şifreleme aygıtındaki tüm sertifikaları listele:

```
-cert -list all | personal | CA
-crypto module_name -tokenlabel token_label -pw
password
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS

#11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-cert -receive
İkincil anahtar veritabanı desteği ile bir dosyadan şifreleme aygıtına sertifika alın:

```
-cert -receive -file filename -crypto module_name -tokenlabel
token_label
-pw password -default_cert yes | no
-secondaryDB filename -secondaryDBpw password -format
ascii | binary
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

runmqakm komutunu kullanarak:

-certreq -create
Şifreleme aygıtında sertifika isteği yarat:

```
-certreq -create -crypto module_name -tokenlabel token_label

-pw password -label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA
|
MD5WithRSA | SHA1WithDSA | SHA1WithRSA
|
SHA256_WITH_RSA | SHA256WithRSA
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

Not: Ayırt edici adda birden çok Kuruluş Birimi (kuruluş birimi) özniteliği içeren bir sertifikayı içe aktaramazsınız.

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-certreq -delete
Şifreleme aygıtından sertifika silme isteği:

```
-certreq -delete -crypto module_name -tokenlabel token_label

-pw password -label label
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-certreq -details
Şifreleme aygıtındaki belirli bir sertifika isteğine ilişkin ayrıntılı bilgileri listeleyin:

```
-certreq -details -crypto module_name -tokenlabel token_label
```

```
-pw password -label label
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

Bir sertifika isteğiyle ilgili ayrıntılı bilgileri listeleyin ve şifreleme aygıtında tam sertifika isteğini gösterin:

```
-certreq -details -showOID -crypto module_name -tokenlabel
token_label
-pw password -label label
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-certreq -extract

Şifreleme aygıtındaki bir sertifika isteği veritabanından bir dosyaya sertifika isteği çıkarın:

```
-certreq -extract -crypto module_name -tokenlabel token_label

-pw password -label label -target filename
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

-certreq -list

Şifreleme aygıtındaki sertifika isteği veritabanındaki tüm sertifika isteklerini listele:

```
-certreq -list -crypto module_name -tokenlabel token_label

-pw password
```

PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' in 64 bitlik programlar olduğunu unutmayın. PKCS #11 desteği için gerekli dış modüller 64 bitlik bir işleme yüklenecek, bu nedenle şifreleme donanımının yönetimi için 64 bitlik bir PKCS #11 kitaplığınızın kurulu olması gerekir. Bu platformlarda **strmqikm** ve **runmqckm** programları 32 bit olduğu için, Windows ve Linux x86 32 bit platformları tek istisnadır.

ULW UNIX, Linux, and Windows üzerinde runmqckm ve runmqakm seçenekleri

Anahtarları, sertifikaları ve sertifika isteklerini yönetmek için **runmqckm** (iKeycmd) ve **runmqakm** komut satırı seçeneklerini kullanabilirsiniz.

ULW `runmqakm` komutu UNIX, Linux, and Windowsüzerinde kullanılabilir.

Windows UNIX `runmqckm` komutu, UNIX ve Windowssistemlerinde kullanılabilir.

Not: IBM MQ , SHA-3 ya da SHA-5 algoritmalarını desteklemez. Her iki algoritma da SHA-2 ailesinin üyesi olduğundan, SHA384WithRSA ve SHA512WithRSA dijital imza algoritması adlarını kullanabilirsiniz.

Sayısal imza algoritması adları SHA3WithRSA ve SHA5WithRSA , sırasıyla SHA384WithRSA ve SHA512WithRSA kısaltması oldukları için kullanımdan kaldırılmıştır.

Bir seçeneğin anlamı, komutta belirtilen nesneye ve işleme bağlı olabilir.

*Çizelge 90. **runmqckm** ve **runmqakm** ile kullanılabilen seçenekler*

Değiştirge	**Açıklama**
`-create`	Anahtar veritabanı yaratma seçeneği.
`-crypto`	PKCS #11 şifreleme aygıtını yönetmek için kullanılan modülün adı. Özellikler dosyasında modül adını belirtirseniz, **-crypto** ' den sonraki değer isteğe bağlıdır. PKCS #11 şifreleme donanımında saklanan sertifikaları ya da anahtarları kullanıyorsanız, **runmqckm** ve **strmqikm** ' nin IBM MQ kuruluşuyla birlikte sağlanan Java sanal makinesi (JVM) kullanılarak çalıştırıldığına dikkat edin. PKCS #11 desteği için gereken dış modüller JVM işlemine yüklenecek; bu nedenle, JVM ' nin bit değeriyle eşleşen şifreleme donanımının yönetimi için bir PKCS #11 kitaplığınız kurulu olmalıdır ve bu kitaplığı **runmqckm** ya da **strmqikm**olarak belirtmeniz gerekir.
-db	Anahtar veritabanının tam olarak nitelenmiş yol adı.
-default_cert	Bir sertifikayı varsayılan sertifika olarak ayarlar. Değer `evet` ya da `hayır`olabilir. Varsayılan değer no' dur.
-dn	X.500 ayırt edici adı. Değer, çift tırnak içine alınmış bir dizedir; örneğin, `"CN=John Smith,O=IBM,OU=Test,C=GB"`. Yalnızca O ve C özniteliklerinin gerekli olduğunu unutmayın. Ortak bir ad (CN) belirtilmesi isteğe bağlıdır.
-encryption	Sertifika dışa aktarma komutunda kullanılan şifreleme gücü. Değer `güçlü` ya da `zayıf`olabilir. Varsayılan değer `strong`(güçlü) değeridir.
-expire	Bir sertifikanın ya da veritabanı parolasının son kullanma tarihi (gün). Varsayılan değer, bir sertifika parolası için 365 gündür. Veritabanı parolası için varsayılan zaman yoktur: Veritabanı parolası süre sonunu belirtik olarak ayarlamak için **-expire** değiştirgesini kullanın.
-file	Sertifika ya da sertifika isteğinin dosya adı.
-fips	komutun FIPS kipinde çalıştırılacağını belirtir. FIPS kipindeyken, ICC bileşeni FIPS 140-2 doğrulanmış algoritmaları kullanır. ICC bileşeni FIPS kipinde başlatılmazsa, **runmqakm** komutu başarısız olur.
-format	Sertifikanın biçimi. Değer, Base64_encoded ASCII için `ascii` ya da İkili DER verileri için `binary` olabilir. Varsayılan değer `ascii`' dir.
-label	Bir sertifika ya da sertifika isteğine eklenen etiket. Sertifika, bir IBM MQ istemci uygulamasını ya da kuyruk yöneticisini tanımlamak için kullanılan kişisel bir sertifikaysa, etiketin IBM MQ sertifika etiketi (CERTLABL) ayarına karşılık gelmesi gerekir; ek bilgi için bkz. “Dijital sertifika etiketleri, gereksinimleri anlama” sayfa 25.
-new_format	Anahtar veritabanının yeni biçimi.
-new_label	Bir sertifika içe aktarma komutunda kullanılan bu seçenek, bir sertifikanın kaynak anahtar veritabanında sahip olduğu etiketten farklı bir etiketle içe aktarılmasına olanak sağlar. Sertifika, bir IBM MQ istemci uygulamasını ya da kuyruk yöneticisini tanımlamak için kullanılan kişisel bir sertifikaysa, etiketin IBM MQ sertifika etiketi (CERTLABL) ayarına karşılık gelmesi gerekir; ek bilgi için bkz. “Dijital sertifika etiketleri, gereksinimleri anlama” sayfa 25.

*Çizelge 90. **runmqckm** ve **runmqakm** ile kullanılabilen seçenekler (devamı var)*	
Değiştirge	**Açıklama**
-new_pw	Yeni veritabanı parolası.
-old_format	Anahtar veritabanının eski biçimi.
-pw	Anahtar veritabanı ya da PKCS #12 dosyasının parolası.
-secondaryDB	PKCS #11 aygıt işlemleri için ikincil anahtar veritabanının adı.
-secondaryDBpw	PKCS #11 aygıt işlemlerine ilişkin ikincil anahtar veritabanının parolası.
-showOID	Tam sertifika ya da sertifika isteğini görüntüler.
-sig_alg	Bir sertifika isteği, kendinden onaylı bir sertifika ya da bir sertifikanın imzalanması sırasında kullanılan hash algoritması. Bu hash algoritması, yeni yaratılan sertifika ya da sertifika isteğiyle ilişkili imzayı yaratmak için kullanılır. **runmqckm**için değer 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. Varsayılan değer SHA1WithRSAdeğeridir. **runmqakm**için değer 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_SHA384ya da EC_ecdsa_with_SHA512. Varsayılan değer SHA1WithRSAdeğeridir.
-size	Anahtar boyutu. **runmqckm**için değer 512, 1024 ya da 2048 olabilir. Varsayılan değer 1024 bittir. **runmqakm**için değer, imza algoritmasına bağlıdır: • RSA imza algoritmaları için (**-sig_alg** belirtilmezse kullanılan varsayılan algoritma), değer 512, 1024, 2048 ya da 4096 olabilir. **-fips** parametresi etkinleştirildiyse 512 bitlik RSA anahtarı boyutuna izin verilmez. Varsayılan RSA anahtarı boyutu 1024 bittir. • Eliptik Eğri algoritmaları için değer 256, 384 ya da 512 olabilir. Varsayılan Eliptik Eğri anahtar boyutu imza algoritmasına bağlıdır. SHA256için 256; SHA384için 384; SHA512için 512 'dir.
-stash	Anahtar veritabanı parolasını bir dosyada saklamanızı sağlar. Yalnızca CMS ve PKCS12tipindeki veritabanları için geçerlidir. **Not: -stash** , **-keydb** -create komutlarında **runmqckm**/**runmqakm** ' e parolayı içeren bir parola saklama dosyası oluşturmasını söylemek için geçerlidir. $ runmqakm -help komutu verilirken, yalnızca üst düzey yardım parametreleri listelenir.

*Çizelge 90. **runmqckm** ve **runmqakm** ile kullanılabilen seçenekler (devamı var)*	
Değiştirge	**Açıklama**
-stashed	Anahtar veritabanına ilişkin parolayı ya da PKCS #12 dosyasının bir parola saklama dosyasında olduğunu gösterir. **Not: -stashed** seçeneği, **-keydb** -create komutları dışındaki çağrılarda geçerlidir. Bu seçeneği belirlemezseniz, **-pw**komutunu kullanarak parolayı girmeniz gerekir. Ayrıca, yalnızca komuta ne tür bir işlem gerçekleştirmekte olduğunuzu bildirdiğinizde, **-stashed** ' u gösteren ayrıntılı yardım görüntülenir.
-target	Hedef dosya ya da veritabanı.
-target_pw	**-target** bir anahtar veritabanı belirtiyorsa, anahtar veritabanının parolası.
-target_type	**-target** işleneni tarafından belirtilen veritabanı tipi. İzin verilen değerler için bkz. **-type** parametresi.
-tokenLabel	PKCS #11 şifreleme aygıtının etiketi.
-trust	Bir CA sertifikasının güven durumu. Değer `enable` ya da `disable`olabilir. Varsayılan değer `enable`' dır.
-type	Veritabanı tipi. Değer, aşağıdaki değerlerden herhangi biri olabilir: • CMS anahtar veritabanı için `cms` • Bir PKCS #12 dosyası için `pkcs12` .
-x509version	Yaratılacak X.509 sertifikasının sürümü. Değer 1, 2 ya da 3 olabilir. Varsayılan 3'tür.

-rfc3339	Bu parametreyi, aşağıdaki biçimde olan `runmqakm -cert -details` komutu için RFC 3339 biçiminde tarih çıkışı yapmak için kullanın:
	`Not Before : 2015-08-26T08:53:37Z`
	`Not After : 2016-08-26T08:53:37Z`
	-rfc3339 değiştirgesinin ek değiştirgelerden sonra komutta görünmesi gerektiğini unutmayın:
	`runmqakm -cert -details -db exampleDB -stashed -label certficateLabel -rfc3339`

Not: `runmqckm` yardımcı programında simetrik anahtar şifrelemesi **-seckey** parametresiyle ilgili IBM Global Security Kit (GSKit) ile sağlanan özellikler yoksayılır ve IBM MQtarafından desteklenmez.

ULW UNIX, Linux, and Windows üzerinde runmqakm hata kodları

runmqakm tarafından verilen sayısal hata kodlarının ve bunların ne anlama geliyor olduğunu içeren bir çizelge.

Hata kodu	Hata İletisi
0	Başarılı
1	Bilinmeyen hata oluştu
2	Bir ASN.1 kodlama/kod çözme hatası oluştu.

Hata kodu	Hata İletisi
3	ASN.1 kodlayıcısı/kod çözücü kullanıma hazırlanırken bir hata oluştu.
4	Aralık dışı bir dizin ya da var olmayan bir isteğe bağlı alan nedeniyle ASN.1 kodlama/kod çözme hatası oluştu.
5	Bir veritabanı hatası oluştu.
6	Veritabanı dosyası açılırken bir hata oluştu, dosyanın varolup olmadığını ve izni denetleyin.
7	Veritabanı dosyası yeniden açılırken hata oluştu.
8	Veritabanı oluşturma başarısız oldu.
9	Veritabanı zaten var.
10	Veritabanı dosyası silinirken bir hata oluştu.
11	Veritabanı açılamadı.
12	Veritabanı dosyası okunurken bir hata oluştu.
13	Veri taban kt § ne veri yazlrken hata ortaya ‡kt.
14	Veritabanı geçerlilik denetimi hatası oluştu.
15.000	Geçersiz bir veritabanı sürümüyle karşılaşıldı.
16	Geçersiz bir veritabanı parolasıyla karşılaşıldı.
17	Geçersiz bir veritabanı dosyası tipiyle karşılaşıldı.
18	Belirtilen veritabanı bozulmuş.
19	Geçersiz bir parola sağlandı ya da anahtar veritabanı kurcalanmış ya da bozulmuş.
20	Veritabanı anahtarı giriş bütünlüğü hatası oluştu.
21	Veritabanında yinelenen bir sertifika var.
22	Veritabanında yinelenen bir anahtar var (Kayıt Tanıtıcısı).
23	Anahtar veritabanında aynı etikete sahip bir sertifika zaten var.
24	Veritabanında yinelenen bir anahtar var (İmza).
25	Veritabanında yinelenen bir anahtar var (İmzalanmamış Sertifika).
26	Veritabanında yinelenen bir anahtar zaten var (Veren ve Seri Numarası).
27	Veritabanında yinelenen bir anahtar zaten var (Subject Public Key Info).
28	Veritabanında yinelenen bir anahtar zaten var (İmzalanmamış CRL).
29	Etiket veritabanında kullanıldı.
30	Parola şifreleme hatası oluştu.

Hata kodu	Hata İletisi
31	LDAP ile ilgili bir hata oluştu. (LDAP bu program tarafından desteklenmiyor)
24	Şifreleme hatası oluştu.
33	Şifreleme/şifre çözme hatası oluştu.
34	Geçersiz bir şifreleme algoritması bulundu.
%35	Veriler imzalanırken bir hata oluştu.
36	Veriler doğrulanırken hata oluştu.
37	Verilerin özeti hesaplanırken bir hata oluştu.
38	Geçersiz bir şifreleme parametresi bulundu.
39	Desteklenmeyen bir şifreleme algoritmasıyla karşılaşıldı.
40	Belirtilen giriş büyüklüğü, desteklenen modülo büyüklüğünden fazla.
41	Desteklenmeyen bir modül boyutu bulundu.
42	Veritabanı geçerlilik denetimi hatası oluştu.
43	Anahtar girişi geçerlilik denetimi başarısızlıkla sonuçlandı.
44	Yinelenen bir uzantı alanı var.
45	Anahtarın sürümü yanlış.
46	Gerekli bir uzantı alanı yok.
47	Geçerlilik süresi bugünü içermiyor ya da sertifika verenin geçerlilik süresi içinde yer almıyor
48	Geçerlilik süresi bugünü içermiyor ya da sertifika verenin geçerlilik süresi içinde yer almıyor.
49	Özel anahtar kullanım uzantısının geçerliliği denetlenirken bir hata oluştu.
50	Anahtarı veren bulunamadı.
51	Gerekli bir sertifika uzantısı eksik.
52	Geçersiz bir temel kısıt uzantısı bulundu.
53	Anahtar imzası geçerlilik denetimi başarısız oldu.
54	Anahtarın kök anahtarı güvenilir değil.
55	Anahtar iptal edildi.
56	Yetki anahtarı tanıtıcısı uzantısının geçerliliği denetlenirken hata oluştu.
57	Özel anahtar kullanım uzantısının geçerliliği denetlenirken bir hata oluştu.
58	Konu alternatif ad uzantısının geçerliliği denetlenirken bir hata oluştu.

Hata kodu	Hata İletisi
59	Sertifika veren diğer ad uzantısının geçerliliği denetlenirken bir hata oluştu.
60	Anahtar kullanım uzantısının geçerliliği denetlenirken bir hata oluştu.
61	Bilinmeyen bir kritik uzantı bulundu.
62	Anahtar çifti girişleri doğrulanırken bir hata oluştu.
63	CRL doğrulanırken bir hata oluştu.
64	Muteks hatası oluştu.
65	Geçersiz bir parametre bulundu.
86	Boş değerli bir parametre ya da bellek ayırma hatasıyla karşılaşıldı.
%67	Sayı ya da boyut çok büyük ya da çok küçük.
75	Eski parola geçersiz.
75	Yeni parola geçersiz.
70	Parolanın süresi doldu.
77	İş parçacığıyla ilgili bir hata oluştu.
68	İş parçacıkları yaratılırken hata oluştu.
73	Bir iş parçacığı çıkmayı beklerken hata oluştu.
74	Bir G/Ç hatası oluştu.
75	CMS yüklenirken bir hata oluştu.
76	Şifreleme donanımıyla ilgili bir hata oluştu.
77	Kitaplık kullanıma hazırlama yordamı başarıyla çağrılamadı.
65	İç veritabanı tanıtıcı çizelgesi bozuk.
65	Bellek ayırma hatası oluştu.
80	Tanınmayan bir seçenek bulundu.
81	Saat bilgileri alınırken hata oluştu.
82	Muteks oluşturma hatası oluştu.
76	İleti kataloğu açılırken hata oluştu.
84	Hata iletisi kataloğu açılırken hata oluştu
85	Boş değerli bir dosya adı bulundu.
69	Dosyalar açılırken bir hata oluştu, dosyanın varlığını ve izinlerini denetleyin.
87	Okunacak dosyalar açılırken bir hata oluştu.
88	Yazmak için dosyalar açılırken bir hata oluştu.
89	Böyle bir dosya yok.
90	İzin ayarı nedeniyle dosya açılamıyor.

Hata kodu	Hata İletisi
91	Dosyalara veri yazılırken hata oluştu.
92	Dosyalar silinirken bir hata oluştu.
93	Geçersiz Base64-encoded veri bulundu.
94	Geçersiz bir Base64 ileti tipi bulundu.
95	Veriler Base64 kodlama kuralıyla kodlanırken bir hata oluştu.
96	Base64-encoded verilerin kodu çözülürken bir hata oluştu.
97	Ayırt edici ad etiketi alınırken hata oluştu.
98	Gerekli ortak ad alanı boş.
99	Gerekli ülke ya da bölge adı alanı boş.
100	Geçersiz bir veritabanı tanıtıcısı bulundu.
101	Anahtar veritabanı yok.
102	İstek anahtarı çifti veritabanı yok.
103	Parola dosyası yok.
104	Yeni parola eskisiyle aynı.
105	Anahtar veritabanında anahtar bulunamadı.
106	İstek anahtarı bulunamadı.
107	Güvenilir bir CA bulunamadı.
108	Sertifika için istek anahtarı bulunamadı.
109	Anahtar veritabanında özel anahtar yok.
110	Anahtar veritabanında varsayılan anahtar yok.
111	Anahtar kaydında özel anahtar yok.
112	Anahtar kaydında sertifika yok.
113	CRL girişi yok.
114	Geçersiz bir anahtar veritabanı dosyası adı bulundu.
115	Tanınmayan bir özel anahtar tipi bulundu.
116	Geçersiz bir ayırt edici ad girişi bulundu.
117	Belirtilen anahtar etiketine sahip bir anahtar girişi bulunamadı.
118	Anahtar etiketi listesi bozulmuş.
119	Giriş verileri geçerli PKCS12 verileri değil.
120	Parola geçersiz ya da PKCS12 verileri bozulmuş ya da daha sonraki bir PKCS12 sürümüyle yaratılmış
121	Tanınmayan bir anahtar dışa aktarma tipi bulundu.

Hata kodu	Hata İletisi
122	Desteklenmeyen bir parola tabanlı şifreleme algoritması bulundu.
123	Anahtarlık dosyası CMS anahtar veritabanına dönüştürülürken bir hata oluştu.
124	CMS anahtar veritabanı bir anahtarlık dosyasına dönüştürülürken hata oluştu.
125	Sertifika isteği için sertifika yaratılırken hata oluştu.
126	Tam bir sertifika veren zinciri oluşturulamıyor.
127	Geçersiz WEBDB verileri bulundu.
128	Anahtarlık dosyasına yazılacak veri yok.
129	Girdiğiniz gün sayısı, izin verilen geçerlilik süresini aşıyor.
130	Parola çok kısa; en az {0} karakterden oluşmalıdır.
131	Bir parola en az bir sayısal sayı içermelidir.
132	Paroladaki tüm karakterler alfabetik ya da sayısal karakterlerdir.
133	Tanınmayan ya da desteklenmeyen bir imza algoritması belirtildi.
134	Geçersiz bir veritabanı tipiyle karşılaşıldı.
135	Belirtilen ikincil anahtar veritabanı başka bir PKCS#11 aygıtı tarafından kullanılıyor.
136	İkincil anahtar veritabanı belirtilmedi.
137	Etiket PKCS#11 aygıtında yok.
138	PKCS#11 aygıtına erişmek için parola gerekli.
139	PKCS#11 aygıtına erişmek için parola gerekli değil.
140	Şifreleme kitaplığı yüklenemiyor.
141	PKCS#11 bu işlem için desteklenmiyor.
142	PKCS#11 aygıtındaki bir işlem başarısız oldu.
143	LDAP kullanıcısı geçerli bir kullanıcı değil. (LDAP bu program tarafından desteklenmiyor)
144	LDAP kullanıcısı geçerli bir kullanıcı değil. (LDAP bu program tarafından desteklenmiyor)
145	LDAP sorgusu başarısız oldu. (LDAP bu program tarafından desteklenmiyor)
146	Geçersiz bir sertifika zinciri bulundu.
147	Kök sertifika güvenilir değil.
148	İptal edilen bir sertifikayla karşılaşıldı.
149	Bir şifreleme nesnesi işlevi başarısız oldu.
150	Kullanılabilir sertifika iptal listesi veri kaynağı yok.

Hata kodu	Hata İletisi
151	Kullanılabilir şifreleme aygıtı yok.
152	FIPS kipi kullanılamıyor.
153	FIPS kipi ayarlarıyla bir çakışma var.
154	Girilen parola, gerekli güvenlik düzeyi alt sınırını karşılamıyor.
200	Program başlatılırken bir hata oluştu.
201	Runmqakm Programına geçirilen bağımsız değişkenlerin bölümlenmesi başarısız oldu.
202	Komutta belirtilen nesne tanınan bir nesne değil.
203	Geçirilen işlem bilinen bir -keydb işlemi değil.
204	Geçirilen işlem bilinen bir -cert işlemi değil.
205	Geçirilen işlem, bilinen bir -certreq işlemi değil.
206	İstenen komut için bir etiket eksik.
207	-version etiketiyle geçirilen değer tanınan bir değer değil.
208	-size etiketiyle geçirilen değer tanınan bir değer değil.
209	-dn etiketiyle geçirilen değer doğru biçimde değil.
210	-format etiketiyle geçirilen değer tanınan bir değer değil.
211	Dosya açılırken bir hata oluştu.
212	PKCS12 bu aşamada desteklenmiyor.
213	Parolasını değiştirmeye çalıştığınız şifreleme simgesi parola korumalı değil.
214	PKCS12 bu aşamada desteklenmiyor.
215	Girilen parola, gerekli güvenlik düzeyi alt sınırını karşılamıyor.
216	FIPS kipi kullanılamıyor.
217	Süre bitim tarihi olarak girdiğiniz gün sayısı, izin verilen aralığın dışında.
218	Parola güvenlik düzeyi, minimum gereksinimleri karşılayamadı.
219	İstenen anahtar veritabanında Varsayılan sertifika bulunamadı.
220	Geçersiz bir güven durumuyla karşılaşıldı.
221	Desteklenmeyen bir imza algoritmasıyla karşılaşıldı. Bu aşamada yalnızca MD5 ve SHA1 desteklenir.
222	PCKS11 belirli bir işlem için desteklenmiyor.
223	Geçirilen işlem bilinen bir rasgele işlem değil.

Hata kodu	Hata İletisi
224	Sıfırdan küçük bir uzunluğa izin verilmez.
225	-strong etiketi kullanırken, parola uzunluğu alt sınırı 14 karakterdir.
226	-strong etiketi kullanırken, parola uzunluğu üst sınırı 300 karakterdir.
227	MD5 algoritması FIPS kipindeyken desteklenmez.
228	-cert -list komutu için site etiketi desteklenmiyor. Bu öznitelik, geriye dönük uyumluluk ve gelecekteki olası geliştirme için eklenir.
229	-ca etiketiyle ilişkili değer tanınmıyor. Değer 'true' ya da 'false ' olmalıdır.
230	-type etiketiyle geçirilen değer geçerli değil.
231	-expire etiketiyle geçirilen değer, izin verilen aralığın altında.
232	Kullanılan ya da istenen şifreleme algoritması desteklenmiyor.
233	Hedef zaten var.

Veritabanı kimlik doğrulaması ayrıntılarının korunması

Veritabanı yöneticisine bağlanmak için kullanıcı adı ve parola kimlik doğrulamasını kullanıyorsanız, parolayı `qm.ini` dosyasında düz metin olarak saklamaktan kaçınmak için bunları MQ XA kimlik bilgileri deposunda saklayabilirsiniz.

Kaynak yöneticisi için XAOpenString güncelleme

Kimlik bilgileri deposunu kullanmak için, `qm.ini` dosyasında XAOpenString dosyasını değiştirmelisiniz. Dizgi, veritabanı yöneticisine bağlanmak için kullanılır. You specify replaceable fields to identify where the user name and password are substituted within the XAOpenString string.

- +USER+ alanı, XACredentials mağazasında saklanan kullanıcı adı değeriyle değiştirilir.
- +PASSWORD+ alanı, XACredentials mağazasında saklanan parola değeriyle değiştirilir.

Aşağıdaki örneklerde, veritabanına bağlanmak için kimlik bilgileri dosyasını kullanmak üzere bir XAOpenString ' in nasıl değiştirileceği gösterilmektedir.

Db2 veritabanıyla bağlantı kurulması

```
XAResourceManager:
  Name=mydb2
  SwitchFile=db2swit
  XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t
  ThreadOfControl=THREAD
```

Oracle veritabanına bağlanma

```
XAResourceManager:
  Name=myoracle
  SwitchFile=oraswit
  XAOpenString=Oracle_XA+Acc=P/+USER+/+PASSWORD++SesTm=35
            +LogDir=/tmp+threads=true
  ThreadOfControl=THREAD
```

Veritabanına ilişkin kimlik bilgileriyle MQ XA kimlik bilgileri deposuna çalışma

`qm.ini` dosyasını, değiştirilebilir kimlik bilgileri dizgileriyle güncelledikten sonra, **setmqxacred** komutunu kullanarak MQ kimlik bilgileri deposuna kullanıcı adı ve parolayı eklemeniz gerekir. Ayrıca, var olan kimlik bilgilerini değiştirmek, kimlik bilgilerini silmek ya da kimlik bilgilerini listelemek için **setmqxacred** ' u da kullanabilirsiniz. Aşağıdaki örneklerde bazı tipik kullanım senaryoları verilebilir:

Kimlik bilgileri ekleme

Aşağıdaki komut, `mqdb2`adlı kaynak için `QM1` kuyruk yöneticisine ilişkin kullanıcı adını ve parolayı güvenli bir şekilde kaydeder.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

Kimlik bilgileri güncelleniyor

Bir veritabanına bağlanmak için kullanılan kullanıcı adını ve parolayı güncelleştirmek için, yeni kullanıcı adı ve parolayla **setmqxacred** komutunu yeniden verin:

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

Değişikliklerin yürürlüğe girmesi için kuyruk yöneticisini yeniden başlatmalısınız.

Kimlik bilgileri siliniyor

Aşağıdaki komut, kimlik bilgilerini siler:

```
setmqxacred -m QM1 -x mydb2 -d
```

Kimlik bilgileri listesi

Aşağıdaki komut kimlik bilgilerini listeler:

```
setmqxacred -m QM1 -l
```

İlgili başvurular

setmqxacred

güvenlikManaged File Transfer

Doğrudan kurulumdan sonra ve herhangi bir değişiklik yapılmadan Managed File Transfer , korumalı bir ortamda test veya değerlendirme amacıyla uygun olabilecek bir güvenlik düzeyine sahiptir. Ancak, bir üretim ortamında, dosya aktarma işlemlerini kimin başlatabileceğini, kimlerin aktarıldığını okuyup yazabileceğini ve dosyaların bütünlüğünün nasıl korunabileceğini doğru bir şekilde denetlemeniz gerekir.

İlgili görevler

Restricting group authorities for MFT-specific resources

MFT' a özgü kaynaklara ilişkin yetkilerin yönetilmesi

“Advanced Message Security ile Managed File Transferkomutunu kullanma” sayfa 581

Bu senaryoda, bir Managed File Transferaracılığıyla gönderilen veriler için ileti gizliliği sağlamak üzere Advanced Message Security ' un nasıl yapılandırılacağı açıklanmaktadır.

İlgili başvurular

MFT ' nin dosya sistemlerine erişmesi için yetkililer

commandPath MFT özelliği

MFT Agent günlük ve durum iletilerini yayınlama yetkisi

MFT ve IBM MQ bağlantı doğrulaması

Bağlantı kimlik doğrulaması, bir kuyruk yöneticisinin, sağlanan bir kullanıcı kimliği ve parola kullanarak uygulamaların kimliğini doğrulayabilmesi için yapılandırılmasına olanak sağlar. İlişkili kuyruk yöneticisinde

güvenlik etkinleştirildiyse ve kimlik bilgileri ayrıntıları (kullanıcı kimliği ve parola) gerektiriyorsa, kuyruk yöneticisiyle başarılı bir bağlantı kurulabilmesi için bağlantı kimlik doğrulama özelliğinin etkinleştirilmesi gerekir. Bağlantı kimlik doğrulaması uyumluluk kipinde ya da MQCSP kimlik doğrulama kipinde çalıştırılabilir.

Kimlik bilgisi ayrıntılarını sağlayan yöntemler

Birçok Managed File Transfer komutu, kimlik bilgileri ayrıntılarının sağlandığı aşağıdaki yöntemleri destekler:

Komut satırı bağımsız değişkenleriyle sağlanan ayrıntılar.
Kimlik bilgileri ayrıntıları, **-mquserid** ve **-mqpassword** parametreleri kullanılarak belirtilebilir. **-mqpassword** sağlanmazsa, kullanıcıdan girişin görüntülenmediği parolayı sorulur.

Bir kimlik bilgileri dosyasından sağlanan ayrıntılar: `MQMFTCredentials.xml`.
Kimlik bilgileri ayrıntıları, `MQMFTCredentials.xml` dosyasında açık metin ya da gizlenmiş metin olarak önceden tanımlanabilir.

IBM MQ for Multiplatforms üzerinde MQMFTCredentials.xml dosyası ayarlama hakkında bilgi için bkz. “Configuring MQMFTCredentials.xml on multiplatforms” sayfa 521.

IBM MQ for z/OS üzerinde MQMFTCredentials.xml dosyası ayarlama hakkında bilgi için bkz. “z/OS üzerinde MQMFTCredentials.xml ' ın yapılandırılması” sayfa 523.

Öncelik

Kimlik bilgileri ayrıntılarının belirlenmesinin önceliği:

1. Komut satırı bağımsız değişkeni.
2. `MQMFTCredentials.xml` dizini, ilişkili kuyruk yöneticisi ve komutu çalıştıran kullanıcı tarafından.
3. `MQMFTCredentials.xml` dizini ilişkili kuyruk yöneticisine göre.
4. IBM MQya da IBM WebSphere MQ ' in önceki yayınlarıyla uyumluluğu sağlamak için kimlik bilgisi ayrıntılarının sağlanmadığı varsayılan geriye doğru uyumluluk kipi

Notlar:

- **`fteStartAgent`** ve **`fteStartLogger`** komutları, **-mquserid**ya da **-mqpassword**komut satırı bağımsız değişkenini desteklemez ve kimlik bilgileri ayrıntıları yalnızca `MQMFTCredentials.xml` dosyasıyla belirtilebilir.
- z/OS

  z/OS' da, kullanıcı parolasının küçük harfleri olsa bile, parola büyük harfli olmalıdır. Örneğin, kullanıcının parolası "password" ise, "PASSWORD" olarak girilmelidir.

İlgili başvurular
Hangi MFT komutunun hangi kuyruk yöneticisine bağlandığı
MFT kimlik bilgileri dosya biçimi

Configuring `MQMFTCredentials.xml` on multiplatforms

Güvenlik etkinleştirilmiş olarak Managed File Transfer (MFT) yapılandırılırsa, bağlantı kimlik doğrulaması, kullanıcı kimliği ve parola kimlik bilgilerini sağlamak için bir kuyruk yöneticisiyle bağlantı sağlayan tüm MFT komutlarının kullanılmasını gerektirir. Benzer şekilde, bir veritabanına bağlanırken bir kullanıcı kimliği ve parola belirtmek için MFT kaydedicilerini de belirtmeniz gerekebilir. Bu kimlik bilgisi bilgileri, MFT kimlik bilgileri dosyasında depolanabilir.

Bu görev hakkında

`MQMFTCredentials.xml` dosyasındaki öğelerin `MQMFTCredentials.xsd` şemasına uygun olması gerekir. `MQMFTCredentials.xml`biçimiyle ilgili bilgi için bkz. MFT kimlik bilgileri dosya biçimi.

You can find a sample credentials file in the `MQ_INSTALLATION_PATH/mqft/samples/credentials` directory.

You can have one MFT credentials file for the coordination queue manager, one for the command queue manager, one for each agent, and one for each logger. Diğer bir seçenek olarak, topolojinizde her şey tarafından kullanılan bir dosya da olabilir.

MFT kimlik bilgileri dosyasının varsayılan konumu şu şekildir:

Linux UNIX **UNIX and Linux**

`$HOME`

Windows **Windows**

`%USERPROFILE%` ya da `%HOMEDRIVE%%HOMEPATH%`

Kimlik bilgileri dosyası farklı bir yerde saklandıysa, komutların nereye bakması gerektiğini belirtmek için aşağıdaki özellikleri kullanabilirsiniz:

Çizelge 91. : Çeşitli komutlar için MQMFTCredentials.xml dosyasının konumunu tanımlayan özellikler.

Komut tipi	**Özellik Dosyası**	**Özellik adı**
Koordinasyon kuyruğu yöneticisine bağlanan komut	coordination.properties	coordinationQMgrAuthenticationCredentialsDosyası
Komut kuyruk yöneticisine bağlanan komut	connection.properties	connectionQMgrAuthenticationCredentialsDosyası
Bir aracı işlemine bağlanan komut	agent.properties	agentQMgrAuthenticationCredentialsDosyası
Bir günlüğe kaydedici işlemine bağlanan komut	logger.properties	loggerQMgrAuthenticationCredentialsDosyası

Çizelge 92. : Aracılar ve günlüğe kaydedici işlemleri için MQMFTCredentials.xml dosyasının konumunu tanımlayan özellikler.

Komut tipi	**Özellik Dosyası**	**Özellik adı**
MFT aracılar	agent.properties	agentQMgrAuthenticationCredentialsDosyası
MFT Günlüğe kaydediciler	logger.properties	loggerQMgrAuthenticationCredentialsDosyası

Hangi komut ve süreçlerin hangi kuyruk yöneticisine bağlanacağı ile ilgili ayrıntılar için bkz. Hangi MFT komutları ve işlemleri hangi kuyruk yöneticisine bağlanır.

Kimlik bilgileri dosyası, kullanıcı kimliği ve parola bilgilerini içerdiğinden, yetkisiz erişimi önlemek için özel izinler gerektirir:

Linux UNIX **UNIX and Linux**

```
chown <agent owner userid>
chmod 600
```

Windows **Windows**

Edinmenin etkinleştirilmediğinden emin olun ve kimlik bilgileri dosyasını kullanacak olan aracıyı ya da kaydediciyi çalıştıran kullanıcılar dışındaki tüm kullanıcı kimliklerini kaldırın.

The credential details used to connect to an MFT coordination queue manager, in the IBM MQ Explorer Managed File Transfer plug-in for , depends on the type of configuration:

Genel (yerel diskteki yapılandırma)
Genel yapılandırma, eşgüdümleme ve komut özelliklerinde belirtilen kimlik bilgileri dosyasını kullanır.

Yerel (IBM MQ Exploreriçinde tanımlı):
Yerel bir yapılandırma, IBM MQ Explorer' ta ilişkili kuyruk yöneticisinin bağlantı ayrıntılarının özelliklerini kullanır.

İlgili görevler

"MFTiçin bağlantı kimlik doğrulamasının etkinleştirilmesi" sayfa 525
Bir koordinasyon kuyruğu yöneticisi ya da komut kuyruğu yöneticisiyle bağlantı kuran IBM MQ Explorer MFT eklentisinin bağlantı kimlik doğrulaması ve bir koordinasyon kuyruk yöneticisine ya da komut kuyruğu yöneticisine bağlantı kuran bir Managed File Transfer aracısına ilişkin bağlantı kimlik doğrulaması uyumluluk kipinde ya da MQCSP kimlik doğrulama kipinde çalıştırılabilir.

İlgili başvurular

MFT kimlik bilgileri dosya biçimi

`fteObfuscate`: hassas verileri şifreleyin

z/OS z/OS üzerinde `MQMFTCredentials.xml` ' ın yapılandırılması

Managed File Transfer (MFT) güvenlik etkinleştirilmiş olarak yapılandırıldıysa, bağlantı kimlik doğrulaması, kullanıcı kimliği ve parola kimlik bilgilerini sağlamak için tüm MFT aracılarını ve bir kuyruk yöneticisine bağlanan komutları gerektirir.

Benzer şekilde, MFT kaydedicilerinin bir veritabanına bağlanırken kullanıcı kimliği ve parola belirtmeleri gerekebilir.

Bu kimlik bilgileri MFT kimlik bilgileri dosyasında saklanabilir. Kimlik bilgileri dosyalarının isteğe bağlı olduğunu, ancak ortamı özelleştirmeden önce gerek duyduğunuz dosyayı ya da dosyaları tanımlamanın daha kolay olduğunu unutmayın.

Buna ek olarak, kimlik bilgileri dosyalarınız varsa, daha az uyarı iletisi alırsınız. Uyarı iletileri, MFT ' in kuyruk yöneticisi güvenliğinin kapalı olduğunu ve bu nedenle kimlik doğrulama ayrıntılarını sağlamadığınızı belirtmiştir.

`MQ_INSTALLATION_PATH/mqft/samples/credentials` dizininde örnek bir kimlik bilgileri dosyası bulabilirsiniz.

Aşağıda bir `MQMFTCredentials.xml`dosyası örneği verilmiştir:

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MFTCredentials.xsd">
  <tns:qmgr name="MQPH" user="ADMIN" mqUserId="JOHNDOEH" mqPassword="cXXXX" />
  <tns:qmgr name="MQPI" user="ADMIN" mqUserId="JOHNDOEI" mqPassword="yXXXX" />
  <tns:qmgr name="MQPH" mqUserId="NONEH" mqPassword="yXXXX" />
  <tns:qmgr name="MQPI" mqUserId="NONEI" mqPassword="yXXXX" />
</tns:mqmftCredentials>
```

ADMIN kullanıcı kimlikli bir işin kuyruk yöneticisi MQPH ' ye bağlanması gerektiğinde, *JOHNDOEH* kullanıcı kimliğini geçirir ve *cXXXX*parolasını kullanır.

İş başka bir kullanıcı kimliği tarafından çalıştırılırsa ve MQPH ile bağlantı kurarsa, bu iş *NONEH* kullanıcı kimliğini ve *yXXXX*parolasını geçirir.

`MQMFTCredentials.xml` dosyasının varsayılan konumu, kullanıcının z/OS UNIX System Services (USS) üzerindeki ana dizinidir. Ayrıca, dosyayı USS ' de farklı bir yerde ya da bölümlenmiş bir veri kümesindeki bir üyede saklayabilirsiniz.

Kimlik bilgileri dosyası farklı bir konumda saklandıysa, komutların bu dosyayı nerede arayacağını belirtmek için aşağıdaki özellikleri kullanabilirsiniz:

Çizelge 93. : Çeşitli komutlar için MQMFTCredentials.xml dosyasının yerini tanımlayan özellikler.		
Komut tipi	**Özellik Dosyası**	**Özellik adı**
Koordinasyon kuyruk yöneticisine bağlanan komut	coordination.properties	coordinationQMgrAuthenticationCredentialsDosyası
Komut kuyruğu yöneticisine bağlanan komut	connection.properties	connectionQMgrAuthenticationCredentialsDosyası
Bir aracı işlemine bağlanan komut	agent.properties	agentQMgrAuthenticationCredentialsDosyası
Bir kaydedici işlemine bağlanan komut	logger.properties	loggerQMgrAuthenticationCredentialsDosyası

Çizelge 94. : Aracılar ve kaydedici işlemleri için MQMFTCredentials.xml dosyasının yerini tanımlayan özellikler.		
Komut tipi	**Özellik Dosyası**	**Özellik adı**
MFT aracılar	agent.properties	agentQMgrAuthenticationCredentialsDosyası
MFT Günlüğe kaydediciler	logger.properties	loggerQMgrAuthenticationCredentialsDosyası

Hangi komutların ve işlemlerin hangi kuyruk yöneticisine bağlanacağı hakkında ayrıntılı bilgi için Hangi MFT komutlarının ve işlemlerinin hangi kuyruk yöneticisine bağlandığıkonusuna bakın.

Bölümlenmiş bir veri kümesi içinde kimlik bilgileri dosyası oluşturmak için aşağıdaki adımları gerçekleştirin:

- VB ve mantıksal kayıt uzunluğu (Lrecl) 200 biçimindeki bir PDSE yaratın.
- Veri kümesi içinde bir üye oluşturun, veri kümesi ve üyeyi not edin ve üyeye aşağıdaki kodu ekleyin:

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MQMFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MQMFTCredentials.xsd">
  <!—-credentials information goes here-->
</tns:mqmftCredentials>
```

Kimlik bilgileri dosyasını bir güvenlik ürünü kullanarak koruyabilirsiniz; örneğin, RACF, ancak Managed File Transfer komutlarını çalıştıran kullanıcı kimlikleri ve aracı ve günlük kaydedici işlemlerini yönetme, bu dosyaya okuma erişimi gerekir.

Bu dosyadaki bilgileri BFGCROBS üyesindeki JCL ' yi kullanarak gizleyebilirsiniz. Bu işlem dosyayı alır ve IBM MQ kullanıcı kimliğini ve parolasını şifreler. Örneğin, BFGCROBS üyesi satırı alır

```
<tns:qmgr name="MQPI" user="JOHNDOE2" mqUserId="JOHNDOE1" mqPassword="yXXXX" />
```

ve yaratır

```
<tns:qmgr mqPasswordCipher="e977c61e9b9c363c" mqUserIdCipher="c394c5887867157c"
name="MQPI" user="JOHNDOE2"/>
```

Kullanıcı kimliğini IBM MQ kullanıcı kimliği eşlemesine alıkoymak istiyorsanız, dosyaya açıklamalar ekleyebilirsiniz. Örnek:

```
<!--      name="MQPI" user="ADMIN"    mqUserId="JOHNDOE1 -->
```

Bu yorumlar, gizleme süreci tarafından değiştirilmez.

İçeriğin gizlendiğini, güçlü bir şekilde şifrelenmediğini unutmayın. Dosyaya erişebilecek kullanıcı kimliklerini sınırlandırmanız gerekir.

İlgili görevler

“Configuring MQMFTCredentials.xml on multiplatforms” sayfa 521
Güvenlik etkinleştirilmiş olarak Managed File Transfer (MFT) yapılandırılırsa, bağlantı kimlik doğrulaması, kullanıcı kimliği ve parola kimlik bilgilerini sağlamak için bir kuyruk yöneticisiyle bağlantı sağlayan tüm MFT komutlarının kullanılmasını gerektirir. Benzer şekilde, bir veritabanına bağlanırken bir kullanıcı kimliği ve parola belirtmek için MFT kaydedicilerini de belirtmeniz gerekebilir. Bu kimlik bilgisi bilgileri, MFT kimlik bilgileri dosyasında depolanabilir.

MFTiçin bağlantı kimlik doğrulamasının etkinleştirilmesi

Bir koordinasyon kuyruğu yöneticisi ya da komut kuyruğu yöneticisiyle bağlantı kuran IBM MQ Explorer MFT eklentisinin bağlantı kimlik doğrulaması ve bir koordinasyon kuyruk yöneticisine ya da komut kuyruğu yöneticisine bağlantı kuran bir Managed File Transfer aracısına ilişkin bağlantı kimlik doğrulaması uyumluluk kipinde ya da MQCSP kimlik doğrulama kipinde çalıştırılabilir.

Bu görev hakkında

IBM MQ 9.1.1öncesinde uyumluluk kipi, bağlantı kimlik doğrulaması için varsayılan ayardır. Ancak, varsayılan uyumluluk modunu geçersiz kılabilir ve MQCSP kimlik doğrulama kipini etkinleştirebilirsiniz.

V 9.1.1 IBM MQ 9.1.1' tan, MQCSP kimlik doğrulama kipi varsayılan değerdir.

IBM MQ Explorer Managed File Transfer eklentisine ilişkin bağlantı kimlik doğrulaması ya da CLIENT iletimi kullanılarak bir kuyruk yöneticisine bağlanan Managed File Transfer aracıları için, 12 karakterden uzun parolalar yalnızca MQCSP kimlik doğrulama kipi için desteklenir. Uyumluluk kipi kullanılarak yetki verilirken 12 karakterden daha uzun bir parola belirtirseniz, bir hata oluşur ve aracı kuyruk yöneticisiyle kimlik doğrulamasında olmaz. Tanılama iletileri: BFGAG0001 - BFGAG9999içindeki BFGAG0187E iletisine bakın.

Yordam

- IBM MQ Explorer' ta bir eşgüdümleme kuyruk yöneticisi ya da komut kuyruğu yöneticisi için bağlantı kimlik doğrulama kipini seçmek üzere aşağıdaki adımları tamamlayın:
  a) Bağlanmak istediğiniz kuyruk yöneticisini seçin.
  b) Farenin sağ düğmesini tıklatın ve beliren menüden **Bağlantı Ayrıntıları-> Özellikler** seçeneklerini belirleyin.
  c) **Kullanıcı kimliği** etiketini tıklatın.
  d) Kullanmak istediğiniz bağlantı kimlik doğrulaması moduna ilişkin onay kutusunun seçili olduğundan emin olun:
     – V 9.1.0 Varsayılan olarak, IBM MQ 9.1.0' tan **Kullanıcı kimliği uyumluluk kipi** onay kutusu seçilmez. Diğer bir deyişle, **Kullanıcı kimliğini etkinleştir** onay kutusu seçiliyse, IBM MQ Explorer kuyruk yöneticisine bağlanırken MQCSP kimlik doğrulamasını kullanır. IBM MQ Explorer 'in kuyruk yöneticisine MQCSP kimlik doğrulaması yerine uyumluluk kipini kullanarak bağlanması gerekiyorsa, hem **Kullanıcı kimliğini etkinleştir** ' in hem de **Kullanıcı tanımlama uyumluluğu kipi** onay kutularının seçili olmasına dikkat edin.
     – IBM MQ 9.1.0öncesinde, varsayılan olarak **Kullanıcı tanıtımı uyumluluk kipi** onay kutusu seçili olur. Diğer bir deyişle, **Kullanıcı kimliğini etkinleştir** onay kutusu seçiliyse, IBM MQ Explorer kuyruk yöneticisine bağlanırken uyumluluk kipini kullanır. IBM MQ Explorer ' in MQCSP kimlik doğrulamasını kullanarak kuyruk yöneticisine bağlanması gerekiyorsa, **Kullanıcı kimliğini geçerli kıl** onay kutusunun seçili olduğundan ve **Kullanıcı tanımlama uyumluluğu kipi** onay kutusunun seçili olmadığından emin olun.

- To enable or disable MQCSP authentication mode for a Managed File Transfer agent by using the `MQMFTCredentials.xml` file, add the parameter **useMQCSPAuthentication** to the `MQMFTCredentials.xml` file for the relevant user.

  useMQCSPAuthentication parametresi aşağıdaki değerlere sahiptir:

  doğru
  MQCSP kimlik doğrulama kipi, kullanıcı kimliğini kuyruk yöneticisiyle doğrulamak için kullanılır.

  V 9.1.1 IBM MQ 9.1.1' tan, `true` varsayılan değerdir. If the **useMQCSPAuthentication** parameter is not specified, it is by default set to `doğru` and MQCSP authentication mode is used to authenticate the user with the queue manager..

  yanlış
  Uyumluluk kipi, kullanıcı kimliğini kuyruk yöneticisiyle doğrulamak için kullanılır.

  Before IBM MQ 9.1.1, if the **useMQCSPAuthentication** parameter is not specified, it is by default set to `yanlış` and compatibility mode is used to authenticate the user with the queue manager.

  Aşağıdaki örnek, `MQMFTCredentials.xml` dosyasında **useMQCSPAuthentication** parametresinin nasıl ayarlanacak şekilde ayarlanacak şekilde gösterileceğini göstermektedir:

```
<tns:qmgr name="CoordQueueMgr" user="ernest" mqUserId="ernest"
    mqPassword="AveryL0ngPassw0rd2135" useMQCSPAuthentication="true"/>
```

İlgili kavramlar

“MQCSP parola koruması” sayfa 28
From IBM MQ 8.0, you can send passwords that are included in the MQCSP structure either protected, by using IBM MQ functionality, or encrypted, by using TLS encryption.

İlgili başvurular

“MFT ve IBM MQ bağlantı doğrulaması” sayfa 520
Bağlantı kimlik doğrulaması, bir kuyruk yöneticisinin, sağlanan bir kullanıcı kimliği ve parola kullanarak uygulamaların kimliğini doğrulayabilmesi için yapılandırılmasına olanak sağlar. İlişkili kuyruk yöneticisinde güvenlik etkinleştirildiyse ve kimlik bilgileri ayrıntıları (kullanıcı kimliği ve parola) gerektiriyorsa, kuyruk yöneticisiyle başarılı bir bağlantı kurulabilmesi için bağlantı kimlik doğrulama özelliğinin etkinleştirilmesi gerekir. Bağlantı kimlik doğrulaması uyumluluk kipinde ya da MQCSP kimlik doğrulama kipinde çalıştırılabilir.

MFT kimlik bilgileri dosya biçimi

MFT sandboxes

Aracının aktarmanın bir parçası olarak erişebildiği dosya sisteminin alanını kısıtlayabilirsiniz. Aracının kısıtlanmış olduğu alan korumalı alan adı verilir. Ya aracıya ya da bir aktarım isteğinde bulunan kullanıcıya sınırlandırmalar uygulayabilirsiniz.

Aracı bir iletişim kuralı köprüsü aracıysa ya da bir Connect:Direct köprüsü aracıysa, çalışma yerleri desteklenmez. You can not use agent sandboxing for agents that need to transfer to or from IBM MQ queues.

İlgili başvurular

“MFT aracı korumalı alanlarıyla çalışma” sayfa 527
Managed File Transfer' a ek bir güvenlik düzeyi eklemek için, aracının erişebileceği bir dosya sisteminin alanını sınırlayabilirsiniz.

“MFT kullanıcı korumalı alanlarıyla çalışma” sayfa 528
Dosyaların aktarılabildiği dosya sisteminin alanını kısıtlayabilir ve aktarımın istendiği MQMD kullanıcı adına dayalı olarak bu alana veri aktarılabilir.

MFT aracı korumalı alanlarıyla çalışma

Managed File Transfer' a ek bir güvenlik düzeyi eklemek için, aracının erişebileceği bir dosya sisteminin alanını sınırlayabilirsiniz.

IBM MQ kuyruklarından ya daqueueskuyruklarından aktarım yapan aracılar için aracı kum bokunu kullanamazsınız. Restricting access to IBM MQ queues with sandboxing can be implemented instead by using user sandboxing which is the recommended solution for any sandboxing requirements. Kullanıcı kum boksu hakkında daha fazla bilgi için bkz. “MFT kullanıcı korumalı alanlarıyla çalışma” sayfa 528

Aracı kum bokunu etkinleştirmek için kısıtlamak istediğiniz aracıya ilişkin `agent.properties` dosyasına aşağıdaki özelliği ekleyin:

```
sandboxRoot=[!]restricted_directory_nameseparator...separator[!]restricted_directory_name
```

Burada:

- *restricted_directory_name* , izin verilecek ya da reddedilecek bir dizin yolsıdır.
- `!` isteğe bağlıdır ve *restricted_directory_name* için aşağıdaki değerin reddedildiğini (kapsam dışı bırakıldı) belirtir. If `!` is not specified *restricted_directory_name* is an allowed (included) path.
- *separator* , platforma özgü ayırıcıdır.

For example, if you want to restrict the access that AGENT1 has to the `/tmp` directory only, but not allow the subdirectory `private` to be accessed, set the property as follows in the `agent.properties` file belonging to AGENT1: `sandboxRoot=/tmp:!/tmp/private`.

sandboxRoot özelliği, Gelişmiş aracı özellikleriiçinde açıklanır.

İletişim kuralı köprüsü aracılarında ya da Connect:Direct köprüsü aracılarında hem aracı hem de kullanıcı zımpara işlemi desteklenmez.

UNIX, Linuxve Windows platformlarında bir korumalı alanda çalışma

ULW UNIX, Linuxve Windows platformlarında, kum havuzu, Managed File Transfer Agent ' un hangi dizinlerden okuyabileceği ve yazabileceği dizinlere kısıtlar. Kum havuzu etkinleştirildiğinde Managed File Transfer Agent , izin verilen dizinleri ve belirtilen dizinlerin içerdiği alt dizinleri sandboxRoot' de reddedilen şekilde belirtilinceye kadar okuyabilir ve bu dizinlerin içereceği alt dizinlere yazabilir. Managed File Transfer kum havuzu, işletim sistemi güvenliğinden öncelikli değildir. Managed File Transfer Agent ' e başlayan kullanıcı, dizine okuyabilmek ya da dizine yazabilmek için, herhangi bir dizine uygun işletim sistemi düzeyinde erişime sahip olmalıdır. Bağlı dizin belirtilen sandboxRoot dizinlerinin (ve alt dizinlerinin) dışındaysa, dizine sembolik bir bağlantı izlenmez.

z/OSüzerinde bir korumalı alanda çalışma

z/OS z/OS'ta kum havuzu, Managed File Transfer Agent ' un okuyabileceği ve yazabileceği veri kümesi adı niteleyicilerini kısıtlar. Managed File Transfer Agent ' i başlatan kullanıcı, ilgili veri kümelerine ilişkin doğru işletim sistemi yetkililerine sahip olmalıdır. Bir sandboxRoot veri kümesi adı niteleyicisi değerini çift tırnak içine aldıysanız, değer, normal z/OS kuralını izler ve tam olarak nitelenmiş olarak işlem görür. Çift tırnak işaretlerini çıkarırsanız, sandboxRoot önekli olarak yürürlükteki kullanıcı kimliği eklenir. Örneğin, sandboxRoot özelliğini şu şekilde ayarlayın: `sandboxRoot=//test`, aracı aşağıdaki veri kümelerine (standart z/OS gösteriminde) *//username*`.test.**` yürütme sırasında erişebilir; tam olarak çözümlenen veri kümesi adının ilk düzeyleri sandboxRootile eşleşmiyorsa, aktarma isteği reddedilir.

IBM i sistemlerinde bir çalışma yerinde çalışma

IBM i IBM i sistemlerindeki tümleşik dosya sistemindeki dosyalar için, kum havuzu, Managed File Transfer Agent ' un okuyabileceği ve yazabileceği dizinlere kısıtlar. Kum havuzu etkinleştirildiğinde Managed File Transfer Agent , izin verilen dizinleri ve belirtilen dizinlerin içerdiği alt dizinleri sandboxRoot'

de reddedilen şekilde belirtilinceye kadar okuyabilir ve bu dizinlerin içereceği alt dizinlere yazabilir. Managed File Transfer kum havuzu, işletim sistemi güvenliğinden öncelikli değildir. Managed File Transfer Agent ' e başlayan kullanıcı, dizine okuyabilmek ya da dizine yazabilmek için, herhangi bir dizine uygun işletim sistemi düzeyinde erişime sahip olmalıdır. Bağlı dizin belirtilen sandboxRoot dizinlerinin (ve alt dizinlerinin) dışındaysa, dizine sembolik bir bağlantı izlenmez.

İlgili başvurular

"Genel arama karakteri aktarımları için ek denetimler" sayfa 531
Aracının dosya aktarabileceği yerleri kısıtlamak için bir kullanıcı ya da aracı kum havuzu ile yapılandırılmış bir aracı yapılandırıldıysa, o aracı için genel arama karakteri aktarımları üzerinde ek denetimler yapılabileceğini belirtebilirsiniz.

"MFT aracı korumalı alanlarıyla çalışma" sayfa 527
Managed File Transfer' a ek bir güvenlik düzeyi eklemek için, aracının erişebileceği bir dosya sisteminin alanını sınırlayabilirsiniz.

The MFT `agent.properties` file

MFT kullanıcı korumalı alanlarıyla çalışma

Dosyaların aktarılabildiği dosya sisteminin alanını kısıtlayabilir ve aktarımın istendiği MQMD kullanıcı adına dayalı olarak bu alana veri aktarılabilir.

Aracı bir iletişim kuralı köprüsü aracıysa ya da bir Connect:Direct köprüsü aracıysa, kullanıcı çalışma yerleri desteklenmez.

Kullanıcı kum bokunu etkinleştirmek için kısıtlamak istediğiniz aracıya ilişkin `agent.properties` dosyasına aşağıdaki özelliği ekleyin:

```
userSandboxes=true
```

When this property is present and set to true the agent uses the information in the *MQ_DATA_PATH*/`mqft/config/`*coordination_qmgr_name*`/agents/`*agent_name*`/UserSandboxes.xml` file to determine which parts of the file system the user who requests the transfer can access.

`UserSandboxes.xml` XML, sıfır ya da daha fazla <sandbox> öğesi içeren bir <agent> öğelerinden oluşur. Bu öğeler, hangi kullanıcıların hangi kurallara uygulandığını açıklar. <sandbox> öğesinin `user` özniteliği, isteğin MQMD kullanıcısıyla eşleşmek için kullanılan bir örüntüdür.

`UserSandboxes.xml` dosyası düzenli olarak aracı tarafından yeniden yüklenir ve dosyada yapılan geçerli değişiklikler, aracının davranışını etkiler. Varsayılan yeniden yükleme aralığı 30 saniyedir. Bu aralık, `agent.properties` dosyasında xmlConfigReloadInterval adlı aracı özelliği belirtilerek değiştirilebilir.

`userPattern="regex"` özniteliğini veya değerini belirtirseniz, `user` özniteliği bir Java düzenli ifadesi olarak yorumlanır. Daha fazla bilgi için bkz. MFT tarafından kullanılan düzenli ifadeler.

`userPattern="regex"` özniteliğini ya da değerini belirtmezseniz, `user` özniteliği aşağıdaki genel arama karakterlerine sahip bir örüntü olarak yorumlanır:

- yıldız işareti (*), sıfır ya da daha fazla karakteri temsil eder
- tam olarak bir karakteri temsil eden soru işareti (?)

Matches are performed in the order that the <sandbox> elements are listed in the file. Yalnızca ilk eşleşme kullanılır, dosyadaki tüm olası eşleşmeler yoksayılır. Dosyada belirtilen <sandbox> öğelerinden hiçbiri, aktarma isteği iletisiyle ilişkili MQMD kullanıcısıyla eşleşmiyorsa, aktarma dosya sistemine erişemez. MQMD kullanıcı adı ve bir `user` özniteliği arasında bir eşleşme bulunduğunda, eşleştirme, aktarıma uygulanan bir <sandbox> öğesinin içindeki bir kural kümesini tanımlar. This set of rules is used to determine which filesYa da veri kümeleri, can be read from or written to as part of the transfer.

Her bir kural kümesi, hangi dosyaların okunabileceğini tanımlayan bir <read> öğesini ve hangi dosyaların yazılabileceğini tanımlayan bir <write> öğesini belirtebilir. <read> ya da <write> öğelerini bir kural kümesinden çıkarırsanız, bu kural kümesiyle ilişkilendirilmiş kullanıcının okuma ya da yazma işlemi gerçekleştirmesine izin verilmediği varsayılır.

Not: The <read> element must be before the <write> element, and the <include> element must be before the <exclude> element, in the UserSandboxes.xml file.

Her <read> ya da <write> öğesi, bir dosyanın korumalı alanda olup olmadığını ve aktarılıp aktarılamayacağını belirlemek için kullanılan bir ya da daha fazla kalıp içerir. <include> ve <exclude> öğelerini kullanarak bu örüntüleri belirtin. <include> ya da <exclude> öğesinin name özniteliği, eşleştirilecek örüntüyi belirtir. İsteğe bağlı bir type özniteliği, ad değerinin bir dosya mı, yoksa kuyruk örünü mü olduğunu belirtir. type özniteliği belirtilmezse, aracı örüntüye bir dosya ya da dizin yolu örünü olarak davranır. Örneğin:

```
<tns:read>
    <tns:include name="/home/user/**"/>
    <tns:include name="USER.**" type="queue"/>
    <tns:exclude name="/home/user/private/**"/>
</tns:read>
```

The <include> and <exclude> name patterns are used by the agent to determine whether files, veri kümeleri, or queues can be read from or written to. Kurallı dosya yolu, veri kümesi, ya da kuyruk adı, içerilen örüntülerin en az biri ve dışlanan örüntülerin tam olarak sıfırı ile eşleşiyorsa, bir işleme izin verilir. <include> ve <exclude> öğelerinin name özniteliği kullanılarak belirtilen kalıplar, aracının üzerinde çalışmakta olduğu platforma uygun yol ayırıcıları ve kuralları kullanır. Göreli dosya yolları belirtirseniz, yollar aracının transferRoot özelliğine göre çözümlenir.

Bir kuyruk kısıtlaması belirtirken, aşağıdaki kurallarla birlikte QUEUE@QUEUEMANAGER sözdizimi desteklenir:

- Girdide karakter (@) eksikse, örüntü, herhangi bir kuyruk yöneticisinde erişilebilen bir kuyruk adı olarak kabul edilir. Örneğin, örüntü name ise, name@**ile aynı şekilde davranılır.
- Girişteki karakter (@) ilk karakterse, örüntü kuyruk yöneticisi adı olarak kabul edilir ve kuyruk yöneticisinde tüm kuyruklara erişilebilir. Örneğin, örüntü @name ise, **@nameile aynı şekilde davranılır.

<include> ve <exclude> öğelerinin name özniteliğinin bir parçası olarak bunları belirlediğinizde, aşağıdaki genel arama karakterlerinin özel anlamı vardır:

*****
: Tek bir yıldız işareti, bir dizin adındaki sıfır ya da daha fazla karakterle ya da bir veri kümesi adı ya da kuyruk adının niteleyicisinde eşleşir.

?
: Soru işareti, bir dizin adında ya da bir veri kümesi adı ya da kuyruk adının niteleyicisinde tam olarak bir karakterle eşleşir.

******
: İki yıldız işareti, sıfır ya da daha fazla dizin adı ya da bir veri kümesi adı ya da kuyruk adında sıfır ya da daha fazla niteleyiciyle eşleşir. Ayrıca, yol ayırıcısıyla biten yollar, yolun sonuna eklenmiş örtük bir "**" ' ya sahiptir. Yani /home/user/ , /home/user/**ile aynıdır.

Örneğin:

- /**/test/** , yoluna test dizini olan herhangi bir dosyayla eşleşir.
- /test/file? , /test dizgisiyle başlayan ve file dizgisiyle başlayan ve ardından herhangi bir tek karakter ile eşleşen herhangi bir dosya ile eşleşir.
- c:\test*.txt matches any file inside the c:\test directory with a .txt extension
- c:\test***.txt , 'c:\test dizinindeki herhangi bir dosyaya ya da .txt uzantısına sahip olan alt dizinlerinden biriyle eşleşir.
- z/OS //'TEST.*.DATA' matches any data set that has the first qualifier of TEST, has any second qualifier, and a third qualifier of DATA.
- *@QM1 , tek bir niteleyiciye sahip QM1 kuyruk yöneticisindeki kuyruklarla eşleşir.

- TEST.*.QUEUE@QM1 matches any queue on the queue manager QM1 that has the first qualifier of TEST, has any second qualifier, and a third qualifier of QUEUE.
- **@QM1 , kuyruk yöneticisindeki tüm kuyruklarla eşleşiyor QM1.

Simgesel bağlantılar

<include> ve <exclude> öğelerinde sabit bağlantılar belirterek, UserSandboxes.xml dosyasındaki dosya yollarında kullandığınız simgesel bağlantıları tam olarak çözmeniz gerekir. For example, if you have a symbolic link where /var maps to /SYSTEM/var, you must specify this path as <tns:include name="/SYSTEM/var"/>, otherwise the intended transfer fails with a user sandbox security error.

Örnek

This example shows how to allow the user with the MQMD user name guest to transfer any file from the /home/user/public directory or any of its subdirectories on the system where the agent AGENT_JUPITER is running, by adding the following <sandbox> element to the file UserSandboxes.xml in AGENT_JUPITER's configuration directory:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
        xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
        xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
    <tns:agent>
        <tns:sandbox user="guest">
            <tns:read>
                <tns:include name="/home/user/public/**"/>
             </tns:read>
        </tns:sandbox>
    </tns:agent>
</tns:userSandboxes>
```

Örnek

This example shows how to allow any user with the MQMD user name account followed by a single digit, for example account4, to complete the following actions:

- Transfer any file from the /home/account directory or any of its subdirectories, excluding the /home/account/private directory on the system where the agent AGENT_SATURN is running
- Herhangi bir dosyayı /home/account/output dizinine ya da sistemin, AGENT_SATURN görevlisinin çalıştığı sistemdeki alt dizinlerinden herhangi birine aktarın.
- Read messages from queues on the local queue manager starting with the prefix ACCOUNT. unless it starts with ACCOUNT.PRIVATE. (that is has PRIVATE at the second level).
- Verileri, herhangi bir kuyruk yöneticisiyle ilgili olarak ACCOUNT.OUTPUT. önekiyle başlayan kuyruklara aktarabilirsiniz.

MQMD kullanıcı adı account olan bir kullanıcının bu işlemleri tamamlamasına izin vermek için, şu <sandbox> öğesini AGENT_SATURN ' in yapılanış dizininde UserSandboxes.xmlkütüğüne ekleyin:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
            xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
            xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
    <tns:agent>
        <tns:sandbox user="account[0-9]" userPattern="regex">
            <tns:read>
                <tns:include name="/home/account/**"/>
                <tns:include name="ACCOUNT.**" type="queue"/>
                <tns:exclude name="ACCOUNT.PRIVATE.**" type="queue"/>
                <tns:exclude name="/home/account/private/**"/>
                                                    </tns:read>
            <tns:write>
                <tns:include name="/home/account/output/**"/>
                <tns:include name="ACCOUNT.OUTPUT.**" type="queue"/>
```

```
            </tns:write>
        </tns:sandbox>
    </tns:agent>
</tns:userSandboxes>
```

İlgili başvurular

“Genel arama karakteri aktarımları için ek denetimler” sayfa 531
Aracının dosya aktarabileceği yerleri kısıtlamak için bir kullanıcı ya da aracı kum havuzu ile yapılandırılmış bir aracı yapılandırıldıysa, o aracı için genel arama karakteri aktarımları üzerinde ek denetimler yapılabileceğini belirtebilirsiniz.

The MFT `agent.properties` file

Genel arama karakteri aktarımları için ek denetimler

Aracının dosya aktarabileceği yerleri kısıtlamak için bir kullanıcı ya da aracı kum havuzu ile yapılandırılmış bir aracı yapılandırıldıysa, o aracı için genel arama karakteri aktarımları üzerinde ek denetimler yapılabileceğini belirtebilirsiniz.

additionalWildcardSandboxChecking özelliği

Genel arama karakteri aktarımları için ek denetleme etkinleştirmek istiyorsanız, denetlemek istediğiniz aracıya ilişkin `agent.properties` dosyasına aşağıdaki özelliği ekleyin.

```
additionalWildcardSandboxChecking=true
```

Bu özellik true değerine ayarlandığında ve aracı, genel arama karakteriyle eşleşen dosya için tanımlı çalışma yeri dışında olan bir konumu okuma girişiminde bulunan bir aktarma isteği gönderirse, aktarma başarısız olur. Bir aktarma isteğinde birden çok aktarma varsa ve bu isteklerden biri kum havuzunun dışında bir yeri okumayı denediği için başarısız olursa, tüm aktarma başarısız olur. Denetleme başarısız olursa, hata nedenine bir hata iletisinde verilir.

If the additionalWildcardSandboxChecking property is omitted from an agent's `agent.properties` file or is set to false, no additional checks are made on wildcard transfers for that agent.

Joker karakter denetimi için hata iletileri

Bir genel arama karakteri aktarma isteği yapılandırılmış bir korumalı alan konumu dışında bir konuma yapıldığında bildirilen iletiler aşağıdaki gibidir.

Bir aktarma isteğindeki genel arama dosyası yolu kısıtlı korumalı alanın dışında bulunuyorsa aşağıdaki ileti oluşur:

```
BFGSS0077E: Dosya yolunu okuma girişimi: yol reddedildi.
Dosya yolu, sınırlı aktarma korumalı alanın dışında bulunuyor.
```

Birden çok aktarma isteğinde bulunan bir aktarma, yolun kısıtlı kum havuzunun dışında bulunduğu bir genel arama karakteri aktarma isteği içerdiğinde aşağıdaki ileti oluşur:

```
BFGSS0078E: Dosya yolunu okuma girişimi: yol başka bir aktarma olarak yoksayıldı.
yönetilen aktarımda bulunan öğe, sınırlı aktarma korumalı alanın dışında okumayı denedi.
```

Aşağıdaki ileti, kısıtlı korumalı alanın dışında bir dosya bulunduğunda gerçekleşir:

```
BFGSS0079E:  file path kütüğünü okuma girişimi reddedildi.
Dosya, sınırlı aktarım korumalı alanı dışında bulunuyor.
```

Başka bir genel arama karakteri aktarma isteğinin yoksayılmasına neden olan birden çok aktarma isteğinde aşağıdaki ileti ortaya çıkar:

```
BFGSS0080E: Dosya okuma girişimi: file path (dosya yolu) başka bir aktarma olarak yoksayıldı
yönetilen aktarımda bulunan öğe, sınırlı aktarma korumalı alanın dışında okumayı denedi.
```

Genel arama karakteri içermeyen tek dosya aktarımları durumunda, aktarma işlemi, kum havuzunun dışında bulunan bir dosyayı içerdiğinde bildirilen ileti önceki yayın düzeylerinden değiştirilmeden kalır:

```
BFGIO0056E: "FILE" dosyasını okuma girişimi reddedilmiş.
Dosya, sınırlı aktarım korumalı alanı dışında bulunuyor.
```

İlgili başvurular

“MFT kullanıcı korumalı alanlarıyla çalışma” sayfa 528
Dosyaların aktarılabildiği dosya sisteminin alanını kısıtlayabilir ve aktarımın istendiği MQMD kullanıcı adına dayalı olarak bu alana veri aktarılabilir.

“MFT aracı korumalı alanlarıyla çalışma” sayfa 527
Managed File Transfer' a ek bir güvenlik düzeyi eklemek için, aracının erişebileceği bir dosya sisteminin alanını sınırlayabilirsiniz.

The MFT `agent.properties` file

MFTiçin SSL ya da TLS şifrelemesini yapılandırma

SSL ya da TLS ' yi kullanarak, aracılar ile aracı kuyruk yöneticileri arasındaki iletişimi, bağlanmakta oldukları kuyruk yöneticilerini ve topolojiniz içindeki kuyruk yöneticisi bağlantılarını kuyruğa almak için çeşitli kuyruk yöneticisini kullanarak, IBM MQ Managed File Transfer ile kullanılabilir.

Başlamadan önce

Bir IBM MQ Managed File Transfer topolojisinde akan iletileri şifrelemek için SSL ya da TLS şifrelemesini kullanabilirsiniz. Bu üyeler şunlardır:

- Bir aracı ile aracı kuyruk yöneticisi arasında geçen iletiler.
- Komutlara ve bağlanmakta oldukları kuyruk yöneticilerine ilişkin iletiler.
- Topoloji içinde aracı kuyruk yöneticileri, komut kuyruğu yöneticileri ve koordinasyon kuyruk yöneticisi arasında akış yapan iç iletiler.

Bu görev hakkında

For general information about using SSL with IBM MQ, see “SSL/TLS ile çalışma” sayfa 261. IBM MQ terimlerinde, Managed File Transfer standart bir Java istemci uygulamasıdır.

Follow these steps to use SSL with Managed File Transfer:

Yordam

1. Bir güvenilirlik deposu dosyası ve isteğe bağlı olarak bir anahtar deposu dosyası yaratın (bu dosyalar aynı dosya olabilir). İstemci-kimlik doğrulaması gerekmiyorsa (kanallarda SSLCAUTH=OPTIONAL) anahtar deposu sağlamanıza gerek yoktur. Yalnızca kuyruk yöneticisinin sertifikasının kimliğini doğrulamak için bir güvenilirlik deposu gereklidir.

   Güvenli depo ve anahtar depoları için sertifika yaratmak için kullanılan anahtar algoritması, IBM MQile çalışmak için RSA olmalıdır.
2. Set up your IBM MQ queue manager to use SSL.

   Bir kuyruk yöneticisinin IBM MQ Explorer komutunu kullanarak SSL kullanacak şekilde ayarlanmasıyla ilgili bilgi edinmek için Kuyruk yöneticilerindeki SSL ' nin yapılandırılmasıbaşlıklı konuya bakın.
3. Güvenli depo dosyasını ve anahtar deposu dosyasını (varsa) uygun bir yerde saklayın. Önerilen bir konum, *config_directory*/*coordination_qmgr*/agents/*agent_name* dizinidir.
4. Uygun Managed File Transfer özellikler dosyasındaki her SSL etkin kuyruk yöneticisi için gereken SSL özelliklerini ayarlayın. Her özellik kümesi ayrı bir kuyruk yöneticisine (aracı, eşgüdüm ve komut) gönderme yapar; ancak, bir kuyruk yöneticisi bu rollerin iki ya da daha fazlasını gerçekleştirebilse de.

   CipherSpec ya da **CipherSuite** özelliklerinden biri gerekli, tersi durumda istemci SSL olmadan bağlanmayı dener. **CipherSpec** ya da **CipherSuite** özellikleri, IBM MQ ile Javaarasındaki terminoloji farkları nedeniyle sağlanır. Managed File Transfer , her iki özelliği de kabul eder ve gerekli dönüştürmeyi yapar, böylece her iki özelliği de ayarlamamanız gerekir. Hem **CipherSpec** , hem de **CipherSuite** özelliklerini belirtmezseniz, **CipherSpec** öncelik kazanır.

PeerName özelliği isteğe bağlıdır. Özelliği, bağlanmak istediğiniz kuyruk yöneticisinin ayırt edici adını (DN) ayarlayabilirsiniz. Managed File Transfer , uyuşmayan bir Ayırt Edici Ada sahip yanlış bir SSL sunucusuna yönelik bağlantıları reddeder.

Set the **SslTrustStore** and **SslKeyStore** properties to file names that point to the truststore and keystore files. Çalışmakta olan bir aracı için bu özellikleri ayarlıyorsanız, SSL moduna yeniden bağlanmak için aracıyı durdurun ve yeniden başlatın.

Özellikler dosyaları düz metin parolaları içerir, bu nedenle uygun dosya sistemi izinlerini ayarlamayı düşünün.

SSL özellikleri hakkında daha fazla bilgi için bkz. MFTiçin SSL özellikleri.

5. Bir aracı kuyruk yöneticisi SSL kullanıyorsa, aracıyı oluştururken gerekli ayrıntıları sağlayamazsınız. Aracıyı oluşturmak için aşağıdaki adımları kullanın:
   a) **fteCreateAgent** komutunu kullanarak aracıyı oluşturun. Aracıyı koordinasyon kuyruğu yöneticisine yayınlayamamakla ilgili bir uyarı alırsınız.
   b) SSL bilgilerini eklemek için önceki adım tarafından yaratılan `agent.properties` dosyasını düzenleyin. Aracı başarıyla başlatılırsa, yayınlama işlemi yeniden denenir.
6. `agent.properties` dosyasındaki ya da `coordination.properties` dosyasındaki SSL özellikleri değiştirilirken IBM MQ Explorer 'ın aracıları ya da eşgörünümleri çalışıyorsa, aracıyı ya da IBM MQ Explorerdosyasını yeniden başlatmanız gerekir.

İlgili başvurular
The MFT `agent.properties` file

Kanal kimlik doğrulamasıyla istemci kipinde kuyruk yöneticisine bağlanma

IBM WebSphere MQ 7.1 , kanal düzeyinde daha ayrıntılı şekilde erişimi denetlemek için kanal kimlik doğrulama kayıtlarını tanıttı. This change in behavior means that by default newly created IBM WebSphere MQ 7.1 or later queue managers reject client connections from the Managed File Transfer component.

Kanal kimlik doğrulamasıyla ilgili daha fazla bilgi için bkz. “Kanal doğrulama kayıtları” sayfa 47.

Managed File Transfer tarafından kullanılan SVRCONN için kanal kimlik denetimi konfigürasyonu, ayrıcalıklı olmayan bir MCAUSER kimliği belirtiyorsa, Managed File Transfer Agent ve komutların doğru biçimde çalışmasına olanak sağlamak için kuyruk yöneticisi, kuyruklar ve konular için belirli yetki kayıtları vermeniz gerekir. Kanal kimlik doğrulama kayıtlarını yaratmak, değiştirmek ya da kaldırmak için SET CHLAUTH ya da Set Channel Authentication Record (Kanal Kimlik Doğrulama Kaydı Ayarla) MQSC komutunu kullanın. IBM WebSphere MQ 7.1 ya da sonraki bir kuyruk yöneticisine bağlanmak istediğiniz tüm Managed File Transfer aracıları için, tüm aracılarınız için bir MCAUSER kimliği ayarlayabilir ya da her bir aracı için ayrı bir MCAUSER kimliği belirleyebilirsiniz.

Her MCAUSER kimliği için aşağıdaki izinleri verin:

- Kuyruk yöneticisi için gereken yetki kayıtları:
  - CONNECT
  - SETID
  - inq
- Kuyruklar için yetki kayıtları gerekli.

  Aracıya özgü tüm kuyruklar için, aşağıdaki listede *aracı_adı* ' ta sona erdiren kuyruk adlarına sahip olan, istemci bağlantısı kullanarak IBM WebSphere MQ 7.1 ya da sonraki bir kuyruk yöneticisine bağlanmak istediğiniz her aracı için bu kuyruk yetkisi kayıtlarını oluşturmanız gerekir.
  - put, get, dsp (SYSTEM.DEFAULT.MODEL.QUEUE)
  - put, get, setid, browse (SYSTEM.FTE.COMMAND.*agent_name*)
  - tak, get (SYSTEM.FTE.DATA.*agent_name*)
  - tak, get (SYSTEM.FTE.REPLY.*agent_name*)

  - indir, get, inq, browse (SYSTEM.FTE.STATE.*agent_name*)
  - tak, al, göz at (SYSTEM.FTE.EVENT.*agent_name*)
  - tak, get (SYSTEM.FTE)
- Konular için gereken yetki kayıtları:
  - alt, pub (SYSTEM.FTE)
- Dosya aktarımları için yetki kayıtları gerekli.

  Kaynak ve hedef aracı için ayrı MCAUSER kimlikleri varsa, her iki kaynak ve hedefteki aracılar kuyruklarında yetki kayıtlarını oluşturun.

  Örneğin, kaynak aracının MCAUSER kimliği **user1** ise ve hedef aracı MCAUSER kimliği **user2**ise, aracı kullanıcıları için aşağıdaki yetkileri ayarlayın:

AGENT kullanıcısı	Kuyruk	Yetki gerekli
user1	SYSTEM.FTE.DATA.*destination_agent_name*	put
user1	SYSTEM.FTE.COMMAND.*destination_agent_name*	put
user2	SYSTEM.FTE.REPLY.*source_agent_name*	put
user2	SYSTEM.FTE.COMMAND.*kaynak_aracı_adı*	put

Connect:Direct köprüsü aracısı ve Connect:Direct düğümü arasında SSL ya da TLS ' nin yapılandırılması

Configure the Connect:Direct bridge agent and the Connect:Direct node to connect to each other through the SSL protocol by creating a keystore and a truststore, and by setting properties in the Connect:Direct bridge agent properties file.

Bu görev hakkında

Bu adımlar, bir sertifika yetkilisi tarafından imzalanmış anahtarlarınızı almaya ilişkin yönergeleri içerir. Bir sertifika yetkilisi kullanmayacaksa, kendinden onaylı bir sertifika oluşturabilirsiniz. Kendinden onaylı bir sertifika oluşturma hakkında daha fazla bilgi için bkz. “UNIX, Linux, and Windowsüzerinde SSL/TLS ile çalışma” sayfa 273.

Bu adımlar, Connect:Direct bridge Agent için yeni bir anahtar deposu ve güvenilirlik deposu yaratılmasına ilişkin yönergeleri içerir. Connect:Direct köprüsü aracısının, IBM MQ kuyruk yöneticilerine güvenli bir şekilde bağlanmak için kullandığı bir anahtar deposu ve güvenilirlik deposu varsa, Connect:Direct düğümüne güvenli bir şekilde bağlanırken var olan anahtar deposunu ve güvenilir deponu kullanabilirsiniz. Daha fazla bilgi için bkz “MFTiçin SSL ya da TLS şifrelemesini yapılandırma” sayfa 532.

Yordam

Connect:Direct düğümü için aşağıdaki adımları tamamlayın:

1. Connect:Direct düğümü için bir anahtar ve imzalanmış sertifika oluşturun.

   Bunu, IBM MQile birlikte verilen IBM Key Management aracını kullanarak yapabilirsiniz. Daha fazla bilgi için bkz “SSL/TLS ile çalışma” sayfa 261.
2. Anahtarın imzalanmış olması için sertifika yetkilisine bir istek gönderin. Geri dönüşünde bir sertifika alırsınız.
3. Sertifika yetkilinizin genel anahtarını içeren bir metin dosyası oluşturun; örneğin, `/test/ssl/certs/CAcert`.
4. Install the Secure+ Option on the Connect:Direct node.

   Düğüm önceden varsa, var olan kuruluşun yerini belirterek ve yalnızca Secure + Option ürününü kurmayı seçerek, kuruluş programını yeniden çalıştırarak Secure + Option 'ı kurabilirsiniz.
5. Yeni bir metin dosyası oluşturun; örneğin, `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt`.

6. Sertifika yetkilinizden aldığınız sertifikayı ve özel anahtarı (`/test/ssl/cd/privateKeys/`*node_name*`.key`içinde yer alan) metin dosyasına kopyalayın.

   `/test/ssl/cd/keyCertFile/`*node_name*`.txt` içeriğinin aşağıdaki biçimde olması gerekir:

```
-----BEGIN CERTIFICATE-----
MIICnzCCAgigAwIBAgIBGjANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJHQjES
MBAGA1UECBMJSGFtcHNoaXJlMRAwDgYDVQQHEwdIdXJzbGV5MQwwCgYDVQQKEwNJ
Qk0xDjAMBgNVBAsTBU1RSVBUMQswCQYDVQQDEwJDQTAeFw0xMTAzMDExNjIwNDZa
Fw0yMTAyMjYxNjIwNDZaMFAxCzAJBgNVBAYTAkdCMRIwEAYDVQQIEwlIYW1wc2hp
cmUxDDAKBgNVBAoTA0lCTTEOMAwGA1UECxMFTVFGVEUxDzANBgNVBAMTBmJpbmJh
ZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvgP1QIklU9ypSKD1XoODo1yk
EyMFXBOUpZRrDVxjoSEC0vtWNcJ199e+Vc4UpNybDyBu+NkDlMNofX4QxeQcLAFj
WnhakqCiQ+JIAD5Aurhnrwche0MV3kjA84GKH/rOSVqtl984mu/lDyS819XcfSSn
cOOMsK1KbneVSCIV2XECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0E
HxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFNXMIpSc
csBXUniW4A3UrZnCRsv3MB8GA1UdIwQYMBaAFDXY8rmj4lVz5+FVAoQb++cns+B4
MA0GCSqGSIb3DQEBBQUAA4GBAFc7klXa4pGKYgwchxKpE3ZF6FNwy4vBXS216/ja
8h/vl8+iv01OCL8t0ZOKSU95fyZLzOPKnCH7v+ItFSE3CIiEk9Dlz2U6WO9lICwn
l7PL72TdfaL3kabwHYVf17IVcuL+VZsZ3HjLggP2qHO9ZuJPspeT9+AxFVMLiaAb
8eHw
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,64A02DA15B6B6EF9

57kqxLOJ/gRUOIQ6hVK2YN13B4E1jAi1gSme0I5ZpEIG8CHXISKB7/0cke2FTqsV
lvI99QyCxsDWoMNt5fj51v7aPmVeS60bOm+UlGre8B/Ze18JVj2O4K2Uh72rDCXE
5e6eFxSdUM207sQDy20euBVELJtM2kOkL1ROdoQQSlU3XQNgJw/t3ZIx5hPXWEQT
rjRQO64BEhb+PzzxPF8uwzZ9IrUK9BJ/UUnqC6OdBR87IeA4pnJD1Jvb2ML7EN9Z
5Y+50hTKI8OGvBvWXO4fHyvIX5aslwhBoArXIS1AtNTrptPvoaP1zyIAeZ6OCVo/
SFo+A2UhmtEJeOJaZG2XZ3H495fAw/EHmjehzIACwukQ9nSIETgu4A1+CV64RJED
aYBCM8UjaAkbZDH5gn7+eBov0ssXAXWDyJBVhUOjXjvAj/e1h+kcSF1hax5D//AI
66nRMZzboSxNqkjcVd8wfDwP+bEjDzUaaarJTS7lIFeLLw7eJ8MNAkMGicDkycL0
EPBU9X5QnHKLKOfYHN/1WgUk8qt3UytFXXfzTXGF3EbsWbBupkT5e5+lYcX8OVZ6
sHFPNlHluCNy/riUcBy9iviVeodX8IomOchSyO5DKl8bwZNjYtUP+CtYHNFU5BaD
I+1uUOAeJ+wjQYKT1WaeIGZ3VxuNITJul8y5qDTXXfX7vxM5OoWXa6U5+AYuGUMg
/itPZmUmNrHjTk7ghT6i1IQOaBowXXKJBlMmq/6BQXN2IhkD9ys2qrvM1hdi5nAf
egmdiG50loLnBRqWbfR+DykpAhK4SaDi2F52Uxovw3Lhiw8dQP7lzQ==
-----END RSA PRIVATE KEY-----
```

7. Secure + Admin Tool programını başlatın.
   - Linux ya da UNIX sistemlerinde **spadmin.sh**komutunu çalıştırın.
   - Windows sistemlerinde, **Başlat** > **Programlar** > **Sterling Commerce Connect:Direct** > **CD Secure + Admin Tool**seçeneklerini tıklatın.

   Secure + Admin Tool CD ' leri başlatılır.
8. CD Secure + Admin Tool 'da, ana SSL ya da TLS ayarlarını düzenlemek için **.Yerel** satırını çift tıklatın.
   a) Kullandığınız protokole bağlı olarak **SSL İletişim Kuralını Etkinleştir** ya da **TLS İletişim Kuralını Etkinleştir**seçeneğini belirleyin.
   b) **Geçersiz Kılmayı Geçersiz Kıl**seçeneğini belirleyin
   c) En az bir Cipher Suite seçin.
   d) İki yönlü kimlik doğrulaması istiyorsanız, **Enable Client Authentication** (İstemci Kimlik Doğrulamasını Etkinleştir) değerini Yesolarak değiştirin.
   e) **Trusted Root Certificate** (Güvenilen Kök Sertifikası) alanına, sertifikasyon yetkinizin genel sertifika dosyasının yolunu girin `/test/ssl/certs/CAcert`.
   f) **Key Certificate File** (Anahtar Sertifika Dosyası) alanına, oluşturduğunuz dosyanın yolunu girin `/test/ssl/cd/keyCertFile/`*node_name*`.txt`.
9. Ana SSL ya da TLS ayarlarını düzenlemek için **.İstemci** satırını çift tıklatın.
   a) Kullandığınız protokole bağlı olarak **SSL İletişim Kuralını Etkinleştir** ya da **TLS İletişim Kuralını Etkinleştir**seçeneğini belirleyin.
   b) **Geçersiz Kılmayı Geçersiz Kıl**seçeneğini belirleyin

Connect:Direct köprü aracısı için aşağıdaki adımları gerçekleştirin:

10. Bir güvenilirlik deposu yaratın. Bunu, bir kukla anahtar yaratarak ve sonra kukla anahtarı silerek yapabilirsiniz.

    Aşağıdaki komutları kullanabilirsiniz:

    ```
    keytool -genkey -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
    ```

    ```
    keytool -delete -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
    ```

11. Sertifikasyon yetkilisinin genel sertifikasını güvenli depoya aktarın.

    Aşağıdaki komutu kullanabilirsiniz:

    ```
    keytool -import -trustcacerts -alias myCA
            -file /test/ssl/certs/CAcert
            -keystore /test/ssl/fte/stores/truststore.jks
    ```

12. Connect:Direct bridge Agent özellikler dosyasını düzenleyin.

    Dosyanın herhangi bir yerinde aşağıdaki satırları ekleyin:

    ```
    cdNodeProtocol=protocol
    cdNodeTruststore=/test/ssl/fte/stores/truststore.jks
    cdNodeTruststorePassword=password
    ```

    In the example in this step, *iletişim kuralı* is the protocol you are using, either SSL or TLS, and *parola* is the password that you specified when you created the truststore.

13. İki yönlü kimlik doğrulaması istiyorsanız, Connect:Direct bridge Agent için bir anahtar ve sertifika yaratın.

    a) Anahtar deposu ve anahtar oluşturun.

    Aşağıdaki komutu kullanabilirsiniz:

    ```
    keytool -genkey -keyalg RSA -alias agent_name
            -keystore /test/ssl/fte/stores/keystore.jks
            -storepass password -validity 365
    ```

    b) Bir imza isteği oluşturur.

    Aşağıdaki komutu kullanabilirsiniz:

    ```
    keytool -certreq -v -alias agent_name
            -keystore /test/ssl/fte/stores/keystore.jks -storepass password
            -file /test/ssl/fte/requests/agent_name.request
    ```

    c) Önceki adımdan aldığınız sertifikayı anahtar deposuna aktarın. Sertifika, x.509 biçiminde olmalıdır.

    Aşağıdaki komutu kullanabilirsiniz:

    ```
    keytool -import -keystore /test/ssl/fte/stores/keystore.jks
            -storepass password -file certificate_file_path
    ```

    d) Connect:Direct bridge Agent özellikler dosyasını düzenleyin.

    Dosyanın herhangi bir yerinde aşağıdaki satırları ekleyin:

    ```
    cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
    cdNodeKeystorePassword=password
    ```

    Bu adımdaki örnekte *parola* , anahtar deposunu yaratırken belirttiğiniz paroladır.

İlgili görevler

Connect:Direct köprüsünü yapılandırma

ULW AMQP istemcilerinin güvenliğini sağlama

AMQP istemcilerinden bağlantı sağlamak ve verilerin güvenilir bir şekilde ağ üzerinde korunmasını sağlamak için bir dizi güvenlik düzeneği kullanıyorsunuz. MQ Light uygulamalarınıza güvenlik oluşturabilirsiniz. You can also use existing security features of IBM MQ with AMQP clients, in the same way that the features are used for other applications.

Kanal doğrulama kuralları (CHLAUTH)

TCP bağlantılarını kuyruk yöneticiyle sınırlandırmak için kanal doğrulama kurallarını kullanabilirsiniz. AMQP kanalları, kuyruk yöneticiniz için yapılandırdığınız kanal doğrulama kurallarının kullanımını destekler. Kanal doğrulama kuralları, kuyruk yöneticinizin üzerindeki AMQP kanallarıyla eşleşen bir tanıtımla tanımlandıysa, bu kurallar bu kanallara uygulanır. Varsayılan olarak, yeni IBM® MQ kuyruk yöneticisinde kanal kimlik doğrulaması etkinleştirilir; bu nedenle, bir AMQP kanalını kullanmadan önce en az bir yapılandırmayı tamamlamanız gerekir.

Kuyruk yöneticinizin AMQP bağlantılarına izin vermek üzere kanal doğrulama kurallarının nasıl yapılandırılacağı hakkında daha fazla bilgi için AMQP kanallarının yaratılması ve kullanılmasıbaşlıklı konuya bakın.

Bağlantı kimlik doğrulaması (CONNAUTH)

Bir kuyruk yöneticiyle bağlantı doğrulamak için bağlantı kimlik doğrulamasını kullanabilirsiniz. AMQP kanalları, AMQP uygulamalarından kuyruk yöneticisine erişimi denetlemek için bağlantı kimlik doğrulamasının kullanılmasını destekler.

AMQP protokolü, bir bağlantının nasıl doğrulanır olduğunu belirtmek için SASL (Simple Authentication and Security Layer; Basit Kimlik Doğrulama ve Güvenlik Katmanı) çerçevesini kullanır. Çeşitli SASL mekanizmaları vardır ve IBM MQ iki SASL mekanizmasını destekler: ANONYMOUS VE PLAYIN.

ANONYMOUS (anonim) durumunda, istemciden kimlik doğrulaması için kuyruk yöneticisine kimlik bilgileri iletilmedi. CONNAUTH özniteisinde belirtilen MQ AUTHINFO nesnesinin CHCKCLNT IN CHCKCLNT ya da REQDADM değeri (denetimci kullanıcı olarak bağlanılıyorsa) varsa, bağlantı reddedilir. CHCKCLNT değeri NONE ya da OPTIONAL (isteğe bağlı) ise, bağlantı kabul edilir.

PLAIN durumunda, istemciden kimlik doğrulaması için kullanıcı adı ve parola istemciden kuyruk yöneticisine geçirilir. CONNAUTH özniteisinde belirtilen MQ AUTHINFO nesnesinin bir CHCKCLNT değeri NONE ise, bağlantı reddedilir. CHCKCLNT değeri isteğe bağlı, gerekli ya da REQDADM (yönetici kullanıcı olarak bağlantı kuruluyorsa) ise, kullanıcı adı ve parola kuyruk yöneticisi tarafından denetlendi. Kuyruk yöneticisi, işletim sistemini (AUTHINFO nesnesi IDPWOS tipinde) ya da LDAP havuzundan (AUTHINFO nesnesi IDPWLDAP tipinde ise) denetler.

Aşağıdaki çizelge bu kimlik doğrulama davranışını özetlemektedir:

Çizelge 95. SASL mekanizmalarının ve bağlantı kimlik doğrulamasının özeti

SASL mekanizması	**İstemciden kuyruk yöneticisine kimlik bilgileri geçirildi mi?**	**CHKCLNT değeri**
anonim	Hayır	REQUIRD ya da REQDADM-bağlantı reddedildi NONE ya da OPTIONAL-connection kabul edildi

Çizelge 95. SASL mekanizmalarının ve bağlantı kimlik doğrulamasının özeti (devamı var)		
SASL mekanizması	**İstemciden kuyruk yöneticisine kimlik bilgileri geçirildi mi?**	**CHKCLNT değeri**
Düz	Evet, kullanıcı adı ve parola	REQUIRD, REQDADM ya da OPTIONAL-kullanıcı adı ve parola, kuyruk yöneticisi tarafından denetlendi. NONE-bağlantı reddedildi

Bir MQ Light istemcisi kullanıyorsanız, bağlandığınız AMQP adresinde (örneğin,) bunları ekleyerek kimlik bilgilerini belirtebilirsiniz:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

Bir kanalda MCAUSER ayarı

AMQP kanallarının bir MCAUSER özniteliği vardır; bu, kanala kurulan tüm bağlantıların yetkili olduğu IBM MQ kullanıcı kimliğini ayarlamak için kullanılır. Bu kanala AMQP istemcilerinden gelen tüm bağlantılar, yapılandırdığınız MCAUSER kimliğini kabul eder. Bu kullanıcı kimliği, farklı konu başlıklarına ilişkin ileti alışverişi için kullanılır.

Kuyruk yöneticilerine yönelik bağlantıları güvenli kılmak için kanal doğrulaması (CHLAUTH) kullanmanız önerilir. Kanal kimlik doğrulaması kullanıyorsanız, MCAUSER değerini ayrıcalıklı olmayan bir kullanıcıya yapılandırmamanız önerilir. Bu, bir kanala yönelik bağlantının CHLAUTH kuralı ile eşleşmemesi durumunda, bağlantı, kuyruk yöneticiyle ilgili herhangi bir ileti alışverişi gerçekleştirme yetkisine sahip değildir.

Not: Windows Windowsüzerinde, önce IBM MQ 9.1.1, MCAUSER kullanıcı kimliği ayarı yalnızca en çok 12 karakter uzunluğunda olan kullanıcı kimlikleri için desteklenir.

V 9.1.1 IBM MQ 9.1.1' tan 12 karakter sınırı kaldırılır.

SSL/TLS desteği

AMQP kanalları, kuyruk yöneticiniz için yapılandırılan anahtar havuzundan anahtarları kullanarak SSL/TLS şifrelemesini destekler. SSL/TLS şifrelemesi için AMQP kanal yapılandırma seçenekleri, diğer MQ kanalıyla aynı seçenekleri destekler; bir şifre belirtimi ve kuyruk yöneticisinin AMQP istemci bağlantılarından sertifika gerektirip gerektirmediğini belirleyebilirsiniz.

Kuyruk yöneticisinin FIPS özniteliklerini kullanarak, AMQP istemcilerinden gelen bağlantıları güvenli kılmak için kullanabileceğiniz SSL/TLS şifreleme takımlarını denetleyebilirsiniz.

Kuyruk yöneticisi için bir anahtar havuzu ayarlamaya ilişkin bilgi edinmek için UNIX, Linux ve Windows sistemlerinde SSL ya da TLS ile çalışmakonusuna bakın.

Bir AMQP istemci bağlantısı için SSL/TLS desteğinin nasıl yapılandırılacağı hakkında bilgi için bkz. AMQP kanallarının oluşturulması ve kullanılması.

Java Kimlik Doğrulaması ve Yetkilendirme Hizmeti (JAAS)

İsteğe bağlı olarak AMQP kanallarını bir JAAS oturum açma modüle yapılandırabilirsiniz; bu da, bir AMQP istemcisi tarafından sağlanan kullanıcı adını ve parolayı denetleyebilirler. Bkz. “Configuring JAAS for AMQP channels” sayfa 540.

İlgili görevler

AMQP istemci uygulamaları geliştirilmesi

ULW AMQP istemci devralma kısıtlaması

Varolan bir AMQP istemci bağlantısıyla aynı istemci tanıtıcısına sahip bir AMQP istemci bağlantısı yapılırsa, varsayılan olarak, var olan istemci bağlantısının bağlantısı kesilir. Ancak, istemci devralma davranışını kısıtlamak için kuyruk yöneticisini yapılandırabilirsiniz; böylece, devralma yalnızca belirli ölçütler karşılandığında mümkün olur.

Örneğin, varolan istemci bağlantısının kesilmesi, farklı ekipler tarafından geliştirilmekte olan AMQP uygulamaları varsa ve bunların aynı istemci tanıtıcısını kullanmaları durumunda, bu uygulamaların kullanılması uygun olmayabilir. Bu sorunu çözmek için, kullanılmakta olan AMQP kanalının adı, istemcinin IP adresi ve istemci kullanıcı kimliği (SASL kimlik doğrulaması etkinleştirildiğinde) dayalı olarak istemci devralma işlemini sınırlayabilirsiniz.

Use the settings of queue manager attributes **AdoptNewMCA** and **AdoptNewMCACheck** to specify the required level of client takeover restriction, as detailed in the following table:

*Çizelge 96. İstemci devralma işlemini kısıtlamak için **AdoptNewMCA** ve **AdoptNewMCACheck** ayarları*

AdoptNewMCA	**AdoptNewMCACheck**	**İstemci devralmaya izin verilmeden önce denetlenen ölçütler**
NO ya da tanımsız	Burada geçerli değil	Yok. Kimliği doğrulanan tüm istemci bağlantıları için istemci devralma işlemine izin verilir ve tüm CHLAUTH kurallarına geçerler.
ALL (ya da NO dışında bir değer)	QM veya tanımsız	Yok. Kimliği doğrulanan tüm istemci bağlantıları için istemci devralma işlemine izin verilir ve tüm CHLAUTH kurallarına geçerler.
ALL (ya da NO dışında bir değer)	AD	Kullanıcı kimliği (SASL etkin olduğunda) Kanal adı
ALL (ya da NO dışında bir değer)	ADRES	Kullanıcı kimliği (SASL etkin olduğunda) IP adresi
ALL (ya da NO dışında bir değer)	ALL	Kullanıcı kimliği (SASL etkin olduğunda) Kanal adı IP adresi

Kuyruk yöneticisi öznitelikleri **AdoptNewMCA** ve **AdoptNewMCACheck** , KANALLAR stanza içinde tanımlanan kuyruk yöneticisi yapılanışının bir parçasıdır. On IBM MQ for Windows and IBM MQ for Linux x86-64 systems, modify configuration information using the IBM MQ Explorer. On other systems, modify the information by editing the `qm.ini` configuration file. Kuyruk yöneticisi kanalları bilgilerini değiştirmeyle ilgili bilgi için Kanalların öznitelikleribaşlıklı konuya bakın.

İlgili görevler

AMQP istemci uygulamaları geliştirilmesi

AMQP kanallarının yaratılması ve kullanılması

ULW Configuring JAAS for AMQP channels

Java Authentication and Authorization Service (JAAS) özel modülleri, bir AMQP istemcisine bağlı bir AMQP kanalına aktarılan kullanıcı adı ve parola kimlik bilgilerini doğrulamak için kullanılır.

Bu görev hakkında

You might want to use a custom JAAS module if you already use JAAS modules for authentication in other Java-based systems, and want to reuse those modules for authenticating AMQP connections to MQ. Diğer bir seçenek olarak, MQ içine yerleşik kimlik doğrulama özellikleri, kullanmak istediğiniz kimlik doğrulama mekanizmasını desteklemiyorsa, özel bir JAAS modülü yazmak isteyebilirsiniz.

AMQP kanallarına ilişkin JAAS modüllerinin yapılandırılması, kuyruk yöneticisi düzeyinde yapılır. Bunun anlamı, kuyruk yöneticiyle AMQP bağlantılarını doğrulamak üzere bir JAAS birimi yapılandırırsanız, modül tüm AMQP kanallarına uygulanır. JAAS modülünü çağıran kanalın adı, farklı kanallara ilişkin davranışlarda farklı JAAS günlüğünü kodlamanıza olanak tanır.

Diğer bilgiler de JAAS modüllerinden de geçirilir:

- Kimlik doğrulamayı denemiş olan AMQP istemcisinin istemci tanıtıcısı.
- AMQP istemcisinin ağ adresi.
- JAAS modülünü çağıran kanalın adı.

Yordam

Aşağıdaki adımları tamamlayarak, AMQP kanalları için bir JAAS yapılandırma modülü yapılandırıyorsunuz:

1. Bir ya da daha çok JAAS modülü yapılandırma stanzası içeren bir `jaas.config` dosyası tanımlayın. Stanza, JAAS `javax.security.auth.spi.LoginModule` arabirimini gerçekleştiren Java sınıfının tam olarak nitelenmiş adını belirtmelidir.
   - Varsayılan bir `jaas.config` dosyası ürünle birlikte gönderilir ve *QM_data_directory*`/amqp/jaas.config`içinde bulunur.
   - A preconfigured stanza named `MQXRConfig` is already defined in the default `jaas.config` file.
2. AMQP kanalları için kullanılacak stanza adını belirtin.
   - UNIX `amqp_unix.properties` dosyasına bir özellik ekleyin.
   - Windows `amqp_win.properties` dosyasına bir özellik ekleyin.

   Özellik aşağıdaki formu içerir:

   ```
   com.ibm.mq.MQXR.JAASConfig=JAAS_stanza_name
   ```

   Örneğin:

   ```
   com.ibm.mq.MQXR.JAASConfig=MQXRConfig
   ```
3. Kuyruk yöneticisi ortamını, özel modülün sınıfını içerecek şekilde yapılandırın. AMQP hizmeti, JAAS yapılandırma stanzasında yapılandırılan Java sınıfına erişmiş olmalıdır.

   Bunu, yolu JAAS sınıfının yolunu MQ `service.env` dosyasına ekleyerek yapın. Edit the `service.env` file in the MQ configuration directory (*MQ_config_directory*) or the queue manager configuration directory (*QM_config_directory*) to set the CLASSPATH variable to the location of the JAAS module class.

Sonraki adım

Örnek JAAS oturum açma modülü, ürünle birlikte *mq_installation_directory*`/amqp/samples` dizininde gönderilir. Örnek JAAS oturum açma modülü, istemcinin bağlandığı kullanıcı adı ya da paroladan bağımsız olarak tüm istemci bağlantılarını doğrular.

Örneğin kaynak kodunu değiştirebilir ve yalnızca belirli bir parolaya sahip belirli kullanıcıları doğrulamaya çalışmak için yeniden derleyebilirsiniz. Bir UNIX sisteminde AMQP kanalını, ürünle birlikte gönderilen örnek JAAS oturum açma modülünü kullanmak üzere yapılandırmak için:

1. Edit the file `/var/mqm/qmgrs/QMNAME/amqp/amqp_unix.properties` and set the property `com.ibm.mq.MQXR.JAASConfig=MQXRConfig`.
2. Edit the file /var/mqm/service.env and set the property `CLASSPATH=`*`mq_installation_location`*`/amqp/samples`

`jaas.config` dosyası, oturum açma modülü sınıfı olarak `samples.JAASLoginModule` örnek sınıfını belirten `MQXRConfig` adlı bir stanza içerir. Örnek modülü denemeden önce `jaas.config` ' e herhangi bir değişiklik yapılması gerekmez.

İlgili görevler

AMQP istemci uygulamaları geliştirilmesi

AMQP kanallarının yaratılması ve kullanılması

Advanced Message Security

Advanced Message Security (AMS) is a component of IBM MQ that provides a high level of protection for sensitive data flowing through the IBM MQ network, while not impacting the end applications.

Advanced Message Security' a genel bakış

IBM MQ uygulamaları, genel anahtar şifrelemesi modeli kullanılarak farklı koruma düzeylerine sahip yüksek değerli finansal işlemler ve kişisel bilgiler gibi hassas verileri göndermek için Advanced Message Security ' i kullanabilir.

İlgili başvurular

AMS iletilerinde kullanılanGSKit dönüş kodları

Advanced Message Security' in özellikleri ve işlevleri

Advanced Message Security , ileti düzeyinde veri imzalama ve şifreleme sağlamak için IBM MQ güvenlik hizmetlerini genişletir. Genişletilmiş hizmetler, ileti verilerinin bir kuyruğa ilk olarak yerleştirildiğinde ve alındığında değiştirilmediğini garanti eder. Buna ek olarak, AMS , ileti verilerinin göndericisinin, imzalı iletileri bir hedef kuyruğa yerleştirmeye yetkili olduğunu doğrular.

AMS aşağıdaki işlevleri sağlar:

- IBM MQtarafından işlenen hassas ya da yüksek değerli işlemleri korur.
- Bir alma uygulaması tarafından işlenmeden önce, yanlış ya da yetkisiz iletileri saptar ve kaldırır.
- İletilerin kuyruktan kuyruğa taşıma sırasında değiştirilmediğini doğrular.
- Verileri, yalnızca ağ üzerinden akan gibi değil, aynı zamanda bir kuyruğa yerleştirildiği anda da korur.
- IBM MQiçin var olan özel ve müşteri tarafından yazılan uygulamaların güvenliğini sağlar.
- V 9.1.3 z/OS From IBM MQ 9.1.3, IBM MQ for z/OS provides the ability to optionally remove and add AMS protection from, or to, messages that flow across the network, respectively. Bu, *Server to Server Message Channel Agent (MCA) Interception.*olarak bilinir.
- ULW V 9.1.0.4 V 9.1.4 IBM MQ 9.1.4 ve IBM MQ 9.1.0 Fix Pack 4' den, müşterinin uygulama programı içinde çalışan IBM MQ kitaplık koduna bir denetim eklenmiştir. The check runs early in its initialization to read the value of the environment variable *AMQ_AMS_FIPS_OFF* and, if it is set to any value, then the GSKit code will be run in non-FIPS mode in that application.

AMSile sağlanan koruma nitelikleri

Advanced Message Security, `Integrity`, `Privacy`ve `Confidentiality`için üç koruma özelliği vardır.

`Integrity` protection is provided by digital signing, which provides assurance on who created the message, and that the message has not been altered or tampered with.

`Privacy` koruması, dijital imzalama ve şifreleme birleşimi tarafından sağlanır. Şifreleme, ileti verilerinin yalnızca amaçlanan alıcı ya da alıcılar için görüntülenebilmesini sağlar. Yetkisiz alıcılar, şifrelenmiş ileti verilerinin bir kopyasını edinse bile, gerçek ileti verilerinin kendisini görüntüleyemiyorlar.

`Confidentiality` koruması, şifreleme tarafından yalnızca isteğe bağlı anahtar yeniden kullanımla sağlanır.

Performans üzerinde etki

AMS , dijital imzalama ve şifreleme sağlamak için simetrik ve asimetrik şifreleme yordamlarından oluşan bir birleşim kullanır. Simetrik anahtar işlemleri, CPU yoğun olarak kullanılan asimetrik anahtar operasyonlarına kıyasla çok hızlı bir şekilde karşılaştırıldığında, bu durum, AMSile çok sayıda iletinin korunmasına ilişkin maliyetler üzerinde önemli bir etkiye sahip olabilir.

Asimetrik şifreleme yordamları
Örneğin, imzalı bir ileti yerleştirilirken, ileti hash değeri asimetrik bir anahtar işlemi kullanılarak imzalanır.

İmzalı bir ileti alınırken, imzalı HASH ' yi doğrulamak için daha fazla bir asimetrik anahtar işlemi kullanılır.

Bu nedenle, iletiyi imzalamak ve doğrulamak için ileti başına en az iki asimetrik anahtar işlemi gerekir.

Asimetrik ve simetrik şifreleme yordamları
Şifrelenmiş bir ileti yerleştirilirken, simetrik anahtar oluşturulur ve iletinin amaçlanan her alıcısı için asimetrik bir anahtar işlemi kullanılarak şifrelenir.

Daha sonra, ileti verileri simetrik anahtarla şifrelenir. Şifrelenmiş iletinin alınması istenen alıcının, ileti için kullanımında simetrik anahtarı keşfetmek için asimetrik bir anahtar işlemi kullanması gerekir.

Bu nedenle, üç koruma nitelikleri, CPU yoğun asimetrik anahtar operasyonlarının çeşitli öğelerini içerir. Bu işlem, iletiler yerleştirmek ve iletileri almak için ulaşılabilecek en yüksek ileti hızı üst sınırını önemli ölçüde etkiler.

Ancak`Confidentiality` ilkeleri, bir ileti dizisi üzerinde simetrik anahtar yeniden kullanım için izin verir. Simetrik anahtar yeniden kullanımı yoluyla `Confidentiality` ilkeleriyle önemli CPU maliyet tasarrufu yapılabilir. Bu işlem kipi, simetrik şifreleme anahtarını paylaşmak için PKCS#7 biçimini kullanmaya devam eder. Ancak, ileti başına asimetrik anahtar işlemlerini ortadan kaldıran bir dijital imza yoktur. Simetrik anahtarın, her alıcı için asimetrik anahtar işlemleriyle şifrelenmesi gerekir, ancak simetrik anahtar, isteğe bağlı olarak aynı alıcılara yazılmış birden çok ileti üzerinden yeniden kullanılabilir. İlkeye göre anahtar yeniden kullanıma izin veriliyorsa, yalnızca ilk ileti asimetrik anahtar işlemleri gerektirir. Sonraki iletilerin yalnızca simetrik anahtar işlemlerini kullanması gerekir.

Anahtar yeniden kullanımı

`Confidentiality` ilkeleri ile, aynı kuyruğa yerleştirilecek ve aynı alıcıya ya da alıcılara yönelik olarak istenen sayıda iletinin şifrelenmesinde yer alan maliyetleri önemli ölçüde azaltmak için simetrik anahtar yeniden kullanım yaklaşımını kullanabilirsiniz.

Örneğin, aynı alıcı kümesine 10 şifreli ileti yerleştirilirken, iletinin amaçlanan her alıcısı için bir asimetrik anahtar işlemi kullanılarak, bir simetrik anahtar oluşturulur ve sonra ilk ileti için şifrelenir.

İlke denetimli sınırlara dayalı olarak, şifrelenmiş simetrik anahtar, daha sonra, aynı alıcılara yönelik sonraki iletiler tarafından yeniden kullanılabilir. Şifrelenmiş iletiler alan bir uygulama aynı eniyilemeyi uygulayabilir; bu uygulama, bir simetrik anahtar değişmediğinde ve simetrik anahtarı alma masrafından kaçındığında bu uygulamanın algılayabileceği bir uygulamadır.

Bu örnekte, asimetrik anahtar operasyonlarının %90 'ı aynı anahtarı yeniden kullanarak hem koyma hem de uygulama alma işlemi tarafından önlenebilir.

Anahtarın yeniden kullanımını nasıl kullanabilmeye ilişkin ek bilgi için bkz:

- MQSC komutu SET POLICY
- Denetim komutu setmqspl

- IBM i IBM i komutu SETMQMSPL

AMSiçindeki temel kavramlar

Aracın nasıl çalıştığını ve nasıl etkili bir şekilde yönetileceğini anlamak için Advanced Message Security içindeki temel kavramlar hakkında bilgi edinin.

Genel anahtar altyapısı ve Advanced Message Security

Genel anahtar altyapısı (PKI), güvenli iletişimi sağlamak için ortak anahtar şifrelemesi kullanımını destekleyen tesisler, ilkeler ve hizmetlerden oluşan bir sistemdir.

Genel anahtar altyapısının bileşenlerini tanımlayan tek bir standart yoktur, ancak bir PKI genel olarak, genel anahtar sertifikalarının kullanımını içerir ve aşağıdaki hizmetleri sağlayan sertifika yetkililerinden (CA) ve diğer kayıt yetkililerine (RA) içerir:

- Dijital sertifikaların verilmesi
- Dijital sertifikaların geçerliliği denetleniyor
- Dijital sertifikaları iptal etme
- Sertifikaları dağıtma

Kullanıcıların ve uygulamaların kimliği, imzalı ya da şifrelenmiş iletilerle ilişkili bir sertifikadaki **ayırt edici ad (DN)** alanı tarafından temsil edilir. Advanced Message Security , bir kullanıcıyı ya da uygulamayı göstermek için bu kimliği kullanır. Bu kimliğin kimliğini doğrulamak için, kullanıcının ya da uygulamanın, sertifikenin ve ilişkili özel anahtarın saklandığı anahtar deposuna erişimi olmalıdır. Her sertifika, anahtar depoundaki bir etiketle temsil edilir.

İlgili kavramlar

“Anahtar depolarının ve sertifikaların kullanılması” sayfa 584
IBM MQ uygulamalarına şeffaf bir şifreleme koruması sağlamak için Advanced Message Security , anahtar deposu dosyasını, genel anahtar sertifikalarını ve bir özel anahtarın depolandığı anahtar deposu dosyasını kullanır. z/OSüzerinde, bir anahtar deposu dosyası yerine bir SAF anahtar halkası kullanılır.

Digital certificates in AMS

Advanced Message Security , kullanıcıları ve uygulamaları X.509 standart sayısal sertifikalarıyla ilişkilendirir. X.509 sertifikaları genellikle güvenilir bir sertifika yetkilisi (CA) tarafından imzalanır ve şifreleme ve şifre çözme için kullanılan özel ve genel anahtarlar içerir.

Dijital sertifikalar, sahibinin bir birey, bir kuyruk yöneticisi ya da başka bir varlık olup olmadığı, bir genel anahtarı sahibine bağlayarak, kimliğine bürünme konusunda koruma sağlar. Dijital sertifikalar genel anahtar sertifikaları olarak da bilinir, çünkü asimetrik anahtar şeması kullandığınızda bir genel anahtarın sahipliğine ilişkin güvence verir. Bu şema, bir uygulama için bir genel anahtar ve bir özel anahtarın oluşturulmasını gerektirir. Genel anahtarla şifrelenen verilerin şifresi yalnızca ilgili özel anahtar kullanılarak çözülüyor; özel anahtarla şifrelenen veriler yalnızca ilgili genel anahtar kullanılarak şifresi çözülüyor. Özel anahtar, parola korumalı bir anahtar veritabanı dosyasında depolanır. Yalnızca sahibinin, ilgili genel anahtar kullanılarak şifrelenen iletilerin şifresini çözmek için kullanılan özel anahtara erişmesi gerekir.

Genel anahtarlar doğrudan sahipleri tarafından başka bir varlığa gönderilirse, iletinin engellenmiş olması ve genel anahtarın başka bir varlığa geri koyması riski vardır. Bu "orta adam" saldırısı olarak bilinir. Çözüm, genel anahtarları güvenilir bir üçüncü kişi aracılığıyla değiş tokuş etmek, kullanıcıya ortak anahtarın, iletişim kurduğunuz varlığa ait olduğunu güçlü bir güvence sağlar. Genel anahtarınızı doğrudan göndermek yerine, güvenilir bir üçüncü kişinin bunu dijital bir sertifiya dahil etmesi için güvenilir bir üçüncü kişi soruyorsunuz. Sayısal sertifikalara sahip olan güvenilir üçüncü kişi sertifika yetkilisi (CA) olarak adlandırılır.

Dijital sertifikalar hakkında daha fazla bilgi için Dijital sertifikada neler varbaşlıklı konuya bakın.

Sayısal sertifika, bir varlığın genel anahtarını içerir ve genel anahtarın o varlığa ait olduğunu belirtir:

- Bir sertifika tek bir varlık için olduğunda, bu sertifika *kişisel sertifika* ya da *kullanıcı sertifikası*olarak adlandırılır.

- Sertifika bir sertifika yetkilisi için olduğunda, sertifikana *CA sertifikası* ya da *imzalayıcı sertifikası*adı verilir.

Not: Advanced Message Security , hem Java , hem de yerel uygulamalarda kendinden onaylı sertifikaları destekler.

İlgili kavramlar

"Kriptografi" sayfa 7
Şifreleme, *düz metin*adlı okunabilir metin ile *şifreli metin*adı verilen okunamayan bir form arasında dönüştürme işletidir.

Multi *Nesne yetkisi yöneticisi*

Multiplatforms, Object Authority Manager (OAM), IBM MQ ürünleriyle birlikte verilen yetki hizmeti bileşenidir.

Advanced Message Security ' a erişim, IBM MQ kullanıcı grupları ve OAM aracılığıyla denetlenir. Yöneticiler, yetkileri gerektiği şekilde vermek ya da iptal etmek için komut satırı arabirimini kullanabilir. Farklı kullanıcı grupları, aynı nesneler için farklı erişim yetkisine sahip olabilir. Örneğin, bir grup belirli bir kuyruk için hem PUT hem de GET işlemlerini gerçekleştirebilir, ancak başka bir gruba yalnızca kuyruğa göz atma izni verilebilir. Benzer şekilde, bazı gruplar bir kuyruğa GET ve PUT yetkisine sahip olabilir, ancak kuyruğun değiştirilmesine ya da silinmesine izin verilmiyor olabilir.

OAM sayesinde, kontrol edebilirsin.

- Message Queue Interface (MQI) aracılığıyla Advanced Message Security nesnelerine erişim. Bir uygulama programı nesnelere erişmeyi denediğinde, OAM, isteği yapan kullanıcı tanıtımının istenen işlemin yetkilendirmesine sahip olup olmadığını denetler. Bu, kuyruklar ve kuyruklar üzerindeki iletilerin yetkisiz erişimlerden korunabileceği anlamına gelir.
- PCF ve MQSC komutlarını kullanma izni.

İlgili kavramlar

Nesne yetkisi yöneticisi

Message Queue Interface-Genel Bakış

Advanced Message Securitytarafından desteklenen teknoloji

Advanced Message Security , güvenlik altyapısı sağlamak için birkaç teknoloji bileşenine bağlıdır.

Advanced Message Security , aşağıdaki IBM MQ uygulama programlama arabirimlerini (API ' ler) destekler:

- İleti kuyruğu arabirimi (MQI)
- IBM MQ Java Message Service (JMS) 1.0.2 ve 1.1.
- JavaiçinIBM MQ Temel Sınıfları
- Yönetilmeyen kipte ağ içinIBM MQ sınıfları

Not: Advanced Message Security , X.509 uyumlu sertifika yetkililerine destek sağlar.

Bilinen AMSsınırlamaları

There are a number of IBM MQ options that are either not supported, or have limitations for Advanced Message Security.

- Aşağıdaki IBM MQ seçenekleri desteklenmiyor ya da sınırlamalara sahip değil:

  Yayınla/abone ol

  Bir yayınlama/abone olma ileti sistemi modelinin noktadan noktaya iletişim için en önemli avantajlarından biri, gönderme ve alma uygulamalarının, verilerin gönderilmek ve alınmak üzere birbirleri hakkında hiçbir şey bilmemesine gerek kalmaması. Bu avantaj, amaçlanan alıcıları ya da yetkili imzacıları tanımlamalı olan Advanced Message Security ilkelerinin kullanılmasıyla olumsuzlanır. Bir uygulamanın, bir ilke tarafından korunan bir diğer ad kuyruğu tanımlaması aracılığıyla bir konuya yayınlanması mümkündür; ayrıca, abone olunan bir uygulamanın ilke korumalı

bir kuyruktan ileti alabileceği bir uygulama da mümkündür. Bir ilkenin doğrudan bir konu dizgisine atanması mümkün değildir, ilkeler yalnızca kuyruk tanımlamalarına atanabilir.

Kanal veri dönüştürme
Advanced Message Security korunan bir iletinin korunan bilgi yükü ikili biçim kullanılarak iletilir; bu, uygulamalar arasındaki bir kanalda veri dönüştürme işlemi ileti özetini geçersiz kılmamasını sağlar. İlke korumalı bir kuyruktan iletilerin alınması için veri dönüştürme isteğinde bulunulması gerekir; ancak, iletiler başarıyla doğrulandıktan ve korumasız olduktan sonra, korunan bilgi yükünün dönüştürülmesi girişiminde bulunulmuş olur.

Dağıtım listeleri
Advanced Message Security policies can be used when protecting applications putting messages to distribution lists, provided each destination queue in the list has an identical policy defined. Bir uygulama bir dağıtım listesi açtığında tutarsız ilkeler tanımlanırsa, açma işlemi başarısız olur ve uygulamaya bir güvenlik hatası döndürülür.

Uygulama iletisi bölümlemesi
İlke korumalı iletilerin boyutu artacaktır ve uygulamaların, bir iletinin bölüm sınırlarını doğru olarak belirlemesi olanaklı değildir.

Yönetilen kipteki IBM MQ classes for .NET kullanan uygulamalar (istemci bağlantıları)
Yönetilen kipteki (istemci bağlantıları) IBM MQ classes for .NET kullanan uygulamalar desteklenmez.

Not: MCA interception can be used to allow unsupported clients to use AMS.

Yönetilen kipteki .NET (XMS) uygulamaları için Message Service istemcisi
Yönetilen kipteki .NET (XMS) uygulamaları için Message Service istemcisi desteklenmez.

Not: MCA etkileşimi, desteklenmeyen istemcilerin AMS kullanmalarına izin vermek için kullanılabilir.

IMS köprüsü tarafından işlenenIBM MQ kuyrukları
IMS köprüsü tarafından işlenenIBM MQ kuyrukları desteklenmez.

Not: AMS , CICS köprü kuyruklarında desteklenir. CICS köprü kuyruklarında MQPUT (şifreleme) ve MQGET (şifre çözme) için aynı kullanıcı kimliğini kullanmalısınız.

Getter 'ı beklemeye al
Kendileri için tanımlanmış AMS ilkeleri olan kuyruklara karşı alıcı uygulamaları için, alıcı (getter) alıcısının bekleme işlemi desteklenmez.

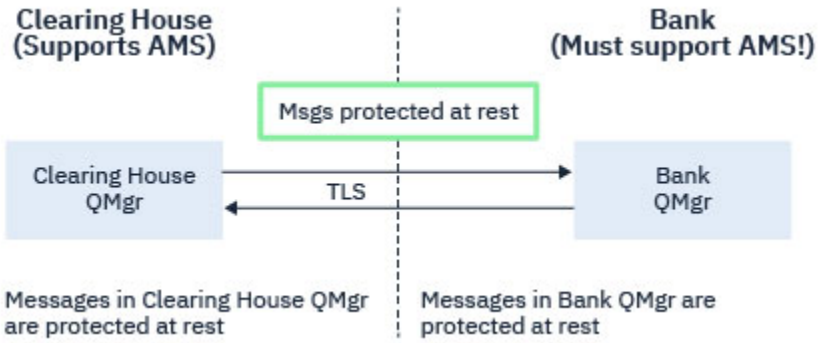
V 9.1.3 **Sunucu MCA ' nın başlangıcına sunucu**
IBM MQ 9.1.3'dan, IBM MQ for z/OS' da sunucu MCA ' yı sunucu arası sunucuya, yalnızca gönderen, sunucu, alıcı ve istekte bulunan kanal tipleri için desteklenmektedir.

- Kullanıcılar, bir iletiyi korurken kullanılacak sertifikenin seçimi tanımlanmadığı için, kullanıcılar tek bir anahtar deposu dosyasında aynı Ayırt Edici Ad ile birden fazla sertifika koymaktan kaçınmalıdır.
- **WMQ_PROVIDER_VERSION** özelliği 6 olarak ayarlandıysa,AMS , JMS içinde desteklenmez.
- AMS yakalayıcısı AMQP ya da MQTT kanalları için desteklenmiyor.

V 9.1.3 z/OS İleti kanallarında Advanced Message Security başlangıcındaki genel bakış

z/OSüzerinde, Advanced Message Security (AMS) başlangıç düzeyi, gönderene, sunucuya, alıcıya ve istekte bulunana kanallara bir güvenlik ilkesi koruması (SPLPROT) ek seçeneği ekleyerek var olan olanağı geliştirir.

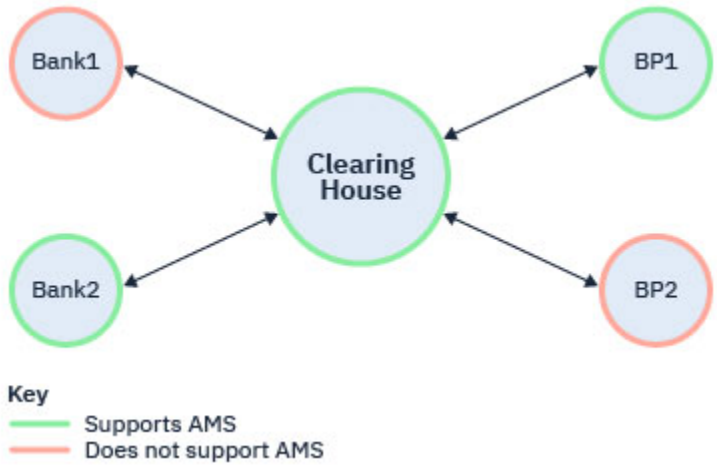
Currently, using the example of a clearing house communicating with a bank, both sides of the system need to support AMS, as shown in Şekil 1.



Şekil 32. AMS ' in geçerli kullanımı

A key benefit of the additional option is, that if your enterprise has AMS configured, and not all of your business partners support AMS, you can remove protection from outbound messages and protect inbound messages on channels to and from those business partners that do not support AMS.

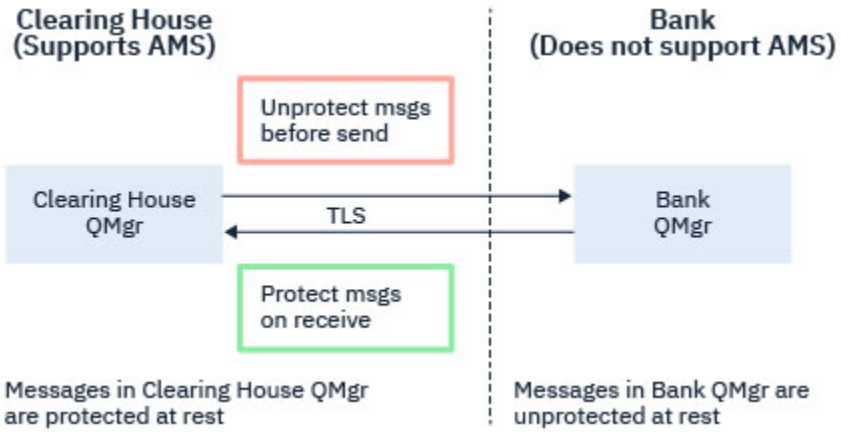
Bir temizleme evi ve banka örneğini kullanarak, bu senaryo Şekil 2'de gösterilir; burada, bazı kurumlarda AMS' in olduğu ve diğerlerinin olmadığı, temizleme eviyle, bankalarla ve çözüm ortaklarının arasında bir ileti akışı vardır.



Şekil 33. Bazı çözüm ortakları AMS ' yi destekler ve bazıları

Kanallar genellikle TLS ' dir (TLS) etkindir.

Ancak, bazı bankaların ve çözüm ortaklarının AMS' yi desteklemediği ve tüm bankalar ile iş ortakları arasında ileti alışverişi için bir gereksinim olduğu bir durum olabilir. Bu senaryo Şekil 3içinde gösterilmektedir



Şekil 34. İş ortakları arasındaki ileti akışı

İlgili görevler

Sunucudan sunucuya ileti kanalı arası ileti oluşturma örneği yapılandırmaları

V 9.1.3 z/OS *AMS interception on server-to-server message channels*

Server-to-server message channel interception provides a means to control if messages should have any applicable Advanced Message Security (AMS) policies applied to them, when sender type message channel agents get messages from transmission queues, and receiver type message channel agents put messages to target queues.

This allows AMS protection to be enabled on a queue manager when communicating, using server-to-server message channels of type sender, server, receiver, and requester, with a queue manager that does not have AMS enabled.

Yani, AMS etkin kuyruk yöneticilerinde AMS korumalı iletiler,AMS etkin olmayan kuyruk yöneticilerine gönderilmeden önce korumasız olabilir veAMS etkin olmayan kuyruk yöneticilerinden alınan korunmayan iletiler, uygulanabilir AMS ilkeleri tarafından, AMS etkin kuyruk yöneticilerine karşı korunabilir.

Sunucu-sunucu ileti kanalı arası iletişim başlangıcı yapılandırılıyor

Sunucuyla sunucu arası ileti kanalı etkileşimi, kanal tipi gönderen, sunucu, alıcı ya da istekte bulunan kanallarda SPLPROT öznitelikle yapılandırılır. Davranışı yapılandırmak için kullanılabilecek seçenekler, belirtilen kanal tipine bağımlıdır:

Passthru
Bu kanal için ileti kanalı aracısı tarafından gönderilen ya da alınan iletileri geçirin, değiştirmeden.

Bu değer, kanal tipi (**CHLTYPE**) SDR, SVR, RCVRya da RQSTRolan kanallar için geçerlidir ve varsayılan değerdir.

KALDIR
İleti kanalı aracısı tarafından iletim kuyruğundan alınan iletilerden AMS korumasını kaldırın ve iletileri iş ortağına gönderin.

İleti kanalı aracısı iletim kuyruğundan bir ileti aldığında, iletim kuyruğu için bir AMS ilkesi tanımlanmışsa, iletiyi kanal üzerinden göndermeden önce iletiden herhangi bir AMS korumasını kaldırmak için uygulanır. İletim kuyruğu için bir AMS ilkesi tanımlanmamışsa, ileti olduğu gibi gönderilir.

Bu değer yalnızca SDR ya da SVRkanal tipine sahip kanallar için geçerlidir.

ASPOLICY
Hedef kuyruk için tanımlanan ilkeye dayalı olarak, hedef kuyruğa yerleştirmeden önce gelen iletilere AMS korumasını uygulayın.

İleti kanalı aracısı bir gelen iletisi aldığında, hedef kuyruk için bir AMS ilkesi tanımlanmışsa, AMS hedef kuyruğa konan iletiden önce iletiye koruma uygulanır. Hedef kuyruk için bir AMS ilkesi tanımlanmamışsa, ileti hedef kuyruğa olduğu gibi yerleştirilir.

Bu değer yalnızca RCVR ya da RQSTRkanal tipine sahip kanallar için geçerlidir.

İleti kanalı ara başlangıcı için kullanıcı kimliği

Sunucuyla sunucu arası ileti kanalı arası olarak kullanılan kullanıcı kimliklerine ilişkin gereksinme, var olan AMS etkinleştirilmiş uygulamalar için olanla aynıdır. Çalışan bir kanal için, ileti gönderme kanalı aracısı iletim kuyruğundan ileti alır ve alan ileti kanalı aracısı iletileri hedef kuyruklara yerleştirir. Sunucu üzerinde sunucu kanallarına ayarlanmış olan Message Channel Agent kullanıcı kimliği (MCAUSER) alanı, hangi ileti kanalı aracılarının yerleştirdiği ve istek alacağı kullanıcı kimliğini tanımlar.

Sunucuyla sunucu arası ileti kanalı etkileşimi sırasında AMS işlevleri, diğer AMS etkin uygulamalarıyla olduğu gibi alma ve alma işlemleri sırasında gerçekleştirilir. Bu nedenle, ileti kanalı aracısı kullanıcı tanıtıcıları, AMS uygulama kullanıcı kimlikleri için aynı gereksinimlerin aynılarına sahiptir.

Put ve get işlemlerini gerçekleştirmek için kullanılan MCAUSER yapılandırılabilir ve bir giden ya da gelen kanal olup olmadığına bağlıdır. Seçilen kullanıcı kimliğinin ileti kanalı aracısında işlemleri nasıl gerçekleştireceği ile ilgili ayrıntılar için MCAUSER başlıklı konuya bakın. As such, the user ID that the channel initiator is running under is the user ID that is to be used for AMS functions performed during server-to-server message channel interception. Bu nedenle, bu kullanıcı kimlikleri, AMS uygulama kullanıcı kimlikleriyle aynı koşullara sahiptir.

Kimlik doğrulaması, PUTAUT yapılanışlarıyla kanallara ilişkin kanala ilişkin ayrıntılı kanal için varolan kurallar kullanılarak gerçekleştirilir. Ek bilgi için kanal başlatıcı tarafından kullanılan kullanıcı kimlikleri başlıklı konuya bakın.

Not: Sunucu ile sunucu arası ileti kanalı etkileşimi, PUTAUT kanal özniteliğinin değerini dikkate almamaktadır.

İleti boyutu ve MAXMSGL

AMS koruması nedeniyle, korunan iletilerin ileti büyüklüğü özgün ileti büyüklüğünden fazla olacaktır.

Korunan iletiler, korunmayan iletilerden daha büyük. Bu nedenle, korunan iletilerin büyüklüğünü göz altına almak için hem kuyruklarda hem de kanallarda **MAXMSGL** özniteliğinin değeri değiştirilmelidir.

İlgili başvurular

Sunucudan sunucuya ileti kanalı arası ileti oluşturma örneği yapılandırmaları

Hata işleme

IBM MQ Advanced Message Security , korumasız olamayan iletileri ya da hataları içeren iletileri yönetmek için bir hata işleme kuyruğu tanımlar.

Kusurlu iletiler, kural dışı durumlar olarak ele alındı. Alınan bir ileti, kuyruğa ilişkin güvenlik gereksinmelerini karşılamıyorsa, örneğin, ileti şifrelendiğinde imzalanırsa, şifre çözme ya da imza doğrulaması başarısız olursa, ileti hata işleme kuyruğuna gönderilir. Aşağıdaki nedenlerden dolayı hata işleme kuyruğunda bir ileti gönderilebilir:

- Koruma kalitesi uyuşmazlığı-alınan ileti ile güvenlik ilkesinde QOP tanımlaması arasında bir koruma kalitesi (QOP) uyuşmazlığı var.
- Şifre çözme hatası-iletinin şifresi çözülemez.
- PDMQ üstbilgi hatası- Advanced Message Security (AMS) ileti üstbilgisine erişilemiyor.
- Boyut uyuşmazlığı-şifre çözme beklenenden farklı bir iletinin uzunluğu.
- Şifreleme algoritması güç uyuşmazlığı-ileti şifreleme algoritması gerekenden daha zayıftır.
- Bilinmeyen hata-beklenmeyen bir hata oluştu.

AMS , SYSTEM.PROTECTION.ERROR.QUEUE , hata işleme kuyruğunda. IBM MQ AMS 'nin SYSTEM.PROTECTION.ERROR.QUEUE ' e koyduğu tüm iletilerin önünde bir MQDLH üstbilgisi vardır.

IBM MQ yöneticiniz SYSTEM.PROTECTION.ERROR.QUEUE başka bir kuyruğu işaret eden bir diğer ad olarak kuyruğa aldı.

V 9.1.3 z/OS IBM MQ 9.1.3'dan, IBM MQ for z/OS' da sunucu Message Channel Agent (MCA) iletişim başlangıcındaki sunucu oluşturma işlemi kullanılırsa:

- Daha önce belirtilen nedenlerin biri için IBM MQ AMS , iletileri iletim kuyruğundan hata işleme kuyruğuna taşırsa, gönderen MCA, iletim kuyruğunda bir sonraki kullanılabilir iletiyi işlemeye devam eder.
- Genel olarak, aşağıdaki kanal kuralları geçerli olur:
  - İletileri Ölü İleti Kuyruğu 'ya koyma ve
  - Ölü Mektup Kuyruğuna konması durumunda yapılacak işlemler başarısız olmalıdır.

Belirli senaryolarla ilgili ek bilgi için “Undelivered messages for AMS on z/OS” sayfa 549 ' e bakın.

V 9.1.3 z/OS *Undelivered messages for AMS on z/OS*

Specific scenarios related to server to server Message Channel Agent interception on IBM MQ for z/OS.

IBM MQ 9.1.3'dan, IBM MQ for z/OS' da sunucu Message Channel Agent (MCA) iletişim başlangıcındaki sunucu oluşturma işlemi kullanılırsa:

- Bir iletiyi aldıktan ve korumasız olduktan sonra, gönderen MCA bir nedenden ötürü bir ileti gönderememektedir; örneğin, ileti kanal için çok büyük olduğundan, USEDLQ gönderen kanal özniteliği YES değerine ayarlıysa, gönderen MCA iletiyi yerel ölü mektup kuyruğuna (DLQ) taşımaktadır.

  SYSTEM.DEAD.LETTER.QUEUE , yerel DLQ olarak kullanılıyor, ileti korunmasız olarak yerleştiriliyor.

  Not: IBM MQ AMS , sistem kuyruklarına gönderilen iletilerin korunmasını desteklemez.

  If a named DLQ is being used as the local DLQ, the message will be placed protected if you have defined an IBM MQ AMS policy with the same name as the named DLQ, and unprotected if you have not defined a suitable policy.
- Bir nedenden dolayı yerel DLQ ' ya bir ileti yerleştirilemiyorsa, kanalın NPMSPEED değeri NORMAL olarak ayarlandıysa ya da ileti kalıcı bir iletiyse, yürürlükteki ileti kümesi geriletilir ve kanal RETRY durumuna girilir. Tersi durumda, ileti atılır ve gönderen MCA, iletim kuyruğunda bir sonraki iletiyi işlemeye devam eder.
- Güvenlik ilkelerinin SYSTEM.DEAD.LETTER.QUEUEüzerinde herhangi bir etkisi yoksa ya da SYSTEM.DEAD.LETTER.QUEUE kullanımdaysa, “System queue protection in AMS” sayfa 618'ta listelenen diğer SYSTEM kuyrukları varsa, MCA' lar tarafından bu kuyruğa konan iletiler olduğu gibi yerleştirilir. Yani, iletiler önceden korunduysa, bunlar korunur; tersi durumda, korunmasız olarak yerleştirilir.

  Kuyruk yöneticisi DEADQ özniteliği alternatif (sistem dışı) bir ileti kuyruğu adı olarak ayarlandıysa ve aynı adı taşıyan bir AMS ilkesi yoksa, MCA ' lar tarafından bu kuyruğa konan iletiler olduğu gibi yerleştirilir. Yani, iletiler önceden korunduysa, bunlar korunur; tersi durumda, korunmasız olarak yerleştirilir.

  Kuyruk yöneticisi DEADQ özniteliği bir diğer (sistem dışı) bir ileti kuyruğu adı olarak ayarlandıysa ve DLQ ile aynı adı taşıyan bir AMS ilkesi varsa, bu ilke MCA ' lar tarafından kuyruğa gönderilen iletileri korumak için kullanılan ilke kullanılır. İleti önceden korunmuş ise, yeniden korunmaz; bu, çift korumayı önlemek için kullanılabilir. Aynı adı taşıyan bir AMS ilkesi yoksa, iletiler-olduğu gibi yerleştirilir.
- If there is a policy for the DLQ with the tolerate option in the setmqspl command set to off, that is '**-t** O', the put to the DLQ fails if the message is not AMS protected, and hence does not have a PDMQ header. Bu durum, ileti bir PDMQ üstbilgisi olmadan alıcıya vardığında oluşur. Bu, iletinin özgün biçiminin hedef için bir ilkesi olmadığından ve alıcının SPLPROT (ASPOLICY) ayarına sahip olmadığı için bu iletinin özgün biçiminin belirlenmemiş olması gerekir.
- DLQ için tanımlanan AMS ilkesi, iletiyi korumak için, kanal başlatıcısının çalışmakta olduğu kullanıcı kimliğine izin vermiyorsa, bir MCA iletisi DLQ ' ya bir ileti yerleştiremez.

- Alıcı kanalları genellikle teslim edilmemiş iletileri yerel DLQ 'ya yerleştirirken, gönderen kanalları genellikle bir nedenden dolayı işlenemeyen iletiler (örneğin, ileti kuyruğu için çok büyük ileti ya da hatalı MQXQH üstbilgisi ve yerel DLQ' ya) işlenemez.
- DLQ işleyicileri genel olarak yalnızca DLQ üstbilgisine (DLH) bakar ve ileti bilgi yükünün kendisini değil. Bu nedenle, ileti bilgi yükünün korunabileceği olgusu, iletinin DLQ ' ya neden yerleştirildiğini saptamayı engellememektedir.
- Bir DLQ tanımlanmadıysa, kanal:
  - Kalıcı bir ileti teslim edilemezse, olağandışı bir şekilde sona erer (ve yeniden denenmeye girer).
  - Kalıcı olmayan bir teslim edilmemiş iletiyi atar ve çalışmaya devam eder.

İlgili kavramlar

"Hata işleme" sayfa 548

IBM MQ Advanced Message Security , korumasız olamayan iletileri ya da hataları içeren iletileri yönetmek için bir hata işleme kuyruğu tanımlar.

Kullanıcı senaryoları

Advanced Message Securityile elde edebildiğiniz iş hedeflerini anlamak için olası senaryolar konusunda kendinizi tanıyın.

Windows *Quick Start Guide for AMS on Windows platforms*

Use this guide to quickly configure Advanced Message Security to provide message security on Windows platforms. Tamamladığınız zaman, kullanıcı kimliklerini doğrulamak ve kuyruk yöneticiniz için imzalama/şifreleme ilkeleri tanımlamanız için bir anahtar veritabanı yaratmış olucaksınız.

Başlamadan önce

Sisteminizde en az aşağıdaki özelliklere sahip olmamanız gerekir:

- Sunucu
- Development Toolkit (Örnek programlar için)
- Gelişmiş İleti Güvenliği

Ayrıntılar için Windows sistemleri içinIBM MQ özellikleri başlıklı konuya bakın.

Uygun IBM MQ komutlarının işletim sistemi tarafından konumlandırılması ve yürütülmesi için yürürlükteki ortamı kullanıma hazırlamak üzere **setmqenv** komutunun kullanılmasıyla ilgili bilgi edinmek için bkz. setmqenv (set IBM MQ Environment).

1. Kuyruk yöneticisi ve kuyruk yaratılması

Bu görev hakkında

Aşağıdaki örneklerin tümü, uygulamalar arasında ileti geçirmesi için TEST.Q adlı bir kuyruk kullanır. Advanced Message Security , iletileri standart IBM MQ arabirimi aracılığıyla IBM MQ altyapısına girdikleri noktada imzalamak ve şifrelemek için kesicileri kullanır. Temel kurulum IBM MQ içinde yapılır ve aşağıdaki adımlarda yapılandırılır.

You can use IBM MQ Explorer to create the queue manager QM_VERIFY_AMS and its local queue called TEST.Q by using all the default wizard settings, or you can use the commands found in `C:\Program Files\IBM\MQ\bin`. Aşağıdaki yönetim komutlarını çalıştırmak için `mqm` kullanıcı grubunun bir üyesi olmanız gerektiğini unutmayın.

Yordam

1. Kuyruk yöneticisi yarat

```
crtmqm QM_VERIFY_AMS
```

2. Kuyruk yöneticisini başlatma

```
strmqm QM_VERIFY_AMS
```

3. Create a queue called TEST.Q by entering the following command into **runmqsc** for queue manager QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Sonuçlar

Yordam tamamlandıysa, **runmqsc** içine girilen komut TEST.Qile ilgili ayrıntıları görüntüler:

```
DISPLAY Q(TEST.Q)
```

2. Kullanıcıların yaratılması ve yetkilendirilmesi

Bu görev hakkında

Bu örnekte görünen iki kullanıcı vardır: `alice`, gönderen ve bob, alıcı. Uygulama kuyruğunu kullanmak için, bu kullanıcıların kullanabilmeleri için yetki verilmesi gerekir. Ayrıca, bu kullanıcılara tanımlayacağımız koruma ilkelerini başarıyla kullanmak için bazı sistem kuyruklarına erişim izni verilmelidir. **setmqaut** komutuna ilişkin ek bilgi edinmek için **setmqaut**belgesine bakın.

Yordam

1. İki kullanıcıyı oluşturun ve HOMEPATH ve HOMEDRIVE ' in bu kullanıcılar için ayarlandığından emin olun.
2. Kullanıcıların kuyruk yöneticisine bağlanmasını ve kuyrukla çalışabilmeleri için yetki verir

```
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. Ayrıca, iki kullanıcının sistem ilke kuyruğuna göz atmasına ve iletileri hata kuyruğuna koymalarına izin vermelisiniz.

```
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
```

Uyarı: IBM MQ , ilkeleri önbelleğe alarak başarımı en iyi duruma getirir; böylece, SYSTEM.PROTECTION.POLICY.QUEUE (tüm durumlarda kuyruk).

IBM MQ , var olan tüm ilkeleri önbelleğe almaz. Çok sayıda ilke varsa, IBM MQ sınırlı sayıda ilkeyi önbelleğe alır. So, if the queue manager has a low number of policies defined, there is no need to provide the browse option to the SYSTEM.PROTECTION.POLICY.QUEUE.

Ancak, çok sayıda ilke tanımlanmış olması durumunda ya da eski istemciler kullanıyorsanız, bu kuyruğa göz atma yetkisi vermelisiniz. SYSTEM.PROTECTION.ERROR.QUEUE , AMS kodu tarafından oluşturulan hata iletilerini koymak için kullanılır. Bu kuyruğa ilişkin koyma yetkisi yalnızca, kuyruğa bir hata iletisi koyma girişiminde bulunduğunuzda denetlenir. Bir AMS korumalı kuyruğundan ileti koyma ya da alma girişiminde bulunduğunuzda, kuyruğa koyma yetkiniz denetlenmez.

Sonuçlar

Artık kullanıcılar oluşturulur ve bu kullanıcılara gerekli yetkiler verilir.

Sonraki adım

To verify if the steps were carried out correctly, use the `amqsput` and `amqsget` samples as described in section “7. Kurulumu test etme” sayfa 555.

3. Anahtar veritabanı ve sertifikalar yaratılması

Bu görev hakkında

Dinleyici, iletiyi şifrelemek için gönderen kullanıcıların genel anahtarının olmasını gerektirir. Bu nedenle, genel ve özel anahtarlarla eşlenen kullanıcı kimliklerinin anahtar veritabanı yaratılmalıdır. Kullanıcıların ve uygulamaların birden çok bilgisayar üzerinden dağıldığı gerçek sistemde, her kullanıcının kendi özel anahtar deposu olabilir. Benzer şekilde, bu kılavuzda, `alice` ve bob için temel veritabanları oluşturuyoruz ve kullanıcı sertifikalarını bu kullanıcılar arasında paylaşıyoruz.

Not: Bu kılavuzda, yerel bağ tanımlarını kullanarak C bağlantısında yazılmış örnek uygulamaları kullanırız. İstemci bağ tanımlarını kullanarak Java uygulamalarını kullanmayı planlıyorsanız, JRE 'nin bir parçası olan **keytool** komutunu kullanarak bir JKS anahtar deposu ve sertifikalar yaratmanız gerekir (ek ayrıntılar için “Quick Start Guide for AMS with Java clients” sayfa 572 ' a bakın). Diğer tüm diller için ve yerel bağ tanımlarını kullanan Java uygulamaları için bu kılavuzdaki adımlar doğrudur.

Yordam

1. Use the IBM Key Management GUI (`strmqikm.exe`) to create a new key database for the user `alice`.

   ```
   Type:       CMS
   Filename:   alicekey.kdb
   Location:   C:/Documents and Settings/alice/AMS
   ```

   Not:

   - Veritabanını güvenli kılmak için güçlü bir parola kullanmanız önerilir.
   - **Sstash password to a file** (Dosyaya ilişkin parola) onay kutusunun seçili olduğundan emin olun.
2. Anahtar veritabanı içeriği görünümünü **Kişisel Sertifikalar**olarak değiştirin.
3. **Yeni Otomatik İmzalama** seçeneğini belirleyin. otomatik olarak imzalanmış sertifikalar bu senaryoda kullanılır.
4. Create a certificate identifying the user `alice` for use in encryption, using these fields:

   ```
   Key label: Alice_Cert
   Common Name: alice
   Organisation: IBM
   Country: GB
   ```

   Not:

   - Bu kılavuzun amacı için, Sertifika Yetkilisi (Certificate Authority) kullanılmadan yaratılabilecek kendinden onaylı sertifika kullanırız. Üretim sistemleri için, kendinden imzalı sertifikaların kullanılmaması önerilir, ancak bunun yerine bir Sertifika Yetkilisi tarafından imzalanan sertifikalara güvenilebilir.
   - **`Key label`** parametresi, sertifikaların gerekli bilgileri almak için arayacağı sertifikana ilişkin adı belirtir.
   - **`Common Name`** ve isteğe bağlı parametreler, her kullanıcı için benzersiz olması gereken **Ayırt Edici Ad** ' ın (DN) ayrıntılarını belirtir.
5. Repeat step 1-4 for the user bob

Sonuçlar

The two users `alice` and bob each now have a self-signed certificate.

4. keystore.confOluşturulması

Bu görev hakkında

Advanced Message Security izlemelerini anahtar veritabanlarının ve sertifikaların located.This olduğu dizine, bu bilgilerin düz metin biçiminde tutan `keystore.conf` dosyası aracılığıyla gerçekleştirilmesini işaretlemelisiniz. Her kullanıcının, `.mqs` klasöründe ayrı bir `keystore.conf` dosyası olması gerekir. Bu adımın hem `alice` hem de bobiçin yapılması gerekir.

`keystore.conf` ile ilgili içerik şu biçimde olmalıdır:

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

Örnek

Bu senaryoda, `keystore.conf` içeriği aşağıdaki gibi olur:

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

Not:

- Anahtar deposu dosyasının yolu, dosya uzantısı olmadan sağlanmalıdır.
- Sertifika etiketi boşluk, böylece "Alice_Cert" ve "Alice_Cert" olabilir. (örneğin, bir boşlukla), iki farklı sertifikana ilişkin etiket olarak tanınır. Bununla birlikte, karışıklığı önlemek için etiketin adlarında boşluk kullanılmaması daha iyi olur.
- Şu anahtar deposu biçimleri vardır: CMS (Şifreleme İletisi Sözdizimi), JKS (Java Anahtar Deposu) ve JCEKS (Java Şifreleme Uzantısı Anahtar Deposu). Daha fazla bilgi için bkz. “AMS için anahtar deposu yapılandırma dosyasının (keystore.conf) yapısı” sayfa 585.
- *%HOMEDRIVE%\%HOMEPATH%*\`.mqs\keystore.conf` (örn. C:\Documents and Settings\alice\.mqs\keystore.conf), Advanced Message Security dosyasının `keystore.conf` dosyasını aradığı varsayılan konumdur. `keystore.conf`için varsayılan olmayan bir konumu nasıl kullanabilmeye ilişkin bilgi için bkz. “Anahtar depolarının ve sertifikaların kullanılması” sayfa 584.
- `.mqs` dizini oluşturmak için komut istemini kullanmanız gerekir.

5. Sertifikaları Paylaşma

Bu görev hakkında

Her bir kullanıcının diğerini başarıyla tanıması için, iki anahtar veritabanı arasındaki sertifikaları paylaşın. Bu işlem, her kullanıcının genel sertifikasının bir dosyaya çıkarılarak gerçekleştirilir; daha sonra, diğer kullanıcının anahtar veritabanına eklenir.

Not: *dışa aktarma* seçeneğini kullanmak için dikkatli olun ve *alma* seçeneğini kullanmayın. *Alma* , kullanıcının genel anahtarını alır, *dışa aktar* hem genel hem de özel anahtarı alır. Using *dışa aktarma* by mistake would completely compromise your application, by passing on its private key.

Yordam

1. Extract the certificate identifying `alice` to an external file:

   ```
   runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
   -label Alice_Cert -target alice_public.arm
   ```

2. Sertifikayı bob ' s anahtar deposuna ekleyin:

```
runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
Alice_Cert -file alice_public.arm
```

3. bobiçin yineleme adımları:

```
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
```

Sonuçlar

The two users `alice` and bob are now able to successfully identify each other having created and shared self-signed certificates.

Sonraki adım

Bir sertifikana, GUI ' yi kullanarak göz atarak ya da ayrıntılarını yazdırarak aşağıdaki komutları çalıştırarak anahtar deposunda olduğunu doğrulayın:

```
runmqakm -cert -details -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
Alice_Cert
```

```
runmqakm -cert -details -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Bob_Cert
```

6. Kuyruk ilkesinin tanımlanması

Bu görev hakkında

İleti önleme ve şifreleme anahtarlarına erişim için hazırlanan kuyruk yöneticisi tarafından oluşturulan ve algılayıcılar sayesinde, `setmqspl` komutunu kullanarak `QM_VERIFY_AMS` üzerinde koruma ilkeleri tanımlamaya başlayabiliriz. Bu komutla ilgili ek bilgi için setmqspl belgesine bakın. Her ilke adının, uygulanacak kuyruk adıyla aynı olması gerekir.

Örnek

Bu, `TEST.Q` kuyruğu için tanımlanmış bir ilkeye örnektir. Örnekte, iletiler SHA1 algoritmasıyla imzalanır ve AES256 algoritmasıyla şifrelenir. `alice` , geçerli tek gönderenidir ve bob bu kuyruktaki iletilerin tek nesnesidir:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Not: Ayırt edici adlar (DN), ilgili kullanıcının sertifikasında anahtar veri tabanından tam olarak belirtilenler ile eşleşir.

Sonraki adım

Tanımladığınız ilkeyi doğrulamak için şu komutu verin:

```
dspmqspl -m QM_VERIFY_AMS
```

İlke ayrıntılarını `setmqspl` komutları kümesi olarak yazdırmak için `-export` işaretini kullanın. Bu, önceden tanımlanmış ilkelerin saklanmasına izin verir:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Kurulumu test etme

Bu görev hakkında

Farklı kullanıcıların altında farklı programlar çalıştırarak, uygulamanın doğru yapılandırılıp yapılandırıldığını doğrulayabilirsiniz.

Yordam

1. Kullanıcıyı kullanıcı `alice`olarak çalışacak şekilde değiştir

   `cmd.exe` nesnesini farenin sağ düğmesiyle tıklatın ve **Bu şekilde çalıştır ...**seçeneğini belirleyin. İstendiğinde, kullanıcı `alice`olarak oturum açın.
2. As the user `alice` put a message using a sample application:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
3. İletinin metnini yazın ve Enter tuşuna basın.
4. Kullanıcıyı kullanıcı bobolarak çalışacak şekilde değiştir

   `cmd.exe` seçeneğini farenin sağ düğmesiyle tıklatıp **Bu şekilde çalıştır ...**seçeneğini belirleyerek başka bir pencere açın. İstendiğinde, kullanıcı bobolarak oturum açın.
5. As the user bob get a message using a sample application:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Sonuçlar

Uygulama her iki kullanıcı için de düzgün bir şekilde yapılandırıldıysa, bob uygulaması alma işlemi çalıştırıldığında kullanıcı `alice` ' un iletisi görüntülenir.

8. Şifreleme sınaması

Bu görev hakkında

To verify that the encryption is occurring as expected, create an alias queue which references the original queue `TEST.Q`. Bu diğer ad kuyruğunda güvenlik ilkesi yoktur; bu nedenle, kullanıcının iletinin şifresini çözmek için gereken bilgilere sahip olmayacak ve bu nedenle şifrelenmiş veriler gösterilecektir.

Yordam

1. Kuyruk yöneticisi QM_VERIFY_AMS için **runmqsc** komutunu kullanarak bir diğer ad kuyruğu yaratın.

   ```
   DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
   ```
2. Diğer ad kuyruğundan göz atmak için bob erişimi ver

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
   ```
3. As the user `alice`, put another message using a sample application just as before:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
4. As the user bob, browse the message using a sample application via the alias queue this time:

   ```
   amqsbcg TEST.ALIAS QM_VERIFY_AMS
   ```
5. As the user bob, get the message using a sample application from the local queue:

```
amqsget TEST.Q QM_VERIFY_AMS
```

Sonuçlar

The output from the `amqsbcg` application shows the encrypted data that is on the queue proving that the message has been encrypted.

UNIX *Quick Start Guide for AMS on UNIX*

Use this guide to quickly configure Advanced Message Security to provide message security on UNIX. Tamamladığınız zaman, kullanıcı kimliklerini doğrulamak ve kuyruk yöneticiniz için imzalama/şifreleme ilkeleri tanımlamanız için bir anahtar veritabanı yaratmış olucaksınız.

Başlamadan önce

Sisteminizde en az aşağıdaki bileşenlerin kurulu olması gerekir:

- Yürütme Ortamı
- Sunucu
- Örnek programlar
- IBM Global Security Kit
- Advanced Message Security

Her bir altyapıda bileşen adları için aşağıdaki konulara bakın:

- Linux Linux sistemleri içinIBM MQ bileşenleri
- AIX AIX sistemleri içinIBM MQ bileşenleri
- Solaris Solaris sistemleri içinIBM MQ bileşenleri

1. Kuyruk yöneticisi ve kuyruk yaratılması

Bu görev hakkında

Aşağıdaki örneklerin tümü, uygulamalar arasında ileti geçirmesi için `TEST.Q` adlı bir kuyruk kullanır. Advanced Message Security , iletileri standart IBM MQ arabirimi aracılığıyla IBM MQ altyapısına girdikleri noktada imzalamak ve şifrelemek için kesicileri kullanır. Temel kurulum IBM MQ içinde yapılır ve aşağıdaki adımlarda yapılandırılır.

You can use IBM MQ Explorer to create the queue manager QM_VERIFY_AMS and its local queue called `TEST.Q` by using all the default wizard settings, or you can use the commands found in *MQ_INSTALLATION_PATH*`/bin`. Aşağıdaki yönetim komutlarını çalıştırmak için `mqm` kullanıcı grubunun bir üyesi olmanız gerektiğini unutmayın.

Yordam

1. Kuyruk yöneticisi yarat

```
crtmqm QM_VERIFY_AMS
```

2. Kuyruk yöneticisini başlatma

```
strmqm QM_VERIFY_AMS
```

3. Create a queue called `TEST.Q` by entering the following command into **runmqsc** for queue manager QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Sonuçlar

Yordam başarıyla tamamlandıysa, **runmqsc** içine girilen şu komut, TEST.Q ile ilgili ayrıntıları görüntüler:

```
DISPLAY Q(TEST.Q)
```

2. Kullanıcıların yaratılması ve yetkilendirilmesi

Bu görev hakkında

Bu örnekte görünen iki kullanıcı vardır: `alice`, gönderen ve bob, alıcı. Uygulama kuyruğunu kullanmak için, bu kullanıcıların kullanabilmeleri için yetki verilmesi gerekir. Ayrıca, bu kullanıcılara tanımlayacağımız koruma ilkelerini başarıyla kullanmak için bazı sistem kuyruklarına erişim izni verilmelidir. **setmqaut** komutuna ilişkin ek bilgi edinmek için **setmqaut**belgesine bakın.

Yordam

1. İki kullanıcıyı yarat

```
useradd alice
useradd bob
```

2. Kullanıcıların kuyruk yöneticisine bağlanmasını ve kuyrukla çalışabilmeleri için yetki verir

```
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. Ayrıca, iki kullanıcının sistem ilke kuyruğuna göz atmasına ve iletileri hata kuyruğuna koymalarına izin vermelisiniz.

```
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
```

Uyarı: IBM MQ , ilkeleri önbelleğe alarak başarımı en iyi duruma getirir; böylece, SYSTEM.PROTECTION.POLICY.QUEUE (tüm durumlarda kuyruk).

IBM MQ , var olan tüm ilkeleri önbelleğe almaz. Çok sayıda ilke varsa, IBM MQ sınırlı sayıda ilkeyi önbelleğe alır. So, if the queue manager has a low number of policies defined, there is no need to provide the browse option to the SYSTEM.PROTECTION.POLICY.QUEUE.

Ancak, çok sayıda ilke tanımlanmış olması durumunda ya da eski istemciler kullanıyorsanız, bu kuyruğa göz atma yetkisi vermelisiniz. SYSTEM.PROTECTION.ERROR.QUEUE , AMS kodu tarafından oluşturulan hata iletilerini koymak için kullanılır. Bu kuyruğa ilişkin koyma yetkisi yalnızca, kuyruğa bir hata iletisi koyma girişiminde bulunduğunuzda denetlenir. Bir AMS korumalı kuyruğundan ileti koyma ya da alma girişiminde bulunduğunuzda, kuyruğa koyma yetkiniz denetlenmez.

Sonuçlar

Artık kullanıcı grupları oluşturulur ve gerekli yetkiler kendilerine verilir. Bu şekilde, bu gruplara atanan kullanıcıların kuyruk yöneticisine bağlanma ve kuyruktan alma ve alma iznine de sahip olur.

Sonraki adım

To verify if the steps were carried out correctly, use the `amqsput` and `amqsget` samples as described in section “8. Şifreleme sınaması” sayfa 561.

3. Anahtar veritabanı ve sertifikalar yaratılması

Bu görev hakkında

İletiyi şifrelemek için, engelleyici gönderen kullanıcının özel anahtarını ve alıcıların genel anahtar (lar) ını gerektirir. Bu nedenle, genel ve özel anahtarlarla eşlenen kullanıcı kimliklerinin anahtar veritabanı yaratılmalıdır. Kullanıcıların ve uygulamaların birden çok bilgisayar üzerinden dağıldığı gerçek sistemde, her kullanıcının kendi özel anahtar deposu olabilir. Benzer şekilde, bu kılavuzda, `alice` ve bob için temel veritabanları oluşturuyoruz ve kullanıcı sertifikalarını bu kullanıcılar arasında paylaşıyoruz.

Not: Bu kılavuzda, yerel bağ tanımlarını kullanarak C bağlantısında yazılmış örnek uygulamaları kullanırız. İstemci bağ tanımlarını kullanarak Java uygulamalarını kullanmayı planlıyorsanız, JRE 'nin bir parçası olan **`keytool`** komutunu kullanarak bir JKS anahtar deposu ve sertifikalar yaratmanız gerekir (ek ayrıntılar için “Quick Start Guide for AMS with Java clients” sayfa 572 ' a bakın). Diğer tüm diller için ve yerel bağ tanımlarını kullanan Java uygulamaları için bu kılavuzdaki adımlar doğrudur.

Yordam

1. Create a new key database for the user `alice`

   ```
   mkdir /home/alice/.mqs -p
   runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
   ```

   Not:

   - Veritabanını güvenli kılmak için güçlü bir parola kullanmanız önerilir.
   - The **`stash`** parameter stores the password into the `key.sth` file, which interceptors can use to open the database.
2. Anahtar veritabanının okunabilir olduğundan emin olun

   ```
   chmod +r /home/alice/.mqs/alicekey.kdb
   ```
3. Create a certificate identifying the user `alice` for use in encryption

   ```
   runmqakm -cert -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd
   -label Alice_Cert -dn "cn=alice,O=IBM,c=GB" -default_cert yes
   ```

   Not:

   - Bu kılavuzun amacı için, Sertifika Yetkilisi (Certificate Authority) kullanılmadan yaratılabilecek kendinden onaylı sertifika kullanırız. Üretim sistemleri için, kendinden imzalı sertifikaların kullanılmaması önerilir, ancak bunun yerine bir Sertifika Yetkilisi tarafından imzalanan sertifikalara güvenilebilir.
   - **`label`** parametresi, sertifikaların gerekli bilgileri almak için arayacağı sertifikana ilişkin adı belirtir.
   - **DN** parametresi, her kullanıcı için benzersiz olması gereken **Belirleyici Ad** (DN) ile ilgili ayrıntıları belirtir.
4. Şimdi anahtar veritabanını oluşturduk, bu veritabanını sahipliğini ayarlamamız ve diğer tüm kullanıcıların okuyamadığından emin olmalıyız.

   ```
   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. Repeat step 1-4 for the user bob

Sonuçlar

The two users `alice` and bob each now have a self-signed certificate.

4. keystore.confOluşturulması

Bu görev hakkında

Advanced Message Security algılayıcılarını, anahtar veritabanlarının ve sertifikaların bulunduğu dizine göstermelisiniz. Bu, bilgilerin düz metin biçiminde bulunan `keystore.conf` dosyası aracılığıyla gerçekleştirilir. Her kullanıcının, `.mqs` klasöründe ayrı bir `keystore.conf` dosyası olması gerekir. Bu adımın hem `alice` hem de `bob`için yapılması gerekir.

`keystore.conf` ile ilgili içerik şu biçimde olmalıdır:

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

Örnek

Bu senaryoda, `keystore.conf` içeriği aşağıdaki gibi olur:

```
cms.keystore = /home/alice/.mqs/alicekey
cms.certificate = Alice_Cert
```

Not:

- Anahtar deposu dosyasının yolu, dosya uzantısı olmadan sağlanmalıdır.
- Şu anahtar deposu biçimleri vardır: `CMS` (Şifreleme İletisi Sözdizimi), `JKS` (Java Anahtar Deposu) ve `JCEKS` (Java Şifreleme Uzantısı Anahtar Deposu). Daha fazla bilgi için bkz. “AMS için anahtar deposu yapılandırma dosyasının (keystore.conf) yapısı” sayfa 585.
- `HOME/.mqs/keystore.conf` varsayılan konumdur; burada Advanced Message Security , `keystore.conf` dosyasını arar. `keystore.conf`için varsayılan olmayan bir konumu nasıl kullanabilmeye ilişkin bilgi için bkz. “Anahtar depolarının ve sertifikaların kullanılması” sayfa 584.

5. Sertifikaları Paylaşma

Bu görev hakkında

Her bir kullanıcının diğerini başarıyla tanıması için, iki anahtar veritabanı arasındaki sertifikaları paylaşın. Bu işlem, her kullanıcının genel sertifikasının bir dosyaya çıkarılarak gerçekleştirilir; daha sonra, diğer kullanıcının anahtar veritabanına eklenir.

Not: *dışa aktarma* seçeneğini kullanmak için dikkatli olun ve *alma* seçeneğini kullanmayın. *Alma* , kullanıcının genel anahtarını alır, *dışa aktar* hem genel hem de özel anahtarı alır. Using *dışa aktarma* by mistake would completely compromise your application, by passing on its private key.

Yordam

1. Extract the certificate identifying `alice` to an external file:

   ```
   runmqakm -cert -extract -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Alice_Cert
   -target alice_public.arm
   ```

2. Sertifikayı bob ' s anahtar deposuna ekleyin:

   ```
   runmqakm -cert -add -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert -file
   alice_public.arm
   ```

3. bobiçin adımı yineleyin:

   ```
   runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
   bob_public.arm
   ```

4. Add the certificate for bob to `alice`'s keystore:

```
runmqakm -cert -add -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert -file
bob_public.arm
```

Sonuçlar

The two users `alice` and bob are now able to successfully identify each other having created and shared self-signed certificates.

Sonraki adım

Bir sertifikanda, ayrıntılarını yazan şu komutları çalıştırarak anahtar deposunda bulunduğunu doğrulayın:

```
runmqakm -cert -details -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert
runmqakm -cert -details -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert
```

6. Kuyruk ilkesinin tanımlanması

Bu görev hakkında

İleti önleme ve şifreleme anahtarlarına erişim için hazırlanan kuyruk yöneticisi tarafından oluşturulan ve algılayıcılar sayesinde, `setmqspl` komutunu kullanarak `QM_VERIFY_AMS` üzerinde koruma ilkeleri tanımlamaya başlayabiliriz. Bu komutla ilgili ek bilgi için setmqspl belgesine bakın. Her ilke adının, uygulanacak kuyruk adıyla aynı olması gerekir.

Örnek

Bu, `TEST.Q` kuyruğu için tanımlanmış bir ilkeye örnektir. Bu örnekte, iletiler kullanıcı `alice` tarafından SHA1 algoritması kullanılarak imzalanır ve 256 bit AES algoritması kullanılarak şifrelenir. `alice` , geçerli tek gönderenidir ve bob bu kuyruktaki iletilerin tek nesnesidir:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Not: Ayırt edici adlar (DN), ilgili kullanıcının sertifikasında anahtar veri tabanından tam olarak belirtilenler ile eşleşir.

Sonraki adım

Tanımladığınız ilkeyi doğrulamak için şu komutu verin:

```
dspmqspl -m QM_VERIFY_AMS
```

İlke ayrıntılarını `setmqspl` komutları kümesi olarak yazdırmak için `-export` işaretini kullanın. Bu, önceden tanımlanmış ilkelerin saklanmasına izin verir:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Kurulumu test etme

Bu görev hakkında

Farklı kullanıcıların altında farklı programlar çalıştırarak, uygulamanın doğru yapılandırılıp yapılandırıldığını doğrulayabilirsiniz.

Yordam

1. Örnekleri içeren dizine geçin. MQ varsayılan olmayan bir konuma kurulduysa, bu durum farklı bir yerde olabilir.

```
cd /opt/mqm/samp/bin
```

2. Kullanıcıyı kullanıcı `alice`olarak çalışacak şekilde değiştir

```
su alice
```

3. As the user `alice`, put a message using a sample application:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. İletinin metnini yazın ve Enter tuşuna basın.
5. Kullanıcı `alice`olarak çalıştımeyi durdur

```
exit
```

6. Kullanıcıyı kullanıcı bobolarak çalışacak şekilde değiştir

```
su bob
```

7. As the user bob, get a message using a sample application:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Sonuçlar

Uygulama her iki kullanıcı için de düzgün bir şekilde yapılandırıldıysa, bob uygulaması alma işlemi çalıştırıldığında kullanıcı `alice` ' un iletisi görüntülenir.

8. Şifreleme sınaması

Bu görev hakkında

To verify that the encryption is occurring as expected, create an alias queue which references the original queue TEST.Q. Bu diğer ad kuyruğunda güvenlik ilkesi yoktur; bu nedenle, kullanıcının iletinin şifresini çözmek için gereken bilgilere sahip olmayacak ve bu nedenle şifrelenmiş veriler gösterilecektir.

Yordam

1. Kuyruk yöneticisi QM_VERIFY_AMS için **runmqsc** komutunu kullanarak bir diğer ad kuyruğu yaratın.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Diğer ad kuyruğundan göz atmak için bob erişimi ver

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. As the user `alice`, put another message using a sample application just as before:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. As the user bob, browse the message using a sample application via the alias queue this time:

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. As the user bob, get the message using a sample application from the local queue:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Sonuçlar

amqsbcg uygulamasındaki çıktı, iletinin şifrelendiğini kanıtlayan kuyruğunda bulunan şifrelenmiş verileri gösterir.

z/OS *z/OSüzerindeki örnek yapılandırmalar*

Bu bölümde, z/OSüzerinde Advanced Message Security kuyruğa alma senaryolarına ilişkin ilkelerin ve sertifikaların örnek yapılandırmaları yer alır.

Advanced Message Security'yi nasıl yapılandırmanıza ilişkin ayrıntılar için Advanced Message Security for z/OSyapılandırılıyor ' e bakın.

Örnekler, gerekli Advanced Message Security ilkelerini ve kullanıcıların ve anahtar halkalarının göreli olarak var olması gereken dijital sertifikaları kapsamaya devam eder. Bu örneklerde, senaryolarda yer alan kullanıcıların, Kullanıcıların Advanced Message Securityiçin kaynak izinleri verbaşlıklı konuda sağlanan yönergeleri izleyerek ayarlandığını varsayar.

V 9.1.3 Buna ek olarak, IBM MQ 9.1.3 ' den başlayarak, bkz. sunucu-sunucu ileti kanalı ara düzey örnekleri.

z/OS *z/OSüzerinde bütünlük korumalı iletilerin kuyruğa alınması yerel kuyruğa alma*

Bu örnek, bütünlük korumalı iletileri göndermek ve kuyruktan almak ve uygulamaları almak için yerel olarak yerel olarak göndermek ve almak için gereken Advanced Message Security ilkelerini ve sertifikalarını içerir.

Örnek kuyruk yöneticisi ve kuyruğu aşağıdaki gibi olur:

```
BNK6        - Queue manager
FIN.XFER.Q7 - Local queue
```

Bu kullanıcılar kullanılır:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Kullanıcı sertifikalarını oluşturma

Bu örnekte yalnızca bir kullanıcı sertifikasına gerek vardır. Bu, bütünlük korumalı iletileri imzalamak için gereken kullanıcı sertifikasıdır. Gönderen kullanıcı 'TELLER5'.

Sertifika kuruluşu (CA) sertifikası da gereklidir. Sertifika kuruluşu (CA) sertifikası, kullanıcının sertifikasını veren yetkinin sertifikasıdır. Bu bir sertifika zinciri olabilir. Böyle bir durumda, zincirdeki tüm sertifikalar Advanced Message Security görev kullanıcısının anahtar halkasında, bu durumda WMQBNK6' da gereklidir.

Bir CA sertifikası, RACF RACDCERT komutu kullanılarak yaratılabilir. Bu sertifika, kullanıcı sertifikalarını vermek için kullanılır. Örneğin:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Bu RACDCERT komutu, 'TELLER5' kullanıcısı için kullanıcı sertifikası vermek üzere kullanılabilecek bir CA sertifikası yaratır. Örneğin:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Kuruluşunuzda bir CA sertifikasının seçilmesine ya da yaratılmasına ilişkin yordamlar ve sertifikaların yayınlanmak ve ilgili sistemlere dağıtılması için yordamlar olacaktır.

Bu sertifikaları dışa ve içe aktarırken Advanced Message Security aşağıdakileri gerektirir:

- CA sertifikası (zincir).
- Kullanıcı sertifikası ve özel anahtarı.

RACFkullanıyorsanız, sertifikaları bir veri kümesine aktarmak için RACDCERT EXPORT komutu kullanılabilir ve RACDCERT ADD komutu, sertifikaları veri kümesinden içe aktarmak için kullanılabilir. Bu ve diğer RACDCERT komutlarıyla ilgili daha fazla bilgi için *z/OS: Security Server RACF Command Language Reference*adlı konuya bakın.

The certificates in this case, are required on the z/OS system running queue manager BNK6.

Sertifikalar BNK6çalıştıran z/OS sisteminde içe aktarıldığında, kullanıcı sertifikası TRUST özniteliğini gerektirir. Sertifiya TRUST özniteliğini eklemek için RACDCERT ALTER komutu kullanılabilir. Örneğin:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Bu örnekte alıcı kullanıcı için sertifika gerekli değildir.

Sertifikaları ilgili anahtar halkalarına bağlan

Gerekli sertifikalar oluşturulduğunda ya da içe aktarıldığında ve güvenilir olarak ayarlandığında, bunlar BNK6çalıştıran z/OS sistemindeki uygun kullanıcı anahtarı halkalarına bağlanmalıdır. Anahtar halkalarını yaratmak için RACDCERT ADDRING komutlarını kullanın:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Bu, Advanced Message Security görev kullanıcısı (WMQBNK6) için bir anahtarlık ve gönderen kullanıcı ('TELLER5') için anahtarlık yaratır. drq.ams.keyring anahtar halkası adının zorunlu olduğunu ve adın büyük ve küçük harfe duyarlı olduğunu unutmayın.

Anahtarlık oluşturulduğunda, ilgili sertifikalar bağlanabiliyor:

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Gönderen kullanıcı sertifikası DEFAULT olarak bağlanmalıdır. Gönderen kullanıcının drq.ams.keyringdosyasında birden çok sertifikası varsa, varsayılan sertifika imzalama amacıyla kullanılır.

Kuyruk yöneticisi durdurup yeniden başlatılıncaya ya da Advanced Message Security sertifika yapılandırmasını yenilemek için z/OS **MODIFY** komutu kullanılıncaya kadar, sertifikaların yaratılması ve değiştirilmesi Advanced Message Security tarafından tanınmaz. Örneğin:

```
F BNK6AMSM,REFRESH KEYRING
```

Advanced Message Security ilkesini oluşturun

Bu örnekte, bütünlük korumalı iletiler, 'TELLER5' kullanıcısı olarak çalışan bir uygulama tarafından FIN.XFER.Q7 kuyruğuna konmuş ve 'FINADM2' kullanıcısı olarak çalışan bir uygulama tarafından aynı kuyruktan alınmaktadır, bu nedenle yalnızca bir Advanced Message Security ilkesi gereklidir.

Advanced Message Security ilkeleri, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)adresinde belgelenmiş olan CSQ0UTIL yardımcı programı kullanılarak yaratılır.

Aşağıdaki komutu çalıştırmak için CSQ0UTIL yardımcı programını kullanın:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

Bu ilkede, kuyruk yöneticisi BNK6olarak tanıtılır. İlke adı ve ilişkili kuyruk FIN.XFER.Q7. Gönderenin imzasını oluşturmak için kullanılan algoritma MD5'dir ve gönderen kullanıcının ayırt edici adı (DN)'CN=Teller5,O=BCO,C=US' olur.

İlkeyi tanımladıktan sonra, BNK6 kuyruk yöneticisini yeniden başlatın ya da Advanced Message Security ilke yapılandırmasını yenilemek için z/OS **MODIFY** komutunu kullanın. Örneğin:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Local queuing of privacy-protected messages on z/OS*

Bu örnek, uygulamaları koymak ve uygulamaları almak için yerel güvenlik korumalı iletileri göndermek ve kuyruktan korunan iletileri göndermek ve almak için gereken Advanced Message Security ilkelerini ve sertifikalarını içerir. Gizlilik korumalı iletiler hem imzalanır hem de şifrelenir.

Örnek kuyruk yöneticisi ve yerel kuyruk aşağıdaki gibidir:

```
BNK6        - Queue manager
FIN.XFER.Q8 - Local queue
```

Bu kullanıcılar kullanılır:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Bu senaryonun konfigürasyonunu tanımlamaya ilişkin adımlar şunlardır:

Kullanıcı sertifikalarını oluşturma

Bu örnekte, iki kullanıcı sertifikası gereklidir. Bunlar, iletileri imzalamak için gereken kullanıcı sertifikasıdır ve alıcı kullanıcının sertifika, ileti verilerinin şifrelenmesi ve şifrelerinin çözülmesi için gerekli olan sertifikadır. Gönderen kullanıcı 'TELLER5' ve alıcı kullanıcı 'FINADM2'.

Sertifika kuruluşu (CA) sertifikası da gereklidir.Sertifika kuruluşu (CA) sertifikası, kullanıcının sertifikasını veren yetkinin sertifikasıdır. Bu bir sertifika zinciri olabilir. Böyle bir durumda, zincirdeki tüm sertifikalar Advanced Message Security görev kullanıcısının anahtar halkasında, bu durumda WMQBNK6' da gereklidir.

Bir CA sertifikası, RACF RACDCERT komutu kullanılarak yaratılabilir. Bu sertifika, kullanıcı sertifikalarını vermek için kullanılır. Örneğin:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Bu RACDCERT komutu, 'TELLER5' ve 'FINADM2' kullanıcıları için kullanıcı sertifikalarını vermek üzere kullanılabilen bir CA sertifikası oluşturur. Örneğin:

```
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)
```

Kuruluşunuzda bir CA sertifikasının seçilmesine ya da yaratılmasına ilişkin yordamlar ve sertifikaların yayınlanmak ve ilgili sistemlere dağıtılması için yordamlar olacaktır.

Bu sertifikaları dışa ve içe aktarırken Advanced Message Security aşağıdakileri gerektirir:

- CA sertifikası (zincir).
- Gönderen kullanıcı sertifikası ve özel anahtarı.
- Alıcı kullanıcı sertifikası ve özel anahtarı.

RACFkullanıyorsanız, sertifikaları bir veri kümesine aktarmak için RACDCERT EXPORT komutu kullanılabilir ve RACDCERT ADD komutu, sertifikaları veri kümesinden içe aktarmak için kullanılabilir. Bu ve diğer RACDCERT komutlarıyla ilgili daha fazla bilgi için, *z/OS: Security Server RACF Command Language Reference*adlı yayında RACDCERT (Manage RACF digital certificalar) başlıklı konuya bakın.

The certificates in this case are required on the z/OS system running queue manager BNK6.

Sertifikalar BNK6çalıştıran z/OS sisteminde içe aktarıldığında, kullanıcı sertifikaları TRUST özniteliğini gerektirir. Sertifiya TRUST özniteliğini eklemek için RACDCERT ALTER komutu kullanılabilir. Örneğin:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Sertifikaları ilgili anahtar halkalarına bağlan

Gerekli sertifikalar oluşturulduğunda ya da içe aktarıldığında ve güvenilir olarak ayarlandığında, bunlar BNK6çalıştıran z/OS sistemindeki uygun kullanıcı anahtarı halkalarına bağlanmalıdır. Anahtar halkalarını yaratmak için RACDCERT ADDRING komutunu kullanın:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Bu, gönderme ve alıcı kullanıcılar için Advanced Message Security görevi kullanıcısı ve anahtar halkaları için bir anahtarlık oluşturur. drq.ams.keyring anahtar halkası adının zorunlu olduğunu ve adın büyük ve küçük harfe duyarlı olduğunu unutmayın.

Anahtar halkalar oluşturulduğunda, ilgili sertifikalar bağlanabilir.

```
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))
```

Gönderen ve alıcı kullanıcı sertifikalarının DEFAULT olarak bağlanması gerekir. Kullanıcının drq.ams.keyringanahtarında birden fazla sertifika varsa, imzalama ve şifre çözme amacıyla varsayılan sertifika kullanılır.

Alıcı kullanıcının sertifikasının, Advanced Message Security görev kullanıcısının USAGE (SITE) ile anahtar halkasına da bağlı olması gerekir. Bunun nedeni, ileti verilerini şifrelerken, İleri Düzey İleti Güvenliği görevinin alıcının genel anahtarının olması gerektiğinden kaynaklanır. USAGE (SITE), özel anahtarın anahtarlık içinde erişilir olmasını önler.

Kuyruk yöneticisi durdurup yeniden başlatılıncaya ya da Advanced Message Security sertifika yapılandırmasını yenilemek için z/OS **MODIFY** komutu kullanılıncaya kadar, sertifikaların yaratılması ve değiştirilmesi Advanced Message Security tarafından tanınmaz. Örneğin:

```
F BNK6AMSM,REFRESH KEYRING
```

Advanced Message Security ilkesini oluşturun

Bu örnekte, gizlilik korumalı iletiler, 'TELLER5' kullanıcısı olarak çalışan bir uygulama tarafından FIN.XFER.Q8 kuyruğuna konmuş ve 'FINADM2' kullanıcısı olarak çalışan bir uygulama tarafından aynı kuyruktan alınmaktadır, bu nedenle yalnızca bir Advanced Message Security ilkesi gereklidir.

Advanced Message Security ilkeleri, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)adresinde belgelenmiş olan CSQ0UTIL yardımcı programı kullanılarak yaratılır.

Aşağıdaki komutu çalıştırmak için CSQ0UTIL yardımcı programını kullanın:

```
setmqspl -m BNK6 -p FIN.XFER.Q8 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

Bu ilkede, kuyruk yöneticisi BNK6olarak tanıtılır. İlke adı ve ilişkili kuyruk FIN.XFER.Q8. Gönderenin imzasını oluşturmak için kullanılan algoritma SHA1ve gönderen kullanıcının ayırt edici adı (DN) 'CN=Teller5,O=BCO,C=US' ve alıcı kullanıcı 'CN=FinAdm2,O=BCO,C=US' olur. İleti verilerini şifrelemek için kullanılan algoritma 3DES' dir.

İlkeyi tanımladıktan sonra, BNK6 kuyruk yöneticisini yeniden başlatın ya da Advanced Message Security ilke yapılandırmasını yenilemek için z/OS **MODIFY** komutunu kullanın. Örneğin:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Remote queuing of integrity-protected messages on z/OS*

Bu örnek, iki farklı kuyruk yöneticisi tarafından yönetilen kuyruklara ve bu kuyruklardan bütünlük korumalı iletiler göndermek ve almak için gereken Advanced Message Security ilkelerini ve sertifikalarını ayrıntılarıyla içerir. İki kuyruk yöneticisi aynı z/OS sisteminde ya da farklı z/OS sistemlerinde çalıştırılabilir ya da bir kuyruk yöneticisi Advanced Message Securityçalıştıran dağıtılmış bir sistemde olabilir.

Örnek kuyruk yöneticileri ve kuyrukları şunlardır:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Not: Bu örnekte, BNK6 ve BNK7 , farklı z/OS sistemlerinde çalışan kuyruk yöneticileridir.

Bu kullanıcılar kullanılır:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMStask user on BNK7
```

```
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Bu senaryonun konfigürasyonunu tanımlamak için aşağıdaki adımlar aşağıdaki gibidir:

Kullanıcı sertifikalarını oluşturma

Bu örnekte yalnızca bir kullanıcı sertifikasına gerek vardır. Bu, bütünlük korumalı iletiyi imzalamak için gereken kullanıcı sertifikasıdır. Gönderen kullanıcı 'TELLER5'.

Sertifika kuruluşu (CA) sertifikası da gereklidir.Sertifika kuruluşu (CA) sertifikası, kullanıcının sertifikasını veren yetkinin sertifikasıdır. Bu bir sertifika zinciri olabilir. Böyle bir durumda, zincirdeki tüm sertifikalar Advanced Message Security görev kullanıcısının anahtar halkasında, bu durumda WMQBNK7' de gereklidir.

Bir CA sertifikası, RACF RACDCERT komutu kullanılarak yaratılabilir. Bu sertifika, kullanıcı sertifikalarını vermek için kullanılır. Örneğin:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Bu RACDCERT komutu, 'TELLER5' kullanıcısı için kullanıcı sertifikası vermek üzere kullanılabilecek bir CA sertifikası yaratır. Örneğin:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Kuruluşunuzda bir CA sertifikasının seçilmesine ya da yaratılmasına ilişkin yordamlar ve sertifikaların yayınlanmak ve ilgili sistemlere dağıtılması için yordamlar olacaktır.

Bu sertifikaları dışa ve içe aktarırken Advanced Message Security gereklidir:

- CA sertifikası (zincir).
- Gönderen kullanıcı sertifikası ve özel anahtarı.

RACFkullanıyorsanız, sertifikaları bir veri kümesine aktarmak için RACDCERT EXPORT komutu kullanılabilir ve RACDCERT ADD komutu, sertifikaları veri kümesinden içe aktarmak için kullanılabilir. Bu ve diğer RACDCERT komutlarıyla ilgili daha fazla bilgi için, *z/OS: Security Server RACF Command Language Reference*adlı yayında RACDCERT (Manage RACF digital certificalar) başlıklı konuya bakın.

The certificates in this case, are required on the z/OS system running queue manager BNK6 and BNK7.

Bu örnekte, gönderme sertifikası BNK6çalıştıran z/OS sisteminde içe aktarılmalıdır; CA sertifikası, BNK7çalıştıran z/OS sisteminde içe aktarılmalıdır. Sertifikalar içe aktarıldığında, kullanıcı sertifikası TRUST özniteliğini gerektirir. Sertifiya TRUST özniteliğini eklemek için RACDCERT ALTER komutu kullanılabilir. Örneğin, BNK6:üzerinde

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Sertifikaları ilgili anahtar halkalarına bağlan

Gerekli sertifikalar oluşturulduğunda ya da içe aktarıldığında ve güvenilir olarak ayarlandığında, bunlar BNK6 ve BNK7çalıştıran z/OS sisteminde uygun kullanıcı anahtarı halkalarına bağlanmalıdır.

Anahtar halkalarını yaratmak için BNK6:üzerinde RACDCERT ADDRING komutunu kullanın.

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

This creates a key ring for the sending user on BNK6. drq.ams.keyring anahtar halkası adının zorunlu olduğunu ve adın büyük ve küçük harfe duyarlı olduğunu unutmayın.

BNK7:üzerinde

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Bu, BNK7' de Advanced Message Security görev kullanıcısı için bir anahtarlık oluşturur. BNK7'de'TELLER5' için kullanıcı anahtarı halkası gerekmez.

Anahtar halkalar oluşturulduğunda, ilgili sertifikalar bağlanabilir.

BNK6:üzerinde

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

BNK7:üzerinde

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

Gönderen kullanıcı sertifikası DEFAULT olarak bağlanmalıdır. Gönderen kullanıcının drq.ams.keyringdosyasında birden çok sertifikası varsa, varsayılan sertifika imzalama amacıyla kullanılır.

Kuyruk yöneticisi durdurup yeniden başlatılıncaya ya da Advanced Message Security sertifika yapılandırmasını yenilemek için z/OS **MODIFY** komutu kullanılıncaya kadar, sertifikaların yaratılması ve değiştirilmesi Advanced Message Security tarafından tanınmaz. Örneğin:

BNK6:üzerinde

```
F BNK6AMSM,REFRESH,KEYRING
```

BNK7:üzerinde

```
F BNK7AMSM,REFRESH,KEYRING
```

Advanced Message Security ilkelerini oluşturma

In this example, integrity-protected messages are put to remote queue FIN.XFER.Q7 on BNK6 by an application running as user 'TELLER5', and retrieved from local queue FIN.RCPT.Q7 on BNK7 by an application running as user 'FINADM2', so two Advanced Message Security policies are required.

Advanced Message Security ilkeleri, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)adresinde belgelenmiş olan CSQ0UTIL yardımcı programı kullanılarak yaratılır.

BNK6:üzerindeki uzak kuyruk için bir bütünlük ilkesi tanımlamak üzere aşağıdaki komutu çalıştırmak için CSQ0UTIL yardımcı programını kullanın.

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

Bu ilkede, kuyruk yöneticisi BNK6olarak tanıtılır. İlke adı ve ilişkili kuyruk FIN.XFER.Q7. Gönderenin imzasını oluşturmak için kullanılan algoritma MD5'dir ve gönderen kullanıcının ayırt edici adı (DN)'CN=Teller5,O=BCO,C=US' olur.

Ayrıca, BNK7:üzerinde yerel kuyruk için bir bütünlük ilkesi tanımlamak üzere aşağıdaki komutu çalıştırmak için CSQ0UTIL yardımcı programını kullanın.

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

Bu ilkede, kuyruk yöneticisi BNK7olarak tanımlanır. İlke adı ve ilişkili kuyruk FIN.RCPT.Q7. Gönderenin imzası için beklenen algoritma MD5, gönderen kullanıcının ayırt edici adının (DN) 'CN=Teller5,O=BCO,C=US' olması beklenir.

İki ilkeyi tanımladıktan sonra, BNK6 ve BNK7 kuyruk yöneticilerini yeniden başlatın ya da Advanced Message Security ilke yapılanışlarını yenilemek için z/OS **MODIFY** komutunu kullanın. Örneğin:

BNK6:üzerinde

```
F BNK6AMSM,REFRESH,POLICY
```

BNK7:üzerinde

```
F BNK7AMSM,REFRESH,POLICY
```

z/OS *z/OS üzerinde gizliliğe karşı korumalı iletilerin uzaktan kuyruğa alınması*

Bu örnek, iki farklı kuyruk yöneticisi tarafından yönetilen kuyruklara/kuyruklardan gizlilik korumalı ileti göndermek ve almak için gereken Advanced Message Security ilkelerini ve sertifikalarını ayrıntılı olarak verir. İki kuyruk yöneticisi aynı z/OS sisteminde ya da farklı z/OS sistemlerinde çalışıyor olabilir ya da bir kuyruk yöneticisi Advanced Message Securityçalıştıran dağıtılmış bir sistemde olabilir.

Örnek kuyruk yöneticileri ve kuyrukları şunlardır:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Not: Bu örnekte, BNK6 ve BNK7 aynı adı taşıyan farklı z/OS sistemlerinde çalışan kuyruk yöneticileridir.

Bu kullanıcılar kullanılır:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMS task user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Bu senaryoyu yapılandırma adımları aşağıdaki gibidir:

Kullanıcı sertifikalarını oluştur

Bu örnekte, iki kullanıcı sertifikası gereklidir. Bunlar, iletileri imzalamak için gerekli olan gönderen kullanıcı sertifikası ve ileti verilerini şifrelemek ve şifresini çözmek için gerekli olan alıcı kullanıcı sertifikasıdır. Gönderen kullanıcı: 'TELLER5' ve alıcı kullanıcı: 'FINADM2'.

Sertifika Yetkilisi (CA) sertifikası da gereklidir.CA sertifikası, kullanıcının sertifikasını veren yetkinin sertifikasıdır. Bu bir sertifika zinciri olabilir. Bu durumda, Advanced Message Security görev kullanıcısının anahtarlığı için zincirdeki tüm sertifikalar gereklidir; bu durumda WMQBNK7kullanıcısı gerekir.

RACF RACDCERT komutu kullanılarak bir CA sertifikası yaratılabilir. Bu sertifika, kullanıcı sertifikalarını vermek için kullanılır. Örneğin:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Bu RACDCERT komutu, kullanıcılarınTELLER5've'FINADM2' kullanıcı sertifikalarını yayınlamak için kullanılabilecek bir CA sertifikası yaratır. Örneğin:

```
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)
```

Kuruluşunuzda sertifika seçme ya da yaratma yordamlarının yanı sıra sertifika verme ve bunları ilgili sistemlere dağıtma yordamları da vardır.

Bu sertifikaları dışa ve içe aktarırken Advanced Message Security şunları gerektirir:

- CA sertifikası (zincir).
- Gönderen kullanıcı sertifikası ve özel anahtarı.
- Alıcı kullanıcı sertifikası ve özel anahtarı.

RACFkullanıyorsanız, sertifikaları bir veri kümesine aktarmak için RACDCERT EXPORT komutu kullanılabilir ve sertifikaları veri kümesinden içe aktarmak için RACDCERT ADD komutu kullanılabilir.

Bu ve diğer RACDCERT komutlarıyla ilgili daha fazla bilgi için *z/OS: Security Server RACF Command Language Reference*adlı yayında RACDCERT (Manage RACF digital sertifikalar) başlıklı konuya bakın.

Bu durumda sertifikalar, BNK6 ve BNK7kuyruk yöneticisini çalıştıran z/OS sisteminde gereklidir.

Bu örnekte, gönderen ve alıcı sertifikalarının BNK6çalıştıran z/OS sisteminde içe aktarılması ve CA ve alıcı sertifikalarının BNK7çalıştıran z/OS sistemde içe aktarılması gerekir. Sertifikalar içe aktarıldığında, kullanıcı sertifikaları TRUST özniteliğini gerektirir. RACDCERT ALTER komutu, sertifikaya TRUST özniteliğini eklemek için kullanılabilir. Örneğin:

BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

BNK7:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Sertifikaları ilgili anahtar halkalarına bağla

Gerekli sertifikalar oluşturulduğunda ya da içe aktarıldığında ve güvenilir olarak ayarlandığında, bunlar BNK6 ve BNK7çalıştıran z/OS sistemlerinde uygun kullanıcı anahtarı halkalarına bağlanmalıdır.

Anahtar halkalarını yaratmak için RACDCERT ADDRING komutunu kullanın:

BNK6:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Bu, Advanced Message Security görev kullanıcısı için bir anahtarlık ve BNK6üzerinde gönderen kullanıcı için bir anahtarlık oluşturur. drq.ams.keyring anahtarlık adının zorunlu olduğunu ve adın büyük ve küçük harfe duyarlı olduğunu unutmayın.

BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Bu, Advanced Message Security görev kullanıcısı için bir anahtarlık ve BNK7üzerinde alıcı kullanıcı için bir anahtarlık oluşturur.

Anahtar halkaları oluşturulduğunda, ilgili sertifikalar bağlanabilir.

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))
```

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))
```

Gönderen ve alıcı kullanıcı sertifikalarının DEFAULT olarak bağlanması gerekir. Herhangi bir kullanıcının drq.ams.keyringdosyasında birden fazla sertifikası varsa, varsayılan sertifika imzalama ve şifreleme/şifre çözme amacıyla kullanılır.

BNK6' da, alıcının sertifikasının Advanced Message Security görev kullanıcısının USAGE (SITE) ile anahtarlık halkasına da bağlanması gerekir. Bunun nedeni, Gelişmiş İleti Güvenliği görevinin, ileti verilerini şifrelerken alıcının genel anahtarının gerekli olmasıdır. USAGE (SITE), özel anahtarın anahtar halkasında erişilebilir olmasını önler.

Kuyruk yöneticisi durdurulup yeniden başlatılıncaya ya da Advanced Message Security sertifika yapılandırmasını yenilemek için z/OS **MODIFY** komutu kullanılıncaya kadar sertifikaların yaratılması ve değiştirilmesi Advanced Message Security tarafından tanınmaz. Örneğin:

BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Advanced Message Security ilkelerinin yaratılması

Bu örnekte, gizlilik korumalı iletiler 'TELLER5' kullanıcısı olarak çalışan bir uygulama tarafından BNK6 üzerinde FIN.XFER.Q7 uzak kuyruğuna yerleştirilir ve 'FINADM2' kullanıcısı olarak çalışan bir uygulama tarafından BNK7 üzerindeki FIN.RCPT.Q7 yerel kuyruğundan alınır, bu nedenle iki Advanced Message Security ilkesi gerekir.

Advanced Message Security ilkeleri, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)adresinde belgelenen CSQ0UTIL yardımcı programı kullanılarak yaratılır.

BNK6: üzerinde uzak kuyruk için bir gizlilik ilkesi tanımlamak üzere aşağıdaki komutu çalıştırmak için CSQ0UTIL yardımcı programını kullanın:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

Bu ilkede, kuyruk yöneticisi BNK6olarak tanımlanır. İlke adı ve ilişkili kuyruk: FIN.XFER.Q7. Gönderenin imzasını oluşturmak için kullanılan algoritma şudur: SHA1, gönderen kullanıcının ayırt edici adı (DN): 'CN=Teller5,O=BCO,C=US' ve alıcı kullanıcı: 'CN=FinAdm2,O=BCO,C=US'. İleti verilerini şifrelemek için kullanılan algoritma 3DES' tir.

Ayrıca, BNK7: üzerinde yerel kuyruk için bir gizlilik ilkesi tanımlamak üzere aşağıdaki komutu çalıştırmak için CSQ0UTIL yardımcı programını kullanın:

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

Bu ilkede, kuyruk yöneticisi BNK7olarak tanımlanır. İlke adı ve ilişkili kuyruk: FIN.RCPT.Q7. Gönderenin imzası için beklenen algoritma SHA1, gönderen kullanıcının ayırt edici adının (DN) 'CN=Teller5,O=BCO,C=US' olması ve alıcı kullanıcının 'CN=FinAdm2,O=BCO,C=US' olması beklenir. İleti verilerinin şifresini çözmek için kullanılan algoritma 3DES' tir.

İki ilkeyi tanımladıktan sonra, BNK6 ve BNK7 kuyruk yöneticilerini yeniden başlatın ya da Advanced Message Security ilke yapılandırmasını yenilemek için z/OS **MODIFY** komutunu kullanın. Örneğin:

BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

Quick Start Guide for AMS with Java clients

İstemci bağ tanımlarını kullanarak bağlanan Java uygulamaları için ileti güvenliği sağlamak üzere Advanced Message Security olanağını hızlı bir şekilde yapılandırmak için bu kılavuzu kullanın. Tamamladığınız zaman, kullanıcı kimliklerini doğrulamak ve kuyruk yöneticiniz için imzalama/şifreleme ilkeleri tanımlamanız için bir anahtar deposu yaratmış olacaktır.

Başlamadan önce

Hızlı Başlangıç Kılavuzu ' nda (Windows ya da UNIX) açıklandığı gibi, uygun bileşenlerin kurulmuş olduğundan emin olun.

1. Kuyruk yöneticisi ve kuyruk yaratılması

Bu görev hakkında

Aşağıdaki örneklerin tümü, uygulamalar arasında ileti geçirmesi için TEST.Q adlı bir kuyruk kullanır. Advanced Message Security , iletileri standart IBM MQ arabirimi aracılığıyla IBM MQ altyapısına girdikleri noktada imzalamak ve şifrelemek için kesicileri kullanır. Temel kurulum IBM MQ içinde yapılır ve aşağıdaki adımlarda yapılandırılır.

Yordam

1. Kuyruk yöneticisi yarat

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Kuyruk yöneticisini başlatma

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Create and start a listener by entering the following commands into **runmqsc** for queue manager QM_VERIFY_AMS

   ```
   DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
   START LISTENER(AMS.LSTR)
   ```

4. Create a channel for our applications to connect in through by entering the following command into **runmqsc** for queue manager QM_VERIFY_AMS

```
DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
```

5. Create a queue called TEST.Q by entering the following command into **runmqsc** for queue manager QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Sonuçlar

Yordam başarıyla tamamlandıysa, **runmqsc** içine girilen şu komut, TEST.Qile ilgili ayrıntıları görüntüler:

```
DISPLAY Q(TEST.Q)
```

2. Kullanıcıların yaratılması ve yetkilendirilmesi

Bu görev hakkında

Bu senaryoda yer alan iki kullanıcı vardır: alice, gönderen ve bob, alıcı. Uygulama kuyruğunu kullanmak için, bu kullanıcıların kullanabilmeleri için yetki verilmesi gerekir. Bu senaryoda tanımlanan koruma ilkelerini başarıyla kullanmak için, bu kullanıcıların bazı sistem kuyruklarına erişim izni verilmelidir. **setmqaut** komutuna ilişkin ek bilgi edinmek için **setmqaut**belgesine bakın.

Yordam

1. Create the two users as described in the **Hızlı Başlama Kılavuzu** (Windows or UNIX) for your platform.
2. Kullanıcıların kuyruk yöneticisine bağlanmasını ve kuyrukla çalışabilmeleri için yetki verir

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get +inq +browse
```

3. Ayrıca, iki kullanıcının sistem ilke kuyruğuna göz atmasına ve iletileri hata kuyruğuna koymalarına izin vermelisiniz.

```
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
```

Uyarı: IBM MQ , ilkeleri önbelleğe alarak başarımı en iyi duruma getirir; böylece, SYSTEM.PROTECTION.POLICY.QUEUE (tüm durumlarda kuyruk).

IBM MQ , var olan tüm ilkeleri önbelleğe almaz. Çok sayıda ilke varsa, IBM MQ sınırlı sayıda ilkeyi önbelleğe alır. So, if the queue manager has a low number of policies defined, there is no need to provide the browse option to the SYSTEM.PROTECTION.POLICY.QUEUE.

Ancak, çok sayıda ilke tanımlanmış olması durumunda ya da eski istemciler kullanıyorsanız, bu kuyruğa göz atma yetkisi vermelisiniz. SYSTEM.PROTECTION.ERROR.QUEUE , AMS kodu tarafından oluşturulan hata iletilerini koymak için kullanılır. Bu kuyruğa ilişkin koyma yetkisi yalnızca, kuyruğa bir hata iletisi koyma girişiminde bulunduğunuzda denetlenir. Bir AMS korumalı kuyruğundan ileti koyma ya da alma girişiminde bulunduğunuzda, kuyruğa koyma yetkiniz denetlenmez.

Sonuçlar

Artık kullanıcılar oluşturulur ve bu kullanıcılara gerekli yetkiler verilir.

Sonraki adım

To verify if the steps were carried out correctly, use the `JmsProducer` and `JmsConsumer` samples as described in section “7. Kurulumu test etme” sayfa 576.

3. Anahtar veritabanı ve sertifikalar yaratılması

Bu görev hakkında

İletiyi engelleyici olarak şifrelemek için, gönderen kullanıcıların genel anahtarı gerekir. Bu nedenle, genel ve özel anahtarlarla eşlenen kullanıcı kimliklerinin anahtar veritabanı yaratılmalıdır. Kullanıcıların ve uygulamaların birden çok bilgisayar üzerinden dağıldığı gerçek sistemde, her kullanıcının kendi özel anahtar deposu olabilir. Benzer şekilde, bu kılavuzda, `alice` ve bob için temel veritabanları oluşturuyoruz ve kullanıcı sertifikalarını bu kullanıcılar arasında paylaşıyoruz.

Not: Bu kılavuzda, istemci bağ tanımlarını kullanarak Java ' ta yazılmış örnek uygulamaları kullanırız. Yerel bağ tanımları ya da C uygulamalarını kullanarak Java uygulamalarını kullanmayı planlıyorsanız, **runmqakm** komutunu kullanarak bir CMS anahtar deposu ve sertifikalar oluşturmanız gerekir. Bu, **Hızlı Başlangıç Kılavuzu** ' nda (Windows ya da UNIX) gösterilir.

Yordam

1. Anahtar deponuzun yaratılacağı bir dizin yaratın (örneğin, `/home/alice/.mqs`). Bunu, **Hızlı Başlama Kılavuzu** (Windows ya da UNIX) tarafından kullanılan aynı dizinde oluşturmak isteyebilirsiniz. Platformunuz için.

   Not: Bu dizine aşağıdaki adımlarda *keystore-dir* adı verilir
2. Create a new keystore and certificate identifying the user `alice` for use in encryption

   Not: keytool komutu JRE ' nin bir parçasıdır.

   ```
   keytool -genkey -alias Alice_Java_Cert -keyalg RSA -keystore keystore-dir/keystore.jks
   -storepass passw0rd
   -dname "CN=alice, O=IBM, C=GB" -keypass passw0rd
   ```

   Not:

   - *keystore-dir* boşluk içeriyorsa, anahtar deponuzun tam adını tırnak içine almalısınız
   - Anahtar deposunun güvenliğini sağlamak için güçlü bir parola kullanmanız önerilir.
   - Bu kılavuzun amacı için, Sertifika Yetkilisi (Certificate Authority) kullanılmadan yaratılabilecek kendinden onaylı sertifika kullanırız. Üretim sistemleri için, kendinden imzalı sertifikaların kullanılmaması önerilir, ancak bunun yerine bir Sertifika Yetkilisi tarafından imzalanan sertifikalara güvenilebilir.
   - **alias** parametresi, sertifikaların gerekli bilgileri almak için arayacağı sertifikana ilişkin adı belirtir.
   - **dname** parametresi, her kullanıcı için benzersiz olması gereken **Belirleyici Ad** (DN) ile ilgili ayrıntıları belirtir.
3. UNIX' ta, anahtar deposunun okunabilir olduğundan emin olun

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Repeat step1-4 for the user bob

Sonuçlar

The two users `alice` and bob each now have a self-signed certificate.

4. keystore.confOluşturulması

Bu görev hakkında

Advanced Message Security algılayıcılarını, anahtar veritabanlarının ve sertifikaların bulunduğu dizine göstermelisiniz. Bu işlem, bu bilgileri düz metin biçiminde tutan `keystore.conf` dosyası aracılığıyla gerçekleştirilir. Her kullanıcının ayrı bir `keystore.conf` dosyası olması gerekir. Bu adımın hem `alice` hem de bobiçin yapılması gerekir.

Örnek

For this scenario, the contents of the `keystore.conf` for `alice` are as follows:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

For this scenario, the contents of the `keystore.conf` for bob are as follows:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Not:

- Anahtar deposu dosyasının yolu, dosya uzantısı olmadan sağlanmalıdır.
- Hızlı Başlama Kılavuzu 'nda (Windows ya da UNIX) yönergeleri izlediğiniz için bir `keystore.conf` dosunuz varsa, bu satırları eklemek için var olan dosyayı düzenleyebilirsiniz.
- Daha fazla bilgi için bkz “AMS için anahtar deposu yapılandırma dosyasının (keystore.conf) yapısı” sayfa 585.

5. Sertifikaların paylaşımı

Bu görev hakkında

Her bir kullanıcının diğerini başarıyla tanıması için sertifikaları iki anahtar deposu arasında paylaşın. Bu işlem, her kullanıcının sertifikası çıkarılarak ve diğer kullanıcının anahtar deposuna içe aktarılarak gerçekleştirilir.

Not: *alma* ve *dışa aktarma* terimleri farklı sertifika araçları tarafından farklı şekilde kullanılır. Örneğin, IBM GSKit **`strmqikm`** komutu (ikeyman) aracı, *alma* sertifikaları (genel anahtarlar) ve siz *dışa aktarma* özel anahtarlarınızı bir ayrım yapar. *dışa aktarma* seçeneği yanlışlıkla özel anahtarından geçerek uygulamanızı tamamen tehlikeye sokarsa, bu ayrım her iki seçeneği de sunan araçlar için son derece önemlidir. Bu ayrım çok önemli olduğu için, IBM MQ belgeleri bu terimleri tutarlı bir şekilde kullanmaya çalışmaktadır. Ancak, Java anahtar aracı, yalnızca genel anahtarı çıkaran *exportcert* adlı bir komut satırı seçeneği sağlar. For these reasons, the following procedure refers to *çıkarma* certificates by using the *dışa portsert* option.

Yordam

1. `alice`sertifikasını tanıt.

   ```
   keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passw0rd
   -alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
   ```

2. `alice` sertifikasını, bob ' in kullanacağı anahtar deposuna aktarın. İstendiğinde, bu sertifiya güvenileceğini belirten bir bilgi istemi görüntülenir.

```
keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert
-keystore bob-keystore-dir/keystore.jks -storepass passw0rd
```

3. bobiçin adımları yineleyin.

Sonuçlar

The two users `alice` and bob are now able to successfully identify each other having created and shared self-signed certificates.

Sonraki adım

Bir sertifikanda, ayrıntılarını yazan şu komutları çalıştırarak anahtar deposunda bulunduğunu doğrulayın:

```
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. Kuyruk ilkesinin tanımlanması

Bu görev hakkında

İleti önleme ve şifreleme anahtarlarına erişim için hazırlanan kuyruk yöneticisi tarafından oluşturulan ve algılayıcılar sayesinde, `setmqspl` komutunu kullanarak `QM_VERIFY_AMS` üzerinde koruma ilkeleri tanımlamaya başlayabiliriz. Bu komutla ilgili ek bilgi için setmqspl belgesine bakın. Her ilke adının, uygulanacak kuyruk adıyla aynı olması gerekir.

Örnek

This is an example of a policy defined on the `TEST.Q` queue, signed by the user `alice` using the `SHA1` algorithm, and encrypted using the 256-bit AES algorithm for the user bob:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Not: Ayırt edici adlar (DN), ilgili kullanıcının sertifikasında anahtar veri tabanından tam olarak belirtilenler ile eşleşir.

Sonraki adım

Tanımladığınız ilkeyi doğrulamak için şu komutu verin:

```
dspmqspl -m QM_VERIFY_AMS
```

İlke ayrıntılarını `setmqspl` komutları kümesi olarak yazdırmak için `-export` işareti. Bu, önceden tanımlanmış ilkelerin saklanmasına izin verir:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Kurulumu test etme

Başlamadan önce

Kullanmakta olduğunuz Java sürümünün kısıtlanmamış JCE ilke dosyaları kurulu olduğundan emin olun.

Not: IBM MQ kurulumunda sağlanan Java sürümünün bu ilke dosyaları zaten var. *MQ_INSTALLATION_PATH*`/java/bin`içinde bulunabilir.

Bu görev hakkında

Farklı kullanıcıların altında farklı programlar çalıştırarak, uygulamanın doğru yapılandırılıp yapılandırıldığını doğrulayabilirsiniz. Refer to the **Hızlı Başlama Kılavuzu** (Windows or UNIX) for your platform, for details about running programs under different users.

Yordam

1. To run these JMS sample applications, use the CLASSPATH setting for your platform as shown in IBM MQ classes for JMStarafından kullanılan ortam değişkenleri to ensure the samples directory is included.
2. As the user `alice`, put a message using a sample application, connecting as a client:

```
java JmsProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

3. As the user bob, get a message using a sample application, connecting as a client:

```
java JmsConsumer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

Sonuçlar

Uygulama her iki kullanıcı için de düzgün bir şekilde yapılandırıldıysa, bob uygulaması alma işlemi çalıştırıldığında kullanıcı `alice` ' un iletisi görüntülenir.

Uzak Kuyrukların Korunması

Uzak kuyrukları tam olarak korumak için, iletilerin iletileceği uzak kuyrukta ve yerel kuyrukta ilkeler belirlenmeli.

Bir ileti uzak bir kuyruğa konduğunda, Advanced Message Security işlemi durduruyor ve iletiyi uzak kuyruk için belirlenen bir ilke kümesine göre işler. Örneğin, bir şifreleme ilkesi için, iletiyi işlemek üzere IBM MQ ' e iletilmeden önce ileti şifrelenir. Advanced Message Security uzak bir kuyruğa geçen iletiyi işledikten sonra, IBM MQ bu iletiyi ilişkili iletim kuyruğuna koyar ve hedef kuyruk yöneticisine ve hedef kuyruğa iletir.

Yerel kuyruğunda bir GET işlemi gerçekleştirildiğinde, Advanced Message Security , iletiyi yerel kuyruktaki ilke kümesine göre kodu çözmeyi dener. İşlemin başarılı olması için, iletinin şifresini çözmek için kullanılan ilkenin şifrelemek için kullanılanla aynı olması gerekir. Herhangi bir uyumsuzluk, iletinin reddedilmesine neden olur.

Herhangi bir nedenle her iki ilke de aynı anda ayarlanamazsa, aşamalı bir roll-out desteği sağlanır. İlke, tolerans işareti açık olan yerel bir kuyrukta ayarlanabilir; bu, kuyruktan ileti alma girişimi, güvenlik ilkesi ayarlanmamış bir iletiyi içerdiğinde, kuyrukla ilişkilendirilmiş bir ilkenin yoksayılabilir. Bu durumda GET, iletinin şifresini çözmeyi deneyecek, ancak şifrelenmemiş iletilerin teslim edilmesini sağlayacak. Uzak kuyruklardaki bu yöntem, yerel kuyruklar korunduktan (ve sınandıktan sonra) ayarlanabiliyor.

Unutmayın: Remove the toleration flag once the Advanced Message Security roll-out has been completed.

İlgili başvurular

setmqspl (güvenlik ilkesini ayarla)

IBM Integration Buskomutunu kullanarak korunan iletiler yöneltilmesi

Advanced Message Security can protect messages in an infrastructure where IBM Integration Bus, or WebSphere Message Broker 8.0.0.1 (or later) is installed. IBM Integration Bus ortamında güvenliği uygulamadan önce her iki ürünün doğasını da anlamanız gerekir.

Bu görev hakkında

Advanced Message Security , ileti bilgi yükünün uçtan uca güvenliğini sağlar. Bu, yalnızca geçerli gönderenler ve bir iletinin alıcıları olarak belirtilen tarafların bunu üretebilme ya da alma yeteneğine sahip olduğu anlamına gelir. This implies that in order to secure messages flowing through IBM Integration

Bus, you can either allow IBM Integration Bus to process messages without knowing their content (1. senaryo) or make it an authorized user able to receive and send messages (2. senaryo).

1. senaryo- Integration Bus ileti içeriğini göremiyor

Başlamadan önce

IBM Integration Bus ' nizin var olan bir kuyruk yöneticisine bağlı olması gerekir. *QMgrName* komutunu, izleyen komutlarda var olan kuyruk yöneticisi adıyla değiştirin.

Bu görev hakkında

Bu senaryoda, Alice korumalı bir ileti giriş kuyruğuna QINyerleştirir. Based on the message property routeTo, the message is routed either to *bob 'un* (QBOB),[1](QCECIL) ya da varsayılan (QDEF) kuyruğu. The routing is possible because Advanced Message Security protects only the message payload and not its headers and properties which remain unprotected and can be read by IBM Integration Bus. Advanced Message Security yalnızca *alice*, *bob* ve *cecil*tarafından kullanılır. IBM Integration Busiçin kuruluş ya da yapılandırma gerekli değildir.

IBM Integration Bus , iletinin şifresini çözmek için herhangi bir girişimden kaçınmak için, korunmayan diğer ad kuyruğundan korunan iletiyi alır. Korunan kuyruğu doğrudan kullanacaksa, ileti, şifresini çözmek için, DEAD LETTER kuyruğuna konmuş olur. İleti, IBM Integration Bus tarafından yönlendirilir ve hedef kuyruğa değişmeden gelir. Bu nedenle, özgün yazar tarafından hala imzalanır (hem *bob* hem de *cecil* , yalnızca *alice* tarafından gönderilen iletileri kabul eder) ve daha önce olduğu gibi korumalıdır (yalnızca *bob* ve *cecil* okuyabilir). IBM Integration Bus , yönlendirilmiş iletiyi korunmayan bir diğer ada yerleştirir. Alıcılar, korunan bir çıkış kuyruğundan iletiyi alır; burada AMS , iletiyi saydam bir şekilde şifresini çözer.

Yordam

1. Configure *alice*, *bob* and *Cecil* to use Advanced Message Security as described in the **Hızlı Başlama Kılavuzu** (Windows or UNIX).

   Aşağıdaki adımların tamamlandığından emin olun:

   - Kullanıcıların yaratılması ve yetkilendirilmesi
   - Anahtar Veritabanı ve Sertifikalar Yaratılması
   - keystore.confyaratılması
2. Provide *Alice 'in* certificate to *bob* and *Cecil*, so *alice* can be identified by them when checking digital signatures on messages.

   Do this by extracting the certificate identifying *alice* to an external file, then adding the extracted certificate to *bob 'un* and *Cecil's* keystores. **Görev 5 'te açıklanan yöntemi kullanmanız önemlidir. Hızlı Başlama Kılavuzu (Windows ya da UNIX) içindeSertifikaları Paylaşma** .
3. Provide *bob* and *Cecil's* certificates to *alice*, so *alice* can send messages encrypted for *bob* and *Cecil*.

   Bunu, önceki adımda belirtilen yöntemi kullanarak yapın.
4. Kuyruk yöneticinizde, QIN, QBOB, QCECIL ve QDEFadlı yerel kuyrukları tanımlayın.

   ```
   DEFINE QLOCAL(QIN)
   ```
5. QIN kuyruğu için güvenlik ilkesini uygun bir yapılandırmaya ayarlayın. QBOB, QCECIL ve QDEF kuyrukları için özdeş ayarı kullanın.

   ```
   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"
   ```

   This scenario assumes the security policy where *alice* is the only authorized sender and *bob* and *Cecil* are the recipients.

[1] Cecil's

6. AIN, ABOB ve ACECIL diğer ad kuyruklarını sırasıyla QIN, QBOB ve QCECIL yerel kuyruklarına başvuruda bulunuyor.

```
DEFINE QALIAS(AIN) TARGET(QIN)
```

7. Önceki adımda belirtilen diğer adlara ilişkin güvenlik yapılandırmasının mevcut olmadığını doğrulayın; tersi durumda, ilkeyi NONE (Yok) olarak ayarlayın.

```
dspmqspl -m QMgrName -p AIN
```

8. IBM Integration Bus ' ta, AIN diğer ad kuyruğuna gelen iletileri, iletinin routeTo özelliğine bağlı olarak BOB, CECIL ya da DEF düğümüne yöneltmek için bir ileti akışı yaratın. Bunu yapmak için:
   a) IN adlı bir MQInput düğümü oluşturun ve AIN diğer adını kuyruk adı olarak atayın.
   b) Create MQOutput nodes called BOB, CECIL and DEF, and assign alias queues ABOB, ACECIL and ADEF as their respective queue names.
   c) Create a route node and call it TEST.
   d) IN düğümünü TEST düğümünün giriş terminaline bağlayın.
   e) TEST düğümü için bobve cecil çıkış uçbirimleri oluşturun.
   f) bob çıkış uçbirimini BOB düğümüne bağlayın.
   g) cecil çıkış uçbirimini CECIL düğümüne bağlayın.
   h) DEF düğümünü varsayılan çıkış uçbirimine bağlayın.
   i) Aşağıdaki kuralları uygulayın:

```
$Root/MQRFH2/usr/routeTo/text()="bob"
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. İleti akışını IBM Integration Bus yürütme ortamı bileşenine konuşlandırın.
10. Running as the user Alice put a message that also contains a message property called routeTo with a value of either bob or cecil. Running the sample application **amqsstm** will allow you to do this.

```
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. Running as user *bob* retrieve the message from the queue QBOB using the sample application **amqsget**.

Sonuçlar

alice , QIN kuyruğuna bir ileti yerleştirdiğinde, ileti korunur. It is retrieved in protected form by the IBM Integration Bus from the AIN alias queue. IBM Integration Bus decides where to route the message reading the routeTo property which is, as all properties, not encrypted. IBM Integration Bus , iletiyi uygun korunmayan diğer ad üzerine yerleştirir ve daha fazla korumasını önlemektedir. Kuyruktan *bob* ya da *cecil* tarafından alındığında, iletinin şifresi çözülüyor ve dijital imza doğrulanır.

2. senaryo- Integration Bus ileti içeriğini görebilir

Bu görev hakkında

Bu senaryoda, bir grup kişinin IBM Integration Bus' e ileti göndermesine izin verilir. Başka bir grup, IBM Integration Bustarafından oluşturulan iletileri almaya yetkilidir. Taraflar arasındaki iletim ve IBM Integration Bus ' in dinleme işlemi iptal edilemez.

IBM Integration Bus ' in koruma ilkelerini ve sertifikalarını yalnızca bir kuyruk açıldığında okuduğunu unutmayın; bu nedenle, değişikliklerin yürürlüğe girmesi için koruma ilkelerinde herhangi bir güncelleme yaptıktan sonra yürütme grubunu yeniden yüklemeniz gerekir.

```
mqsireload execution-group-name
```

If IBM Integration Bus is considered an authorized party allowed to read or sign the message payload, you must configure Advanced Message Security for the user starting the IBM Integration Bus service. Bu kullanıcının, iletileri kuyruklara koyan/alan ve IBM Integration Bus uygulamalarını yaratan ve devreye alan kullanıcının ya da bu kullanıcının aynı kullanıcının olması gerekmemekte olduğunu unutmayın.

Yordam

1. Configure *alice*, *bob*, *Cecil* and *dave* and the IBM Integration Bus service user, to use Advanced Message Security as described in the **Hızlı Başlama Kılavuzu** (Windows or UNIX).

   Aşağıdaki adımların tamamlandığından emin olun:

   - Kullanıcıların yaratılması ve yetkilendirilmesi
   - Anahtar Veritabanı ve Sertifikalar Yaratılması
   - keystore.confyaratılması
2. IBM Integration Bus hizmet kullanıcısına *alice*, *bob*, *cecil* ve *dave's* sertifikalarını belirtin.

   Bunu yapmak için, *alice*, *bob*, *cecil* ve *dave* dosyalarını dış dosyalara tanıtan sertifikaların her birini açın ve çıkarılan sertifikaları IBM Integration Bus anahtar deposuna ekleyin. **Görev 5 'te açıklanan yöntemi kullanmanız önemlidir. Hızlı Başlama Kılavuzu (Windows ya da UNIX) içindeSertifikaları Paylaşma** .
3. IBM Integration Bus hizmet kullanıcısının sertifikasını *alice*, *bob*, *cecil* ve *dave*olarak belirtin.

   Bunu, önceki adımda belirtilen yöntemi kullanarak yapın.

   Not: *Alice.* and *bob* need the IBM Integration Bus service user's certificate to encrypt the messages correctly. The IBM Integration Bus service user needs *Alice 'in* and *bob 'un* certificates to verify authors of the messages. IBM Integration Bus hizmet kullanıcısının, iletileri şifrelemek için *cecil's* ve *dave's* sertifikalarına gerek vardır. *Cecil* and *dave* need the IBM Integration Bus service user's certificate to verify if the message comes from IBM Integration Bus.
4. `IN` adlı bir yerel kuyruk tanımlayın ve yazar olarak belirtilen *alice* ve *bob* ile belirtilen güvenlik ilkesini ve alıcı olarak belirtilen IBM Integration Bus için hizmet kullanıcısını tanımlayın:

   ```
   setmqspl -m QMgrName -p IN -s MD5 -a "CN=alice,O=IBM,C=GB" -a "CN=bob,O=IBM,C=GB"
   -e AES256 -r "CN=broker,O=IBM,C=GB"
   ```
5. `OUT`adlı bir yerel kuyruk tanımlayın ve güvenlik ilkesini, yazar olarak belirtilen IBM Integration Bus için hizmet kullanıcısıyla tanımlayın ve alıcılar olarak belirtilen *cecil* ve *dave* değerini belirtin:

   ```
   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. IBM Integration Bus içinde, `MQInput` ve `MQOutput` düğümü ile bir ileti akışı oluşturun. Configure the `MQInput` node to use the `IN` queue and the `MQOutput` node to use the `OUT` queue.
7. İleti akışını IBM Integration Bus yürütme ortamı bileşenine konuşlandırın.
8. Running as user *alice* or *bob* put a message on the queue `IN` using the sample application **amqsput**.

9. Running as user *Cecil* or *dave* retrieve the message from the queue OUT using the sample application **amqsget**.

Sonuçlar

Messages sent by *alice* or *bob* to the input queue IN are encrypted allowing only IBM Integration Bus to read it. IBM Integration Bus yalnızca *alice* ve *bob* iletilerinden gelen iletileri kabul eder ve diğer kişileri reddeder. The accepted messages are appropriately processed, then signed and encrypted with *Cecil's* and *Dave's* keys before being put onto the output queue OUT. Yalnızca *cecil* ve *dave* okuma yeteneğine sahiptir; IBM Integration Bus tarafından imzalanmamış iletiler reddedilir.

Advanced Message Security ile Managed File Transferkomutunu kullanma

Bu senaryoda, bir Managed File Transferaracılığıyla gönderilen veriler için ileti gizliliği sağlamak üzere Advanced Message Security ' un nasıl yapılandırılacağı açıklanmaktadır.

Başlamadan önce

Korumak istediğiniz Managed File Transfer tarafından kullanılan kuyrukları bulunduran IBM MQ kurulumunda Advanced Message Security bileşeniniz olduğundan emin olun.

Managed File Transfer aracılarınız bağ tanımları moduna bağlanıyorsa, GSKit bileşeninin yerel kuruluşlarında kurulu olduğundan da emin olun.

Bu görev hakkında

İki Managed File Transfer aracısı arasında veri aktarımı kesintiye uğratıldığında, aktarımın yönetilmesi için kullanılan temeldeki IBM MQ kuyruklarında gizli veriler korunmasız kalabilir. Bu senaryoda, Managed File Transfer kuyruklarında bu tür verileri korumak için Advanced Message Security olanağının nasıl yapılandırılacağı ve kullanılacağı açıklanır.

Bu senaryoda, Senaryonun genelsenaryoda açıklandığı gibi, tek bir kuyruk yöneticisini paylaşan basit bir topolojiyi iki Managed File Transfer kuyruklarıyla ve iki aracıdan (AGENT1 ve AGENT2) paylaşan basit bir topoloji olarak değerlendiriyoruz. Her iki aracı da, bağ tanımları kipinde ya da istemci kipinde aynı şekilde bağlanır.

1. Sertifika yaratılması

Başlamadan önce

This scenario uses a simple model where a user ftagent in a group FTAGENTS is used to run the Managed File Transfer Agent processes. Kendi kullanıcı ve grup adlarınızı kullanıyorsanız, komutları uygun şekilde değiştirin.

Bu görev hakkında

Advanced Message Security , korunan kuyruklardaki iletileri imzalamak ve/ya da şifrelemek için genel anahtar şifrelemesi kullanır.

Not:

- Managed File Transfer aracılarınız bağ tanımları kipinde çalışıyorsa, bir CMS (Şifreleme İletisi Sözdizimi) anahtar deposu oluşturmak için kullandığınız komutlar, **Hızlı Başlangıç Kılavuzu** ' nda (Windows ya da UNIX) ayrıntılı bir şekilde bulunur. Platformunuz için.
- Managed File Transfer aracılarınız istemci kipinde çalışıyorsa, bir JKS (Java Anahtar Deposu) yaratmak için gereksinim duyacak komutlar “Quick Start Guide for AMS with Java clients” sayfa 572' ta ayrıntılı olarak açıklanmıştır.

Yordam

1. Create a self-signed certificate to identify the user ftagent as detailed in the appropriate Quick Start Guide.
   Aşağıdaki gibi bir Ayırt Edici Ad (DN) kullanın:

```
CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>
```

2. Anahtar deposunun konumunu ve bu anahtar içindeki sertifikayı uygun Hızlı Başlangıç Kılavuzu içinde ayrıntılı şekilde tanımlamak için bir `keystore.conf` dosyası oluşturun.

2. İleti korumasının yapılandırılması

Bu görev hakkında

You should define a security policy for the data queue used by AGENT2, using the **setmqspl** command. Bu senaryoda, aynı kullanıcı her iki aracıyı da başlatmak için kullanılır; dolayısıyla, imzalayanın ve alıcı ayırt edici adı aynı olur ve oluşturduğumuz sertifikayla eşleşir.

Yordam

1. Shut down the Managed File Transfer agents in preparation for protection using the **fteStopAgent** command.
2. SYSTEM.FTE.DATA.AGENT2 kuyruğunu korumak için bir güvenlik ilkesi yaratın.

```
setmqspl -m hubQM -p SYSTEM.FTE.DATA.AGENT2 -s SHA1 -a "CN=ftagent, OU=MFT,
O=<organisation>, L=<location>, ST=<state>, C=<country>"
-e AES128 -r "CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>"
```

3. Managed File Transfer Agent işlemini çalıştıran kullanıcının, sistem ilke kuyruğuna göz atma ve hata kuyruğuna ileti koyma erişimine sahip olduğundan emin olun.

```
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. **fteStartAgent** komutunu kullanarak Managed File Transfer aracılarınızı yeniden başlatın.
5. **fteListAgents** komutunu kullanarak aracılarınızın başarılı bir şekilde yeniden başlatıldığını ve aracıların READY durumunda olduğunu doğrulamayı onaylayın.

Sonuçlar

You are now able to submit transfers from AGENT1 to AGENT2, and the file contents will be transmitted securely between the two agents.

Advanced Message Security Kuruluşa genel bakış

Advanced Message Security bileşenini çeşitli platformlarda kurun.

Bu görev hakkında

Kuruluş yordamlarıyla ilgili bilgi için Installing Advanced Message Security on multiplatforms ve Installing Advanced Message Security on z/OSbaşlıklı konuya bakın.

İlgili görevler

kaldırmaAdvanced Message Security

z/OS z/OSüzerinde denetleme

z/OS içinAdvanced Message Security (AMS), ilke korumalı kuyruklar üzerindeki uygulamalara göre isteğe bağlı olarak gerçekleştirilen işlemlerin denetlenmesine yönelik bir araç sağlar. When enabled, IBM System Management Facility (SMF) audit records are generated for the success and failure of these operations on policy-protected queues. Denetlenen işlemler arasında MQPUT, MQPUT1ve MQGET yer alır.

Auditing is disabled by default, however, you can activate auditing by configuring _AMS_SMF_TYPE and _AMS_SMF_AUDIT in the configured Language Environment® _CEE_ENVFILE file for the AMS address space. Daha fazla bilgi için Advanced Message Securityiçin yordam oluşturmabaşlıklı konuya

bakın. _AMS_SMF_TYPE değişkeni, SMF kayıt tipini belirtmek için kullanılır ve 128 ile 255 arasında bir sayıdır. Bir SMF kayıt tipi 180 'tür, ancak zorunlu değildir. Denetim, 0 değeri belirlenerek geçersiz kılındı. _AMS_SMF_AUDIT değişkeni, başarılı olan işlemler için denetim kayıtlarının oluşturulup oluşturulmayacağını, başarısız olan işlemlerin ya da her ikisinin de yapılandırılacağını yapılandırır. The auditing options can also be dynamically changed while AMS is active using operator commands. Daha fazla bilgi için bkz. Operating Advanced Message Security.

SMF kaydı alt tipler kullanılarak tanımlanır, alt tip 1 genel denetleme olayı olarak tanımlanır. SMF kaydı, işlenmekte olan istekle ilgili tüm verileri içerir.

SMF kaydı CSQ0KSMF makrosu ile eşlenir (makro adındaki sıfır değeri), bu kayıt hedef kitaplık SCSQMACS ' de sağlanır. SMF verileri için veri azaltma programları yazıyorsanız, bu eşleme makrosunu SMF art işleme yordamlarının geliştirilmesine ve uyarlamasına yardımcı olacak şekilde ekleyebilirsiniz.

z/OSiçin Advanced Message Security tarafından üretilen SMF kayıtlarında veriler bölümler halinde düzenlenir. Kayıt şunlardan oluşur:

- standart bir SMF üstbilgisi
- a header extension defined by Advanced Message Security for z/OS
- bir ürün bölümü
- bir veri bölümü

The product section of the SMF record is always present in the records produced by Advanced Message Security for z/OS. Veri bölümü, alt tipe göre değişiklik gösterir. Şu anda bir alt tip tanımlıdır ve bu nedenle tek bir veri bölümü kullanılır.

SMF, z/OS System Management Facilitis manüel (SA22-7630) adlı elkitabında açıklanmaktadır. Geçerli kayıt tipleri, sisteminizin PARMLIB veri kümesinin SMFPRMxx üyesinde açıklanmıştır. Ek bilgi için SMF belgelerine bakın.

Advanced Message Security denetleme raporu üreteci (CSQ0USMF)

Advanced Message Security for z/OS provides an audit report generator tool called CSQ0USMF which is provided in the installation SCSQAUTH library. Sample JCL to run the CSQ0USMF utility called CSQ40RSM is provided in the installation library SCSQPROC.

CSQ0USMF yardımcı programını çalıştırmadan önce, SMF tipi 180 kayıtlarının sistem SMF veri kümelerinden sıralı bir veri kümesine atılması gerekir. Örnek olarak, bu JCL SMF tipi 180 kayıtlarını bir SMF veri kümesinden döküyor ve bunları bir hedef veri kümesine aktarıyor:

```
//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))
/*
```

Kuruluş tarafından kullanılan gerçek SMF veri kümesi adlarını doğrulamanız gerekir. Dökümü alınan kayıtlar için belirlenen hedef veri kümesi VBS ' nin kayıt biçimine ve 32760 kayıt uzunluğuna sahip olmalıdır.

Not: If SMF logstreams are being used, you must use program IFASMFDL to dump a logstream out to a sequential dataset. Kullanılan JCL örneğine ilişkin Tip 116 SMF kayıtlarının işlenmesi başlıklı konuya bakın.

Daha sonra, hedef veri kümesi, bir AMS denetleme raporu üretmek için CSQ0USMF yardımcı programına giriş olarak kullanılabilir. Örneğin:

```
//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
//
```

CSQ0USMF programı, Çizelge 97 sayfa 584içinde listelenen isteğe bağlı iki parametreyi kabul eder:

Çizelge 97. CSQ0USMF isteğe bağlı parametreler

Değiştirge	Değer	Tanım
SMFTYPE	nnn	Denetleme raporu için geçerli SMF kayıt tipi. CSQ0USMF programı, yalnızca rapor oluştururken SMFTYPE değeriyle eşleşen SMF kayıtlarını kullanır. SMFTYPE değerini belirtmezseniz, varsayılan değer olan 180 kullanılır.
M	qmgr	Denetleme raporu için geçerli olan IBM MQ kuyruk yöneticisi adı. -M parametresini belirlemezseniz, denetleme raporu, SMFIN veri kümesinde gösterilen tüm kuyruk yöneticilerine ilişkin tüm denetleme kayıtlarını içerir.

Anahtar depolarının ve sertifikaların kullanılması

IBM MQ uygulamalarına şeffaf bir şifreleme koruması sağlamak için Advanced Message Security , anahtar deposu dosyasını, genel anahtar sertifikalarını ve bir özel anahtarın depolandığı anahtar deposu dosyasını kullanır. z/OSüzerinde, bir anahtar deposu dosyası yerine bir SAF anahtar halkası kullanılır.

Advanced Message Security' ta kullanıcılar ve uygulamalar, genel anahtar altyapısı (PKI) tanıtıcılarıyla temsil edilir. Bu kimlik tipi, iletileri imzalamak ve şifrelemek için kullanılır. PKI kimliği, konunun **ayırt edici adı (DN)** alanı tarafından, imzalanmış ve şifrelenmiş iletilerle ilişkili bir sertifikada temsil edilir. Bir kullanıcı ya da uygulamanın iletilerini şifrelemek için, sertifikaların ve ilişkili özel ve genel anahtarların saklandığı anahtar deposu dosyasına erişmeleri gerekir.

Windows ve UNIX üzerinde anahtar deposunun konumu, varsayılan olarak `keystore.conf` olan anahtar deposu yapılandırma dosyasında bulunur. Her Advanced Message Security kullanıcısının bir anahtar deposu dosyasını işaret eden anahtar deposu yapılandırma dosyasına sahip olması gerekir. Advanced Message Security , anahtar deposu dosyalarının şu biçimini kabul eder: `.kdb`, `.jceks`, `.jks`.

`keystore.conf` dosyasının varsayılan konumu şöyledir:

- IBM i UNIX UNIX ve IBM iüzerinde: `$HOME/.mqs/keystore.conf`
- Windows Windowsüzerinde: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

  Not: Birden çok sürücü harfi kullanılabiliyorsa, Windows ' taki yol, sürücü harfini belirtmeli ve bu harfle ilgili bir değer belirtmelidir.

Belirtilen anahtar deposu dosya adı ve yeri kullanıyorsanız, aşağıdaki komutları kullanmalısınız:

- Javaiçin: `java -D`*`MQS_KEYSTORE_CONF=path/filename app_name`*
- C İstemcisi ve Sunucusu için:
  - UNIX and Linuxüzerinde: `export MQS_KEYSTORE_CONF=`*`path/filename`*
  - Windowsüzerinde: `set MQS_KEYSTORE_CONF=`*`path\filename`*

İlgili kavramlar

“AMS içinde gönderen ayırt edici adları” sayfa 610
Gönderen ayırt edici adları (DN), bir kuyruğa ileti yerleştirme yetkisi olan kullanıcıları tanımlar. Bir gönderen, iletiyi kuyruğa yerleştirmeden önce, iletiyi imzalamak için sertifikasını kullanır.

“AMSiçindeki alıcı ayırt edici adları” sayfa 611
Alıcı ayırt edici adları (DN), kuyruktan ileti alma yetkisi olan kullanıcıları tanımlar.

AMS için anahtar deposu yapılandırma dosyasının (keystore.conf) yapısı

Anahtar deposu yapılandırma dosyası (`keystore.conf`), Advanced Message Security ' yi uygun anahtar deposunun konumunu işaret eder.

Aşağıdaki yapılandırma dosyası tiplerinin her birinin bir öneki vardır:

CMS
Sertifika Yönetimi Sistemi, yapılandırma girişlerine şu öneki eklenir: `cms.`

PKCS#11
Genel Anahtar Şifreleme Standardı #11, yapılandırma girdilerine şu öneki eklenir: `pkcs11.`

IBM i **PEM**
Gizlilik Gelişmiş Posta biçimi, yapılandırma girdilerinin öneki: `pem.`

JKS
Java KeyStore, yapılandırma girişlerine şu öneki eklenir: `jks.`

JCEKS
Java Şifreleme Şifrelemesi KeyStore, yapılandırma girişlerine şu öneki eklenir: `jceks.`

z/OS V 9.1.0 MQ Adv. VUE **JCERACFKS**
Java Cryptographic Encryption RACF keyring KeyStore, yapılandırma girişlerine şu öneki eklenir: `jceracfks`.

Önemli: IBM MQ 9.0 ' den `JCEKS.provider` ve `JKS.provider` değerleri yoksayılır. Bouncy Castle sağlayıcısı, kullanılan JRE tarafından sağlanan JCE/JCE ile birlikte kullanılır. Daha fazla bilgi için bkz “AMSileIBM dışı JRE ' ler için destek” sayfa 588.

Anahtar depolarına ilişkin örnek yapılar:

CMS

```
cms.keystore = /dir/keystore_file
cms.certificate = certificate_label
```

PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
```

IBM i 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
```

V 9.1.0 Java JCERACFKS

```
jceracfks.keystore = safkeyring://user/keyring
jceracfks.certificate = certificate_label
```

Çizelge 98. Her yapılanış kütüğü tipi için gereken değiştirgelerin özeti

Parametreler	Zorunlu	Yapılandırma dosyası tipi			
		V 9.1.0 Java (JKS, JCEKS ve JCERACFKS)	IBM i PEM	PKCS#11	CMS
keystore	✓	✓			✓
IBM i private	✓		IBM i ✓		
IBM i public	✓		IBM i ✓		
IBM i password	✓		IBM i ✓		
library	✓			✓	
certificate	✓	✓		✓	✓
token	✓			✓	
token_pin	✓			✓	
secondary_keystore	✓			✓	
encrypted		✓			
keystore_pass	✓	✓			
key_pass		✓			
provider		✓			

simgesini kullanarak yorum ekleyebileceğinizi unutmayın.

Yapılanış kütüğü değiştirgeleri aşağıdaki gibi tanımlanır:

keystore
Yalnızca CMS ve Java yapılandırması. CMS, JKS ve JCEKS yapılanışına ilişkin anahtar deposu dosyasının yolu.

z/OS V 9.1.0 MQ Adv. VUE JCERACFKS yapılandırması için RACF anahtarlığı URI 'si.

Önemli:

- Anahtar deposu dosyasının yolu dosya uzantısını içermemelidir.
- z/OS V 9.1.0 MQ Adv. VUE RACF anahtarlığı URI 'si şu biçimde olmalıdır:

```
safkeyring://user/keyring
```

Burada:

– *user* , anahtarlık sahibinin kullanıcı kimliğidir
– *keyring* , anahtarlık adıdır.

IBM i **private**
Yalnızca PEM yapılandırması. PEM biçiminde özel anahtar ve sertifika içeren bir dosyanın dosya adı.

IBM i **public**
Yalnızca PEM yapılandırması. PEM biçiminde güvenilen genel sertifikaları içeren bir dosyanın adı.

IBM i **password**
Yalnızca PEM yapılandırması. Şifrelenmiş bir özel anahtarın şifresini çözmek için kullanılan parola.

library
Yalnızca PKCS#11 . PKCS#11 kitaplığının yol adı.

certificate
CMS, PKCS#11 ve Java yapılandırması. Sertifika etiketi.

token
Yalnızca PKCS#11 . Simge etiketi.

token_pin
Yalnızca PKCS#11 . Belirtecin kilidini açmak için PIN girin.

secondary_keystore
Yalnızca PKCS#11 . `.kdb` uzantısı olmadan sağlanan ve PKCS #11 simgesinde saklanan sertifikaların gerektirdiği tutturucu sertifikalarını (kök sertifikaları) içeren CMS anahtar deposunun yol adı.
İkincil anahtar deposu, güven zincirinde ara düzey sertifikaların yanı sıra gizlilik güvenlik ilkesinde tanımlanan alıcı sertifikalarını da içerebilir. Bu CMS anahtar deposuyla birlikte, ikincil anahtar deposuyla aynı dizinde bulunması gereken bir parola saklama dosyası da bulunmalıdır.

encrypted
Yalnızca Java yapılandırması. Parolanın durumu.

keystore_pass
Yalnızca Java yapılandırması. Anahtar deposu dosyasının parolası.

Not:

- CMS anahtar deposu için AMS parola saklama dosyalarına dayanır (`.sth`); JKS ve JCEKS, hem sertifika hem de kullanıcının özel anahtarı için bir parola gerektirebilir.
- **Önemli:** Parolaların düz metin biçiminde saklanması güvenlik riski oluşturur.

z/OS V 9.1.0 MQ Adv. VUE

Not: Erişim bir parola tarafından denetlenmediği için `jceracfks` için yoksayıldı.

key_pass
Yalnızca Java yapılandırması. Kullanıcının özel anahtarının parolası.

Önemli: Parolaların düz metin biçiminde saklanması güvenlik riski oluşturur.

z/OS V 9.1.0 MQ Adv. VUE

Not: Erişim bir parola tarafından denetlenmediği için `jceracfks` için yoksayıldı.

`provider`
Yalnızca Java yapılandırması. Anahtar deposu sertifikasının gerektirdiği şifreleme algoritmalarını uygulayan Java güvenlik sağlayıcısı.

Önemli: Anahtar deposunda saklanan bilgiler, IBM MQkullanılarak gönderilen güvenli veri akışı için çok önemlidir. Güvenlik yöneticileri bu dosyalara dosya izinleri atarken özellikle dikkat etmelidirler.

`keystore.conf` dosyası örneği:

```
# Native AMS application configuration
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

# Java AMS application configurationjceks.keystore = c:/Documents and Settings/Alice/
AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passw0rd
jceks.key_pass = passw0rd
jceks.provider = IBMJCE
```

İlgili görevler

“Protecting passwords in Java” sayfa 601
Anahtar deposu ve özel anahtar parolalarının düz metin olarak saklanması,securitygüvenlik riski oluşturur. Böylece, Advanced Message Security , anahtar deposu dosyasında bulunan bir kullanıcının anahtarını kullanarak bu parolaları karıştırabilecek bir araç sağlar.

AMSileIBM dışı JRE ' ler için destek

IBM MQ classes for Java and IBM MQ classes for JMS support Advanced Message Security operation when running with non-IBM JREs.

Advanced Message Security (AMS), Şifreleme İletisi Sözdizimi (CMS)uygular. CMS sözdizimi, isteğe bağlı ileti içeriğini dijital olarak imzalamak, özetlemek, doğrulamak ya da şifrelemek için kullanılır.

IBM MQ 9.0'tan, IBM MQ classes for Java ve IBM MQ classes for JMS ' deki Advanced Message Security desteği, CMS ' yi desteklemek için açık kaynak Bouncy Castle paketlerini kullanır. Bu, bu sınıflarınIBM dışı JRE ' lerle çalışırken Advanced Message Security işlemini destekleyebileceğinin anlamına gelir.

Before IBM MQ 9.0, Advanced Message Security was not supported in non-IBM JREs in Java clients. IBM MQ classes for Java ve IBM MQ classes for JMS ' deAdvanced Message Security desteği, özellikle Java Cryptography Extensions (JCE) uygulamasının IBM uygulaması tarafından sağlanan CMS desteğine bağımlılar. Bu kısıtlama nedeniyle, işlevsellik yalnızca Java JCE sağlayıcısını içeren bir Java runtime environment (JRE) kullanılırken kullanılabilir.

Solaris Importantly, support on platforms such as Solaris required a hybrid JRE, that is, the standard JRE for the platform with additional elements provided by IBM. Özellikle, platform için standart JRE tarafından sağlanan JCE sağlayıcısından çok IBM JCE sağlayıcısı gereklidir.

Bouncy Castle JAR dosyalarına ilişkin konum ve sürüm numaralandırması

IBM dışı JRE ' ler için destek için gereken Bouncy Castle JAR dosyaları, IBM MQ classes for Java ve IBM MQ classes for JMS kuruluş paketinin bir parçası olarak dahil edilir.

Kullanılan Bouncy Castle JAR dosyaları şu dosyalardır:

"Bouncy Castle" işlemleri için temel olan sağlayıcı JAR dosyası.
Bu JAR dosyası `bcprov-jdk15on.jar`olarak adlandırılır.

Advanced Message Securitytarafından kullanılan CMS işlemlerine ilişkin desteği içeren "PKIX" JAR dosyası.

Bu JAR dosyası `bcpkix-jdk15on.jar`olarak adlandırılır.

V 9.1.0.9 **Diğer Bouncy Castle JAR dosyaları tarafından kullanılan sınıfların bulunduğu "util" JAR dosyası.**

Bu JAR dosyası `bcutil-jdk15on.jar`olarak adlandırılır.

Bağımlılıklar

IBM MQ 9.1 ve sonraki sınıflar, IBM JRE 'leri ve Oracle JRE' leri ile sınanmiştir. Ayrıca, herhangi bir J2SE-compliant JRE ' nin altında da başarılı bir şekilde çalıştırılırlar. Ancak, aşağıdaki bağımlılıkları dikkate almalısınız:

- Advanced Message Security yapılandırmasında herhangi bir değişiklik yok.
- Bouncy Castle sınıfları yalnızca CMS işlemleri için kullanılır. Diğer tüm güvenlikle ilgili işlemler; örneğin, anahtar deposu erişimi, verilerin gerçek şifrelenmesi ve imza sağlama toplamlarının hesaplanması, JRE tarafından sağlanan işlevselliği kullanır.

  Önemli: Bu nedenle, kullanılan JRE ' nin bir JCE sağlayıcısı somutlaması içermesi gerekir.
- Bazı *güçlü* şifreleme algoritmalarını kullanmak için, JRE ' nin JCE somutlaması için *sınırsız* ilke dosyalarını kurmanız gerekebilir.

  Ek ayrıntılar için JRE belgelerine bakın.
- If you have enabled Java security:
  - Bouncy Castle sınıflarının bir güvenlik sağlayıcısı olarak kullanılabilmesi için uygulamaya `java.security.SecurityPermissioninsertProvider.BC` ekleyin.
  - Grant `java.security.AllPermission` to the Bouncy Castle JAR files, which are:

    V 9.1.0.9 *mq_install_dir*`/java/lib/bcutil-jdk15on.jar`
    mq_install_dir`/java/lib/bcpkix-jdk15on.jar`
    mq_install_dir`/java/lib/bcprov-jdk15on.jar`

İlgili kavramlar

JMS için IBM MQ sınıfları için kurulu olan nedir

Java için IBM MQ sınıfları için kurulu olan

Multi Message Channel Agent (MCA) etkileşimi

MCA etkileşimi, IBM MQ altında çalışan bir kuyruk yöneticisinin, sunucu bağlantı kanalları için ilkeleri seçmeli olarak etkinleştirebilmesini sağlar.

MCA ' nın başlatılması, AMS dışında kalan müşterilerin hala bir kuyruk yöneticisine ve iletilerin şifrelenmesine ve şifrelerinin çözülmesine bağlı olmaya devam etmesine olanak sağlar.

MCA interception is intended to provide AMS capability when AMS cannot be enabled at the client. MCA 'yı algılamayı ve AMS' in geçerli kılındığı bir istemcinin, uygulama almak için sorunlu olabilecek iletilerin iki kez korunmasını sağladığına dikkat edin. Daha fazla bilgi için bkz “İstemcide Advanced Message Security devre dışı bırakılması” sayfa 592.

Not: MCA dinlemeleri AMQP ya da MQTT kanalları için desteklenmez.

Anahtar deposu yapılanış dosyası

By default, the keystore configuration file for MCA interception is `keystore.conf` and is located in the `.mqs` directory in the HOME directory path of the user who started the queue manager or the listener. Anahtar deposu aynı zamanda MQS_KEYSTORE_CONF ortam değişkeni kullanılarak da yapılandırılabilir. AMS anahtar deposunu yapılandırma hakkında daha fazla bilgi için bkz. “Anahtar depolarının ve sertifikaların kullanılması” sayfa 584.

MCA ' yı yeniden başlatma özelliğini etkinleştirmek için, anahtar deposu yapılandırma dosyasında kullanmak istediğiniz bir kanal adını sağlamanız gerekir. MCA Interception için yalnızca bir cms anahtar deposu tipi kullanılabilir.

MCA ' nın başlangıcından oluşan bir kuruluş örneği için bkz. “Advanced Message Security MCA başlangıcı örneği” sayfa 590 .

Uyarı: Örneğin, SSL ve SSLPEER ya da CHLAUTH TYPE (SSLPEERMAP) kullanarak, yalnızca yetkili istemcilerin bağlanabilmesini ve bu yeteneği kullanabilmesini sağlamak için, seçilen kanallarda istemci kimlik doğrulamasını ve şifrelemeyi tamamlamanız gerekir.

IBM i

Kuruluşunuz IBM ikullanıyorsa ve sertifikanızı imzalamak için bir ticari Sertifika Yetkilisi (CA) seçtiyseniz, Digital Certificate Manager , PEM (Privacy-Enhanced Mail) biçiminde bir sertifika isteği yaratır. İsteğinizi seçtiğiniz CA ' ya iletmelisiniz.

Bunu yapmak için, `channelname`eiçinde belirtilen kanala ilişkin doğru sertifikayı seçmek için aşağıdaki komutu kullanmanız gerekir:

```
pem.certificate.channel.channelname
```

Advanced Message Security MCA başlangıcı örneği

AMS MCA ' yı nasıl kurabildiğinizi gösteren örnek bir görev.

Başlamadan önce

Uyarı: Örneğin, SSL ve SSLPEER ya da CHLAUTH TYPE (SSLPEERMAP) kullanarak, yalnızca yetkili istemcilerin bağlanabilmesini ve bu yeteneği kullanabilmesini sağlamak için, seçilen kanallarda istemci kimlik doğrulamasını ve şifrelemeyi tamamlamanız gerekir.

Kuruluşunuz IBM ikullanıyorsa ve sertifikanızı imzalamak için bir ticari Sertifika Yetkilisi (CA) seçtiyseniz, Digital Certificate Manager , PEM (Privacy-Enhanced Mail) biçiminde bir sertifika isteği yaratır. İsteğinizi seçtiğiniz CA ' ya iletmelisiniz.

Bu görev hakkında

Bu görev, sisteminizi MCA ' yı (MCA) algılamayı kullanacak şekilde kurma işlemini ve daha sonra, kuruluşu doğrulamanız için size yol sağlar.

Not: IBM WebSphere MQ 7.5öncesinde, AMS , uygulamaları korumak üzere ayrı olarak kurulmuş ve durdurucular için gerekli olan bir eklenti üründü. From IBM WebSphere MQ 7.5 onwards, the interceptors are automatically included and dynamically enabled in the MQ client and server runtime environments. Bu MCA ' lar arası örnekte, kesiciler kanalın sunucu ucunda sağlanır ve daha eski bir istemci çalıştırma zamanı (12. Adımda), kanala korunmayan iletileri MCA dinlemeleri tarafından korunabilecek şekilde görülebilmesi için kullanılır. Bu örnek bir IBM WebSphere MQ 7.5 ya da daha sonraki bir istemci kullansaydı, iletinin iki kez korunmasına neden olur; çünkü MQ istemcisi yürütme ortamı algılayıcısı ve MCA dinleyici, iletiyi MQ' da olduğu gibi korumalıdır.

Uyarı: Koddaki `userID` kodunu kullanıcı kimliğinizle değiştirin.

Yordam

1. Anahtar veri tabanını ve sertifikaları, bir kabuk komut dosyası yaratmak için aşağıdaki komutları kullanarak yaratın.

   Ayrıca, **INSTLOC** ve **KEYSTORELOC** ' yi değiştirin ya da gerekli komutları çalıştırın. bobiçin sertifika oluşturmasına gerek kalmayabileceğini unutmayın.

```
INSTLOC=/opt/mq90
KEYSTORELOC=/home/testusr/ssl/ams1
```

```
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64

gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd
-label bob_cert  -dn "cn=bob,O=IBM,c=IN"  -default_cert yes
```

2. Her bir kullanıcının diğerini başarıyla tanıması için, iki anahtar veritabanı arasındaki sertifikaları paylaşın.

   Görev 5 'te açıklanan yöntemi kullanmanız önemlidir. Hızlı Başlama Kılavuzu (Windows ya da UNIX) içindeSertifikaları Paylaşma .
3. Şu yapılandırmayla `keystore.conf` oluşturun: `Keystore.conf location: /home/userID/ssl/ams1/`

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

4. Kuyruk yöneticisi yarat ve başlat AMSQMGR1
5. *kapı* 14567 ve *denetim* QMGRile bir dinleyici tanımlayın
6. Kanal yetkisini geçersiz kılın ya da kanal yetkisi için kuralları belirleyin.

   Ek bilgi için SET CHLAUTH başlıklı konuya bakın.
7. Kuyruk yöneticisini durdurun.
8. Anahtar deposunu ayarla:

```
export MQS_KEYSTORE_CONF=/home/userID/ssl/ams1/keystore.conf
```

9. Kuyruk yöneticisini aynı kabukta başlatın.
10. Güvenlik ilkesini ayarlayın ve aşağıdakileri doğrulayın:

```
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
```

    Ek bilgi için setmqspl ve dspmqspl başlıklı konuya bakın.
11. Kanal yapılandırmasını ayarlayın:

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. **amqsputc** komutunu, bir MCA algılayıcısı 'nı otomatik olarak etkinleştirmeyen bir MQ istemcisinden çalıştırın; örneğin, IBM WebSphere MQ 7.1 ya da önceki bir istemci. Aşağıdaki iki iletiyi yerleştirin:

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

13. Güvenlik ilkesini kaldırın ve sonucu doğrulayın:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

14. Browse the queue from your IBM MQ 9.0 installation:

```
/opt/mq90/samp/bin/amqsbcg TESTQ AMSQMGR1
```

    Göz atma çıkışı, iletileri şifrelenmiş biçimde gösterir.
15. Güvenlik ilkesini ayarlayın ve sonucu doğrulayın:

```
setmqspl -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqspl -m AMSQMGR1
```

16. **amqsgetc** ' u IBM MQ 9.0 kurulumundan çalıştırın:

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

İlgili görevler

“Quick Start Guide for AMS with Java clients” sayfa 572
İstemci bağ tanımlarını kullanarak bağlanan Java uygulamaları için ileti güvenliği sağlamak üzere Advanced Message Security olanağını hızlı bir şekilde yapılandırmak için bu kılavuzu kullanın. Tamamladığınız zaman, kullanıcı kimliklerini doğrulamak ve kuyruk yöneticiniz için imzalama/şifreleme ilkeleri tanımlamanız için bir anahtar deposu yaratmış olacaktır.

İlgili başvurular

“Bilinen AMSsınırlamaları” sayfa 544
There are a number of IBM MQ options that are either not supported, or have limitations for Advanced Message Security.

İstemcide Advanced Message Security devre dışı bırakılması

Ürünün önceki bir sürümünden bir kuyruk yöneticisine bağlanmak için bir IBM WebSphere MQ 7.5 ya da daha sonraki bir istemci kullanıyorsanız, IBM MQ Advanced Message Security (AMS) olanağını devre dışı bırakmanız gerekir. 2085 （MQRC_UNKNOWN_OBJECT_NAME） hatası raporlanır.

Bu görev hakkında

IBM WebSphere MQ 7.5, IBM MQ Advanced Message Security (AMS), bir IBM MQ istemcisinde otomatik olarak etkinleştirilir ve istemci varsayılan olarak, kuyruk yöneticisinde nesnelere ilişkin güvenlik ilkelerini denetmeye çalışır. Ancak, ürünün önceki sürümlerindeki sunucular (örneğin, IBM WebSphere MQ 7.1), AMS etkin değildir ve bu, 2085 （MQRC_UNKNOWN_OBJECT_NAME） hatasının raporlanmasına neden olur.

Bu hata bildirilirse, ürünün önceki bir sürümünden bir kuyruk yöneticisine bağlanmaya çalıştığınızda, AMS ' yi aşağıdaki gibi devre dışı bırakabilirsiniz:

- Java istemcileri için aşağıdaki yöntemlerden birini kullanın:
  - Bir ortam değişkeni AMQ_DISABLE_CLIENT_AMS ayarlanarak.
  - By setting the Java system property com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - DisableClientAMS özelliğini kullanarak, `mqclient.ini` dosyasındaki **Security** stanza altında.
- C istemcileri için aşağıdaki yöntemlerden birini kullanın:
  - Bir ortam değişkeni MQS_DISABLE_ALL_INTERCEPT ayarını tanımlayarak.
  - DisableClientAMS özelliğini kullanarak, `mqclient.ini` dosyasındaki **Security** stanza altında.

Not: IBM WebSphere MQ 7.5' ta AMQ_DISABLE_CLIENT_AMS ortam değişkenini de kullanabilirsiniz. C istemcileri için. IBM MQ 8.0' tan, C istemcileri için artık AMQ_DISABLE_client_ams ortam değişkenini kullanamazsınız. Bunun yerine MQS_DISABLE_ALL_INTERCEPT ortam değişkenini kullanmanız gerekir.

Yordam

- İstemcide AMS ' i devre dışı bırakmak için aşağıdaki seçeneklerden birini kullanın:

  AMQ_DISABLE_CLIENT_AMS ortam değişkeni
  Bu değişkeni aşağıdaki durumlarda ayarlamanız gerekir:
  - IBM Java Runtime Environment (JRE) dışında Java Runtime Environment (JRE) kullanıyorsanız
  - IBM WebSphere MQ 7.5 ya da daha sonraki bir sürümünü IBM MQ classes for JMS ya da IBM MQ classes for Java istemcisini kullanıyorsanız.

  AMQ_DISABLE_CLIENT_AMS ortam değişkenini yaratın ve uygulamanın çalıştırıldığı ortamda TRUE olarak ayarlayın. Örneğin:

  ```
  export AMQ_DISABLE_CLIENT_AMS=TRUE
  ```

Java sistem özelliği com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS

IBM MQ classes for JMS ve IBM MQ classes for Java istemcileri için, com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS Java sistem özelliğini, Java uygulaması için TRUE değerine ayarlayabilirsiniz.

Örneğin, Java komutu çağrıldığında Java sistem özelliğini bir `-D` seçeneği olarak ayarlayabilirsiniz:

```
java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/
com.ibm.mqjms.jar  my.java.applicationClass
```

Diğer bir seçenek olarak, uygulama bu dosyayı kullanıyorsa, JMS yapılandırma dosyası (`jms.config`) içinde Java sistem özelliğini belirtebilirsiniz.

MQS_DISABLE_ALL_INTERCEPT ortam değişkeni

You need to set this variable if you are using IBM MQ 8.0 or later with native clients and you need to disable AMS at the client.

MQS_DISABLE_ALL_INTERCEPT ortam değişkenini yaratın ve istemcinin çalıştığı ortamdaki TRUE olarak ayarlayın. Örneğin:

```
export MQS_DISABLE_ALL_INTERCEPT =TRUE
```

Yalnızca C istemcileri için MQS_DISABLE_ALL_INTERCEPT ortam değişkenini kullanabilirsiniz. Java istemcileri için, bunun yerine AMQ_DISABLE_CLIENT_AMS ortam değişkenini kullanmanız gerekir.

`mqclient.ini` dosyasındaki`DisableClientAMS` özelliği

Bu seçeneği, IBM MQ classes for JMS ve IBM MQ classes for Java istemcileri için ve C istemcileri için kullanabilirsiniz.

Add the property name `DisableClientAMS` under the **`Security`** stanza the `mqclient.ini` file as shown in the following example:

```
Security:
DisableClientAMS=Yes
```

Ayrıca, aşağıdaki örnekte gösterildiği gibi AMS özelliğini de etkinleştirebilirsiniz:

```
Security:
DisableClientAMS=No
```

Sonraki adım

AMS korumalı kuyrukların açılmasına ilişkin sorunlar hakkında daha fazla bilgi için bkz. Problems opening protected queues when using AMS with JMS.

İlgili kavramlar

“Message Channel Agent (MCA) etkileşimi” sayfa 589
MCA etkileşimi, IBM MQ altında çalışan bir kuyruk yöneticisinin, sunucu bağlantı kanalları için ilkeleri seçmeli olarak etkinleştirebilmesini sağlar.

İlgili görevler

Yapılandırma dosyası kullanarak istemci yapılandırılması

İlgili başvurular

IBM MQ classes for JMS yapılandırma dosyası

AMSiçin sertifika gereksinimleri

Sertifikaların Advanced Message Securityile kullanılabilmesi için RSA genel anahtarı olmalıdır.

Farklı genel anahtar tipleri ve bunların nasıl yaratılacağı hakkında daha fazla bilgi için bkz. “IBM MQ içinde dijital sertifikalar ve CipherSpec uyumluluğu” sayfa 42.

Anahtar kullanım uzantıları

Anahtar kullanım uzantıları, bir sertifikenin kullanılabileceği şekilde ek sınırlamalar sağlar.

In Advanced Message Security, the key usage of X.509 v3 certificates must be set in accordance with the RFC 5280 specification.

Koruma bütünlüğü kalitesi için, sertifika anahtarı kullanım uzantıları ayarlandıysa, bu ayarın en az iki tanesini de içermesi gerekir:

- **nonRepudiation**
- **digitalSignature**

Koruma gizliliği kalitesi için, sertifika anahtarı kullanım uzantıları ayarlandıysa, bu ayarın aşağıdakileri içermesi gerekir:

- **keyEncipherment**

Koruma gizliliği kalitesi için, sertifika anahtarı kullanım uzantıları ayarlandıysa, bu ayarın aşağıdakileri içermesi gerekir:

- **dataEncipherment**

Genişletilmiş anahtar kullanımı, anahtar kullanım uzantılarını daha fazla yeniden sınırlar. Tüm koruma nitelikleri için, sertifika genişletilmiş anahtar kullanımı ayarlandıysa, küme aşağıdakileri içermelidir:

- **emailProtection**

İlgili kavramlar

"Koruma kalitesi" sayfa 613
Advanced Message Security veri koruma ilkeleri, bir koruma kalitesi (QOP) anlamına gelir.

AMSiçinde sertifika geçerlilik denetimi yöntemleri

Kuyruklarınıza ilişkin iletilerin güvenlik standartlarını yerine getirmeyen sertifikalar kullanılarak korunmamasını, iptal etmek ve reddetmek için Advanced Message Security ' u kullanabilirsiniz.

AMS , bir sertifikanın geçerliliğini Online Certificate Status Protocol (OCSP) ya da sertifika iptal listesi (CRL) kullanarak doğrulamanıza olanak tanır.

AMS , OCSP ya da CRL denetimi için yapılandırılabilir ya da her ikisi için de yapılandırılabilir. Her iki yöntem de etkinleştirilmişse, performans nedenlerinden dolayı, AMS önce iptal durumu için OCSP kullanır. Bir sertifikana ilişkin iptal durumu OCSP denetiminden sonra belirlenmezse, AMS CRL denetimini kullanır.

Hem OCSP, hem de CRL denetlerinin varsayılan olarak etkinleştirildiğini unutmayın.

İlgili kavramlar

"AMSiçinde çevrimiçi Sertifika Durumu Protokolü (OCSP)" sayfa 594
OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü), bir sertifikanın iptal edilip edilmediğini belirler ve sertifikanın güvenilir olup olmadığını belirlemeye yardımcı olur. OCSP varsayılan olarak etkindir.

"Certificate revocation lists (CRLs) in AMS" sayfa 596
CRL ' ler, Sertifika Yetkilisi (CA) tarafından, artık çeşitli nedenlerle güvenilmediği için, özel anahtar kaybedilmiş ya da tehlikeye atıldığı sertifikaların bir listesini içerir.

AMSiçinde çevrimiçi Sertifika Durumu Protokolü (OCSP)

OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü), bir sertifikanın iptal edilip edilmediğini belirler ve sertifikanın güvenilir olup olmadığını belirlemeye yardımcı olur. OCSP varsayılan olarak etkindir.

OCSP, IBM i syems üzerinde desteklenmez.

OCSP denetimini Advanced Message Security' in yerli dinlemeleri için etkinleştirme

Advanced Message Security içinde çevrimiçi Sertifika Durumu Protokolü (OCSP) denetimi, kullanılmakta olan sertifikalardaki bilgilere dayalı olarak varsayılan olarak etkinleştirilir.

Yordam

Anahtar deposu yapılanış kütüğüne aşağıdaki seçenekleri ekleyin:

Not: Tüm OCSP stanza isteğe bağlıdır ve bağımsız olarak belirtilebilir.

Seçenek	Tanım
`ocsp.enable=off`	Denetlenmekte olan sertifikanda, OCSP Responder 'ın bulunduğu yerin URI 'sini içeren bir PKIX_AD_OCSP erişim yöntemi içeren bir Yetkili Bilgi Erişimi (AIA) Uzantısına sahip olup olmadığını denetleyerek OCSP denetimini etkinleştirin. Olası değerler: on ya da `off`.
`ocsp.url=`*`responder_URL`*	OCSP yanıtlayıcıya ilişkin URL adresi. Bu seçenek çıkarılırsa, AIA dışı OCSP denetimi devre dışı bırakılır.
`ocsp.http.proxy.host=`*`OCSP_proxy`*	OCSP yetkili sunucusunun URL adresi. Bu seçenek çıkarılırsa, AIA dışı çevrimiçi sertifika denetimleri için bir yetkili sunucu kullanılmaz.
`ocsp.http.proxy.port=`*`port_number`*	OCSP yetkili sunucusunun kapı numarası. Bu seçenek atılırsa, varsayılan kapı 8080 kullanılır.
`ocsp.nonce.generation=on/off`	OCSP sorgulanırken nonce oluşturun. Varsayılan değer `off`değeridir.
`ocsp.nonce.check=on/off`	OCSP 'den yanıt aldıktan sonra nonce' yi denetleyin. Varsayılan değer `off`değeridir.
`ocsp.nonce.size=8`	Byte olarak nonce boyutu.
`ocsp.http.get=on/off`	İstek yönteminiz olarak HTTP GET değerini belirtin. Bu seçenek `off`olarak ayarlandıysa, HTTP POST kullanılır. Varsayılan değer `off`' dir.
`ocsp.max_response_size=20480`	Bayt cinsinden sağlanan OCSP yanıtlayıcısından yanıt boyutu üst sınırı.
`ocsp.cache_size=100`	İç OCSP yanıtı önbelleğe almayı geçerli kılın ve önbellek girişi sayısı sınırını belirleyin.
`ocsp.timeout=30`	Sunucu yanıtı için saniye cinsinden bekleme süresi (saniye olarak), Advanced Message Security zamanaşımına neden olur.
`ocsp.unknown=ACCEPT`	Bir zamanaşımı süresi içinde bir OCSP sunucusuna ulaşılamadığında bu davranışı tanımlar. Olası değerler: • `ACCEPT` Sertifikalara izin verir • `WARN` Sertifikana izin verir ve bir uyarı günlüğe kaydeder • `REJECT` sertifikenin kullanılmasını önler ve bir hatayı günlüğe kaydeder

Enabling OCSP checking in Java in AMS
To enable OCSP checking for Java in Advanced Message Security, modify the `java.security` file or the keystore configuration file.

Bu görev hakkında

There are two ways of enabling OCSP checking in Advanced Message Security:

java.securitykullanılıyor
Sertifikanız bir Authority Information Access (AIA) sertifika uzantısını içerip içermediğini denetleyin.

Yordam

1. AIA ayarlanmadıysa ya da sertifikanızı geçersiz kılmak istiyorsanız, `$JAVA_HOME/lib/security/java.security` dosyasını aşağıdaki özelliklerle düzenleyin:

   ```
   ocsp.responderURL=http://url.to.responder:port
   ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
   ```

   ve oCSP denetimini etkinleştirmek için aşağıdaki satırı kullanarak `$JAVA_HOME/lib/security/java.security` dosyasını düzenleyin:

   ```
   ocsp.enable=true
   ```

2. AIA ayarlandıysa, OCSP denetimini etkinleştirmek için `$JAVA_HOME/lib/security/java.security` dosyasını aşağıdaki satırla düzenleyin:

   ```
   ocsp.enable=true
   ```

Sonraki adım

If you are using Java Security Manager, too complete the configuration, add the following Java permission to `lib/security/java.policy`

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

keystore.confolanağının kullanılması

Yordam

Yapılanış kütüğüne aşağıdaki özniteliği ekleyin:

```
ocsp.enable=true
```

Önemli: Bu özniteliğin yapılandırma dosyasında ayarlanması java.security ayarlarını geçersiz kılar.

Sonraki adım

Yapılandırmayı tamamlamak için aşağıdaki Java izinlerini `lib/security/java.policy`' e ekleyin:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Certificate revocation lists (CRLs) in AMS

CRL ' ler, Sertifika Yetkilisi (CA) tarafından, artık çeşitli nedenlerle güvenilmediği için, özel anahtar kaybedilmiş ya da tehlikeye atıldığı sertifikaların bir listesini içerir.

To validate certificates, Advanced Message Security constructs a certificate chain that consists of the signer's certificate and the certificate authority's (CA's) certificate chain up to a trust anchor. Güven çıpası, bir sertifikanın güvenini göstermek için kullanılan güvenilir bir sertifika ya da güvenilen kök sertifika içeren güvenilir bir anahtar deposu dosyasıdır. AMS , bir PKIX doğrulama algoritması kullanarak sertifika yolunu doğrular. Zincir oluşturulduğunda ve doğrulandığında, AMS , son varlık sertifikasında anahtar kullanım uzantısının var olup olmadığını denetleyerek, geçerli tarihe karşı zincirdeki her bir sertifikana ilişkin sorunun geçerliliğini ve son kullanma tarihini doğrulayan sertifika doğrulamasını tamamladığında, sertifika geçerliliğini tamamlar. Uzantı sertifiya eklenirse, AMS **digitalSignature** ya da **nonRepudiation** da ayarlanıp ayarlanmadığını doğrular. Bunlar değillerse, `MQRC_SECURITY_ERROR` raporlanır ve günlüğe kaydedilir. Daha sonra, AMS kütüklerden CRL 'leri ya da yapılanış kütüğünde belirtilen değerlere bağlı olarak LDAP' den CRL ' leri karşıdan yükler. Yalnızca DER biçiminde kodlanan CRL ' ler AMStarafından desteklenir. Anahtar deposu yapılandırma dosyasında CRL ile ilgili bir yapılandırma bulunmazsa, AMS , CRL geçerlilik denetimi gerçekleştirmez. Her CA sertifikası için AMS , CRL 'yi bulmak için CA' nın Ayırt Edici Adları 'nı kullanarak CRL 'ler için LDAP' i sorgular. LDAP sorgularında aşağıdaki öznitelikler yer alır:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Not: `deltaRevocationList` , yalnızca dağıtım noktaları olarak belirtildiğinde desteklenir.

Sertifika geçerlilik denetimi ve sertifika iptal listesi desteğinin yerel engellilerde geçerli kılınması
Anahtar deposu yapılandırma dosyasını, Advanced Message Security ' un LDAP (Lightweight Directory Access Protocol; Temel Dizin Erişimi Protokolü) sunucusundan yükleyebilmesi için anahtar deposu yapılandırma dosyasını değiştirmelisiniz.

Bu görev hakkında

IBM i Yerel algılayıcılarda sertifika geçerlilik denetimi ve sertifika iptal listesi desteğinin etkinleştirilmesi, IBM iüzerinde Advanced Message Security için desteklenmez.

Yordam

Yapılanış kütüğüne aşağıdaki seçenekleri ekleyin:

Not: Tüm CRL stanza isteğe bağlıdır ve bağımsız olarak belirtilebilir.

Seçenek	Tanım
`crl.ldap.host=`*`host_name`*	LDAP sunucusu anasistem adı.
`crl.ldap.port=`*`port_number`*	LDAP sunucusu kapı numarası. En çok 11 sunucu belirleyebilirsiniz. LDAP bağlantısı hatası durumunda, hata durumunda yedek sisteme geçiş işlemini sağlamak için birden çok LDAP anasistemi kullanılır. Tüm LDAP sunucularının eşlemeler olması ve aynı verileri içermesi beklenir. AMS Java algılayıcısı bir LDAP sunucusuna başarıyla bağlandığında, sağlanan geri kalan sunuculardan CRL ' ler aşağı yüklenmeye çalışmaz.
`crl.cdp=off`	Sertifikalardaki CRLDistributionPoints uzantılarını denetlemek ya da kullanmak için bu seçeneği kullanın.

Seçenek	Tanım
`crl.ldap.version=3`	LDAP iletişim kuralı sürüm numarası. Olası değerler: 2 ya da 3.
`crl.ldap.user=cn=`*`username`*	LDAP sunucusunda oturum açın. Bu değer belirlenmezse, LDAP ' deki CRL öznitelikleri dünya tarafından okunabilir olmalıdır
`crl.ldap.pass=`*`password`*	LDAP sunucusuna ilişkin parola.
`crl.ldap.cache_lifetime=0`	LDAP önbelleği kullanım süresi (saniye). Olası değerler: 0-86400.
`crl.ldap.cache_size=50`	LDAP önbelleği büyüklüğü. Bu seçenek yalnızca `crl.ldap.cache_lifetime` değeri `0`' den büyükse belirtilebilir.
`crl.http.proxy.host=some.host.com`	CDP CRL alma işlemi için http yetkili sunucu kapısı.
`crl.http.proxy.port=8080`	Http yetkili sunucusu kapı numarası.
`crl.http.max_response_size=204800`	GSKit tarafından kabul edilen bir HTTP sunucusundan alınabilen, bayt cinsinden bayt cinsinden maksimum CRL boyutu.
`crl.http.timeout=30`	Sunucu yanıtı için saniye cinsinden bekleme süresi (saniye olarak), daha sonra AMS zamanaşımına neden olur.
`crl.http.cache_size=0`	HTTP önbellek boyutu (bayt).
`crl.unknown=ACCEPT`	Bir CRL sunucusuna zamanaşımı süresi içinde ulaşılamadığında davranışı tanımlar. Olası değerler: • `ACCEPT` Sertifikalara izin verir • `WARN` Sertifikana izin verir ve bir uyarı günlüğe kaydeder • `REJECT` sertifikenin kullanılmasını önler ve bir hatayı günlüğe kaydeder

Enabling certificate revocation list support in Java in AMS
Advanced Message Security'ta CRL desteğini etkinleştirmek için, anahtar deposu yapılandırma dosyasını, AMS ' un CRL 'leri Lightweight Directory Access Protocol (LDAP) sunucusundan CRL' yi karşıdan yüklemesine ve java.security dosyasını yapılandırmasına izin verecek şekilde değiştirmelisiniz.

Yordam

1. Yapılanış kütüğüne aşağıdaki seçenekleri ekleyin:

Üstbilgi	Tanım
`crl.ldap.host=`*`host_name`*	LDAP anasistem adı.

Üstbilgi	Tanım
`crl.ldap.port=`*`port_number`*	LDAP sunucusu kapı numarası. En çok 11 sunucu belirleyebilirsiniz. LDAP bağlantısı hatası durumunda, hata durumunda yedek sisteme geçiş işlemini sağlamak için birden çok LDAP anasistemi kullanılır. Tüm LDAP sunucularının eşlemeler olması ve aynı verileri içermesi beklenir. AMS Java algılayıcısı bir LDAP sunucusuna başarıyla bağlandığında, sağlanan geri kalan sunuculardan CRL ' ler aşağı yüklenmeye çalışmaz. Java , `crl.ldap.user` ve crl.ldaworldp.pass değerlerini kullanmaz. LDAP sunucusuna bağlanırken kullanıcı ve parola kullanmaz. Sonuç olarak, LDAP ' taki CRL öznitelikleri dünya tarafından okunabilen bir değer olmalıdır.
`crl.cdp=on/off`	Sertifikalardaki CRLDistributionPoints uzantılarını denetlemek ya da kullanmak için bu seçeneği kullanın.

2. `JRE/lib/security/java.security` dosyasını aşağıdaki özelliklerle değiştirin:

Özellik Adı	Tanım
`com.ibm.security.enableCRLDP`	Bu özellik şu değerleri alır: `true`, `false`. `true`olarak ayarlanmışsa, sertifika iptal denetimi yaparken CRL 'ler sertifikanın CRL dağıtım noktaları uzantısından URL' yi kullanarak konumlandırılır. `false` olarak ayarlanmışsa ya da ayarlanmazsa, CRL dağıtım noktaları uzantısını kullanarak CRL ' yi kontrol edin.
`ibm.security.certpath.ldap.cache.lifetime`	Bu özellik, LDAP CertStore ' ın bellek önbelleğindeki girdilerin kullanım ömrünü saniye cinsinden ayarlamak için kullanılabilir. 0 değeri önbelleği devre dışı bırakır; -1 ise sınırsız ömür anlamına gelir. Ayarlanmazsa, varsayılan kullanım süresi 30 saniyedir.
`com.ibm.security.enableAIAEXT`	Bu özellik şu değerleri alır: `true`, `false`. `true`değerine ayarlanmışsa, oluşturulmakta olan sertifika yolunun sertifikalarında bulunan herhangi bir Yetkili Bilgi Erişimi uzantısı, LDAP URI ' lerini içerip içermediklerini belirlemek için incelenir. Bulunan her LDAP URI 'si için, bir LDAPCertStore nesnesi yaratılır ve sertifika yolunu oluşturmak için gerekli olan diğer sertifikaları bulmak için kullanılan CertStores derleme nesnesine eklenir. `false` olarak ayarlanmışsa ya da ayarlanmamış ise, ek LDAPCertStore nesneleri yaratılmaz.

z/OS *Enabling certificate revocation lists (CRLs) on z/OS*

Advanced Message Security , veri iletilerini korumak için kullanılan dijital sertifikaların Sertifika İptal Listesi 'ni (CRL) destekler.

Bu görev hakkında

Etkinleştirildiğinde, Advanced Message Security , iletiler bir gizlilik koruma kuyruğuna konduğunda alıcı sertifikalarını doğrulayacak ve korunan bir kuyruktan (bütünlük ya da gizlilik) iletiler alındığında gönderen sertifikalarını doğrulayacak. Bu durumda geçerlilik denetimi, ilgili sertifikaların ilgili bir CRL ' de kaydedilmemiş olduğunu doğrulamayı içerir.

Advanced Message Security , gönderen ve alıcı sertifikalarını doğrulamak için IBM System SSL hizmetlerini kullanır. Sistem SSL sertifikası geçerlilik denetimiyle ilgili ayrıntılı belgeler, z/OS Cryptographic Services System Secure Sockets Layer Programming elkitabında (SC24-5901) bulunabilir.

CRL denetimini geçerli kılınmak üzere, AMS adres alanına ilişkin başlatılan görev JCL ' de CRLFILE GG aracılığıyla bir CRL konfigürasyon dosyasının yerini belirtiyorsunuz. Özelleştirilebilen örnek bir CRL yapılandırma dosyası *thlqual*.SCSQPROC (CSQ40CRL) içinde sağlanır. Bu dosyada izin verilen ayarlar aşağıdaki gibidir:

Çizelge 99. Advanced Message Security CRL yapılandırma değişkenleri

Değişken	**Geçerli değerler**	**Tanım**
crl.ldap.host[.n]	*anasistem adı -ya da-anasistem adı: kapı*	Sertifika veren sertifikalarınızın CRL ' lerini barındıran LDAP sunucunuzun ipaddr/ anasistem adı. LDAP sunucunuz için bir kapı numarası belirtmezseniz, crl.ldap.port tarafından belirlenen kapı numarası kullanılır.
crl.ldap.port	*port*	LDAP sunucunuzun TCP/IP kapı numarası.
crl.ldap.user	*ldap_user*	LDAP sunucusuna bağlanırken kullanılacak LDAP kullanıcı adı.
crl.ldap.pass	*ldap_password*	crl.ldap.userile ilişkili LDAP parolası.

Aşağıdaki gibi birden çok LDAP sunucusu anasistem adı ve bağlantı noktası belirtebilirsiniz:

```
crl.ldap.host.1 = hostname -or hostname:port
crl.ldap.host.2 = hostname -or hostname:port
crl.ldap.host.3 = hostname -or hostname:port
```

En çok 10 anasistem adı belirleyebilirsiniz. LDAP sunucularınız için bir kapı numarası belirlemezseniz, crl.ldap.port tarafından belirlenen kapı numarası kullanılır. Her LDAP sunucusu, erişim için aynı crl.ldap.user/password birleşimini kullanmalıdır.

CRLFILE DD belirtildiğinde, Advanced Message Security adres alanı kullanıma hazırlama sırasında yapılandırma yüklenir ve CRL denetimi etkinleştirilir. CRLFILE DD belirtilmediyse ya da CRL yapılandırma dosyası kullanılamaz ya da geçersiz, CRL denetimi devre dışı bırakılır.

AMS , aşağıdaki gibi IBM System SSL sertifika doğrulama hizmetlerini kullanarak bir CRL denetimi gerçekleştirir:

Çizelge 100. Advanced Message Security CRL denetimleri		
İşlem	**Koruma kalitesi**	**Onay Belgesi (ler) alındı**
PUT	Gizlilik	Alıcı (lar)
GET	Bütünlük/Gizlilik	Gönderen

Bir ileti işlemi CRL denetimini geçemezse, Advanced Message Security aşağıdaki işlemleri gerçekleştirir:

Çizelge 101. Advanced Message Security CRL denetimi hatası davranışı	
İşlem	**CRL denetimi hatası**
PUT	İleti hedef kuyruğa konmaz. Uygulamaya MQCC_FAILED 'ın tamamlanma kodu ve MQRC_SECURITY_ERROR neden kodu döndürülemedi.
GET	İleti hedef kuyruktan kaldırılır ve sistem koruma hatası kuyruğuna taşınır. Uygulamaya MQCC_FAILED 'ın tamamlanma kodu ve MQRC_SECURITY_ERROR neden kodu döndürülemedi.

z/OS içinAMS , CRL ve güvenilirlik denetimini içeren sertifikaların geçerliliğini denetlemek için IBM System SSL hizmetlerini kullanır. IBM System SSL, CRL denetmenin çalışmasını ılımlı olarak GSK_CRL_SECURITY_LEVELL ortam değişkeni sağlar. Örneğin:

```
GSK_CRL_SECURITY_LEVEL=MEDIUM
```

Bu değişken, z/OS Cryptographic Services System Secure Sockets Layer Programming ile belgelenir. Geçerli atamalar şunlardır:

- LOW-Certificate geçerlilik denetimi, LDAP sunucusunda iletişim kurulamazsa başarısız olur.
- MEDIUM-Certificate geçerlilik denetimi, LDAP sunucusunun iletişim kurulmasını gerektirir, ancak CRL ' nin tanımlanmasını gerektirmez.
- HIGH-Certificate geçerlilik denetimi, LDAP sunucusunun kontalabilir olmasını ve bir CRL ' nin tanımlanmasını gerektirir.

IBM Sistem SSL varsayılanı MEDIUM ' dur. Bu değişkeni, AMS adres alanı için başlatılan görev JCL ' de ENVARS DD aracılığıyla belirlenen konfigürasyon dosyasında ayarlayabilirsiniz. Örnek bir ortam değişkeni yapılandırma dosyası, *thlqual*.SCSQPROC (CSQ40ENV) içinde sağlanır.

Not: İlgili Sertifika Yetkilileri için, ilgili LDAP hizmetlerinin kullanılabilmesini ve CRL girişlerini korumak için yöneticilerin sorumluluğundadır.

Protecting passwords in Java

Anahtar deposu ve özel anahtar parolalarının düz metin olarak saklanması,securitygüvenlik riski oluşturur. Böylece, Advanced Message Security , anahtar deposu dosyasında bulunan bir kullanıcının anahtarını kullanarak bu parolaları karıştırabilecek bir araç sağlar.

Başlamadan önce

`keystore.conf` dosya sahibi, dosyayı yalnızca dosya sahibinin okuma yetkisine sahip olduğundan emin olmalıdır. Bu bölümde açıklanan parolaların korunması yalnızca ek bir koruma ölçüsüdür.

Yordam

1. Anahtar deposu ve kullanıcılar etiketine yol eklemek için `keystore.conf` dosyalarını düzenleyin.

```
jceks.keystore = c:/Documents and Setting/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.provider = IBMJCE
```

2. Aracı çalıştırmak için şu komutu verin:

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
private_key_password
```

Şifrelenmiş parolalara sahip bir çıkış oluşturulur ve `keystore.conf` dosyasına kopyalanabilir.

Çıktıyı `keystore.conf` dosyasına otomatik olarak kopyalamak için, şunları çalıştırın:

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
private_key_password >> ~/path_to_keystore/keystore.conf
```

Not:

Çeşitli platformlarda `keystore.conf` ' un varsayılan konumlarının bir listesi için bkz. “Anahtar depolarının ve sertifikaların kullanılması” sayfa 584.

Örnek

Bu tür çıktılara bir örnek:

```
#Fri Jul 30 15:20:29 CEST 2010
jceks.key_pass=MMXh997n5ZOr8uRlJmc5qity9MN2CggGBMKCDxdbn1AyPklvdgTsOLG6X3C1YT7oDzwaqZFlOR4t\r\nm
Zsc7JGAx8nqqxLnAucdGn0NWo6xnjZB1n501YGol2k/
PhaQHhFXKMAU9dKg0f8djOtCAOlX4ETe\r\nfYl9LBUt2wk87uM7dSs\=
jceks.keystore_pass=OIdeayBnSCfLG4cFuxEVrk6SYyAsdSPpDqgPf16s9s1M04cqZjNbhgjoA2EXonudHZHH+4s2drvQ
\r\nCUvQgu9GuaBMJK2F2OjtHJJ1Y4BVeLW2c2okgawo/
W2J1AdUYKkJ0raYTkDouLaTYTQeulyG0xIl\r\niD2si1xUCxhYvvyhbbY\=
jceks.encrypted=yes
```

z/OS Using certificates on z/OS

Bu görev hakkında

Advanced Message Security , üç koruma düzeyi uygular: bütünlük, gizlilik ve gizlilik.

Bir bütünlük ilkesiyle, iletiler orijinalinin özel anahtarı (MQPUT ' un yaptığı uygulama) kullanılarak imzalanır. Bütünlük, ileti değişikliklerinin algılanmasını sağlar, ancak ileti metninin kendisi şifrelenmez.

Gizlilik ilkesiyle, ileti kuyruğa konduğunda şifrelenir. İleti, bir simetrik anahtar kullanılarak şifrelenir ve ilgili Advanced Message Security ilkesinde belirtilen bir algoritma kullanılarak şifrelenir. Simetrik anahtarın kendisi, her alıcının genel anahtarı ile şifrelenir (MQGET işlemi yapan uygulama). Genel anahtarlar, anahtarlık anahtarlarında saklanan sertifikalarla ilişkilendirilir.

Gizlilik ilkesiyle, iletiler imzalanır ve şifrelenir.

Gizlilik ile korunan bir ileti, bir MQGET işlemi yapan bir alıcı uygulaması tarafından kuyruğa alındığında, iletinin şifresi çözülmelidir. Alıcının ortak anahtarı kullanılarak şifrelendiği için, alıcının anahtar halkasında bulunan özel anahtarı kullanılarak şifresi çözülmalıdır.

z/OS *SAF anahtarı halkalarının kullanımı*

Advanced Message Security (AMS), imzalama ve şifreleme için gereken sertifikaları tanımlamak ve yönetmek için z/OS SAF anahtar halkası hizmetlerinin kullanılmasını sağlar. Security products that are functionally equivalent to RACF may be used instead of RACF if they provide the same level of support.

Anahtar halkalarının verimli kullanılması, sertifikaları yönetmek için gereken yönetimi azaltabilir.

Bir sertifika oluşturulduktan (ya da içe aktarıldıktan sonra), erişilebilir hale gelmek için bir anahtarlık (ya da içe aktarıma) bağlanmalıdır. Aynı sertifika birden çok anahtarlık çağrısına bağlanabilir.

Advanced Message Security , iki anahtar halkası kümesini kullanır. Bir küme, ileti gönderen ya da alan kullanıcı kimliklerinin sahip olduğu anahtar halkalardan oluşur. Her anahtar halkası, sahip olan kullanıcı kimliğinin sertifikasıyla ilişkili özel anahtarı içerir. Her sertifikana ilişkin özel anahtar, bütünlük korumalı ya da gizlilik korumalı kuyruklar için iletileri imzalamak için kullanılır. Ayrıca, ileti alınırken gizlilik korumalı ya da gizlilik korumalı kuyruklardan iletilerin şifresini çözmek için de kullanılır.

Diğer küme, AMS adres alanı kullanıcısının iyeliğindeki tek anahtarlı bir yüzüktür. Bu belge, ileti kaynağı ve alıcıların sertifikalarını doğrulamak için gerekli olan CA sertifikalarını imzalama zincirini içerir.

Gizlilik ya da gizlilik koruması kullanıldığında, AMS adres alanı kullanıcısının sahip olduğu anahtarlık, ileti alıcılarının sertifikalarını da içerir. Bu sertifikalardaki ortak anahtarlar, ileti korumalı kuyruğa konduğunda ileti verilerini şifrelemek için kullanılan simetrik anahtarı şifrelemek için kullanılır. Bu iletiler alındığında, ilgili alıcıların özel anahtarı, daha sonra ileti verilerinin şifresini çözmek için kullanılan simetrik anahtarın şifresini çözmek için kullanılır.

Advanced Message Security , sertifikalar ve özel anahtarlar aranırken **drq.ams.keyring** anahtar halkası adını kullanır. Bu, hem kullanıcı, hem de AMS adres alanı anahtar halkalarının vakaları olur.

Sertifikaların ve anahtarlık verilerinin ve bunların veri korumasındaki rollerinin ayrıntılı açıklamaları için Sertifikalarla ilgili işlemlerin özetibaşlıklı konuya bakın.

İmzalama ve şifre çözme için kullanılan özel anahtarda herhangi bir etiket olabilir, ancak varsayılan sertifika olarak bağlanmalıdır.

Dijital sertifikalar ve anahtar halkaları öncelikle RACDCERT komutu kullanılarak RACF ' ta yönetilir.

Sertifikalar, etiketler ve RACDCERT komutu hakkında daha fazla bilgi için bkz. *z/OS: Security Server RACF Command Language Reference* ve *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *RACDCERT komutuna erişim yetkisi verme*

Authorization to use the RACDCERT command is a post-installation task that should have been completed by your z/OS system programmer. Bu görev, Advanced Message Security güvenlik denetimcisine ilgili izinlerin verilmesini içerir.

As a summary, these commands are needed to allow access to the RACF RACDCERT command:

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

Bu örnekte, *admin* güvenlik denetimcinizin kullanıcı kimliğini ya da RACDCERT komutunu kullanmak istediğiniz herhangi bir kullanıcıyı belirtir.

z/OS *Sertifikaların ve anahtar halkalarının oluşturulması*

This section documents the steps required to create the certificates and key rings necessary for z/OS users of Advanced Message Security (AMS), using a RACF Certificate Authority (CA).

z/OSüzerinde Advanced Message Security kullanılırken, sertifikalarla ilgili sorunların çözülmesi

Anahtar depolarında sertifikalarla ve eksik girdilerle ilgili sorunlar yaşıyorsanız, bir GSKIT izlemesi etkinleştirebilirsiniz.

AMS başlatılan görev yordamında ENVARS DD tarafından gönderme yapılan dosyada şunu ekleyin:

```
GSK_TRACE_FILE=/u/... /gsktrace
GSK_TRACE=0xff
```

Ek bilgi için Ortam değişkenleri başlıklı konuya bakın.

Anahtar deposuna erişim her erişim için, veriler GSK_TRACE_FILEiçinde belirtilen izleme dosyasına yazılır.

İzleme dosyasını biçimlemek için şu komutu kullanın:

```
gsktrace inputtrace file > output_file
```

Senaryo

Gerekli adımları açıklamak için bir gönderme uygulamasının senaryosu ve alma uygulaması kullanılır.

Aşağıdaki örneklerde user1 , bir iletinin kökenidir ve user2 alıcı olur. Advanced Message Security adres alanının kullanıcı kimliği: WMQAMSD.

Burada gösterilen örneklerdeki tüm komutlar, yönetici kullanıcı kimliği admintarafından ISPF seçenek 6 'dan yayınlanır.

z/OS *Yerel Sertifika Yetkilisi sertifikasının tanımlanması*

CA ' niz olarak RACF kullanıyorsanız, önceden yapmadıysanız, bir sertifika yetkilisi sertifikası oluşturmanız gerekir. Burada gösterilen komut bir sertifika yetkilisi (ya da imzalayıcı) sertifikası yaratır. Bu örnek, Advanced Message Security kullanıcılarının ve uygulamalarının kimliğini yansıtan sonraki sertifikalar yaratılırken kullanılacak AMSCA adlı bir sertifika yaratır.

Bu komut, kuruluşunuzda kullanılan adlandırma yapısını ve kuralları yansıtmak için özel olarak SUBJECTSDNolarak değiştirilebilir.

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

Not: Bu yerel sertifika yetkilisi sertifikasıyla imzalanan sertifikalar, RACDCERT LIST komutuyla listelenirken CN=AMSCA, O=ibm, C=us yayıncısının bir yayınını gösterir.

z/OS *Özel anahtarla sayısal sertifika yaratılması*

Her bir Advanced Message Security kullanıcısı için özel bir anahtara sahip bir dijital sertifika oluşturulmalıdır. Burada gösterilen örnekte, RACDCERT komutları, AMSCA etiketiyle tanımlanan yerel CA sertifikasıyla imzalanmış user1 ve user2için sertifikalar oluşturmak için kullanılır.

```
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
```

Sertifiya TRUST özniteliğini eklemek için RACDCERT ALTER komutu gereklidir. Bir sertifika ilk olarak bu yordam kullanılarak yaratılırsa, imzalama sertifikasından farklı bir geçerli tarih aralığı vardır. Sonuç olarak, RACF bu değeri NOTRUST olarak işaretler. Bu, sertifikanının kullanılmaması anlamına gelir. TRUST özniteliğini ayarlamak için RACDCERT ALTER komutunu kullanın.

Advanced Message Securitytarafından kullanılan sertifikalar için KEYUSAGE öznitelikleri TOKALAŞMA, DATAENCRYPT ve DOCSIGN belirtilmeli.

Çizelge 102. RACDCERT KEYUSAGE değerleri ve göstergeleri	
KEYUSAGE Değeri	**Göstergeler Kümesi**
SAK	digitalSignature ve keyEncipherment
VERİEN	dataEncipherment
DOCSIGN	nonRepudiation
CERTSIGN	keyCertİşareti ve cRLSign

z/OS *RACF anahtar halkalarının oluşturulması*

Burada gösterilen komutlar, RACFtanımlı kullanıcı kimlikleri user1, user2ve Advanced Message Security adres alanı görevi kullanıcısı WMQAMSD için bir anahtarlık yaratır. Anahtarlık adı Advanced Message Security tarafından sabittir ve tırnak işaretleri olmadan, gösterildiği gibi kodlanmalıdır. Ad, büyük ve küçük harfe duyarlıdır.

```
RACDCERT ID(user1) ADDRING(drq.ams.keyring)
RACDCERT ID(user2) ADDRING(drq.ams.keyring)
RACDCERT ID(WMQAMSD) ADDRING(drq.ams.keyring)
```

z/OS *Sertifikaların anahtarlık halkalarına bağlanması*

Kullanıcı ve CA sertifikalarını anahtarlık halkalarına bağlayın:

```
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))
```

Şifre çözme için kullanılan özel anahtarı içeren sertifikanda, kullanıcının anahtar halkasına varsayılan sertifika olarak bağlanmalıdır.

RACDCERT USAGE (SITE) özniteliği, özel anahtarın anahtarlık içinde erişilebilir olmasını önler, RACDCERT KULLANıMı (PERSONAL) özniteliği, varsa, özel anahtarın kullanılmasına olanak sağlar. User2's certificate must be connected to the Advanced Message Security address space key ring because its public key is needed to encrypt messages as they are put to the queue. KULLANıM (SITE), user2' nin özel anahtarının kullanımını sınırlar.

AMSCA etiketli CERTAUTH sertifikasının Advanced Message Security adres alanı anahtarlık belgesine bağlanması gerekir; bu, ileti kaynağı olan user1sertifikasını imzalamak için kullanıldığından, bu ringle bağlantı kurulmalıdır. user1' in imzalama sertifikasının geçerliliğini denetlemek için kullanılır.

z/OS *Anahtarlık doğrulaması*

Anahtar halkası, tüm komutların girildikten sonra burada gösterildiği gibi görünmelidir:

```
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
```

Tek tek sertifikalar listelenirken, halka ilişkilendirmesini de gösterir.

```
RACDCERT ID(user2) LIST(label('user2'))
Digital certificate information for user USER2:

***
Label: user2
Certificate ID: 2QfH8Pny9/LzpKKFmfFA
Status: TRUST
Start Date: 2010/05/03 22:59:53
End Date:  2011/05/04 22:59:52
Serial Number:>15<:
Issuer's Name:>OU=AMSCA.O=ibm.C=us<:
Subject's Name:>CN=user2.O=ibm.C=us<:
Key Usage: HANDSHAKE, DATAENCRYPT, DOCSIGN
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
Ring Owner: USER2
Ring:>drq.ams.keyring<:
Ring Owner: WMQAMSD
Ring:>drq.ams.keyring<:
```

Başarımı artırmak için, AMS adres alanıyla ilişkilendirilen drq.ams.keyring içeriğinin, adres alanının ömrü için önbelleğe alınması gerekir. Anahtar halkadaki değişiklikler otomatik olarak yürürlüğe girmez. Sistem yöneticisi önbelleği aşağıdaki gibi yenileyebilir:

- Kuyruk yöneticisi durduruluyor ve yeniden başlatılıyor.
- z/OS MODIFY komutunu kullanma:

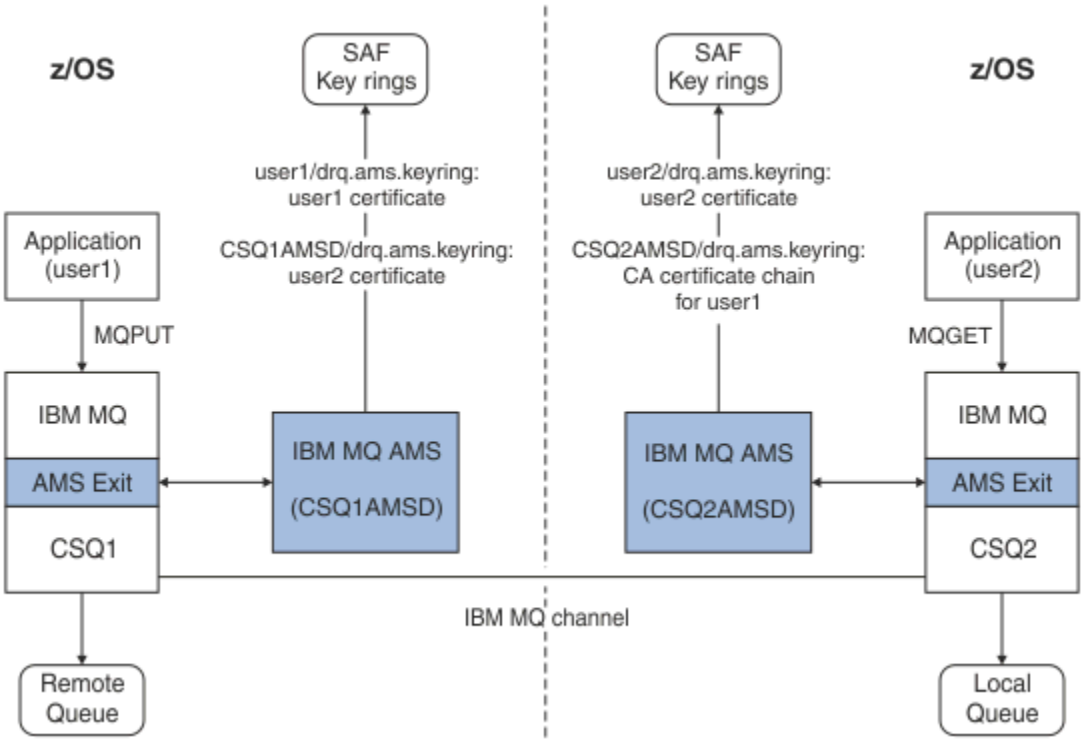
```
F qmgrAMSM,REFRESH KEYRING
```

İlgili görevler

ÇalışırkenAdvanced Message Security

z/OS *Sertifikan ilgili işlemlerin özeti*

Şekil 35 sayfa 607 , uygulama ve ilgili sertifikalar gönderme ve alma arasındaki ilişkileri gösterir. Bu senaryoda, gizliliğin bir veri koruma ilkesi kullanılarak iki z/OS kuyruk yöneticisi arasında uzaktan kuyruğa alma işlemi yer aldığından, bu senaryo, uzaktan kuyruğa alma işlemini içerir. Şekil 35 sayfa 607içinde "AMS", " Advanced Message Security".



Şekil 35. Uygulama ve sertifika ilişkileri

In this diagram, an application running as 'user1' puts a message to a remote queue managed by queue manager CSQ1, intended to be retrieved by an application running as 'user2' from a local queue managed by queue manager CSQ2. The diagram assumes an Advanced Message Security policy of privacy, which means the message is both signed and encrypted.

Advanced Message Security , bir put ortaya çıktığında iletiyi yakalar ve ileti verilerini şifrelemek için kullanılan bir simetrik anahtarı şifrelemek için user2' nin sertifikasını (AMS adres alanı kullanıcısının anahtar halkasında saklanır) kullanır.

user2' nin sertifikasının AMS adres alanı kullanıcı anahtarı halkasına USAGE (SITE) seçeneğiyle bağlandığısına dikkat edin. Bu, AMS adres alanı kullanıcısının sertifiya ve genel anahtara erişebileceği, ancak özel anahtarı kullanmadığı anlamına gelir.

On the receiving end, Advanced Message Security intercepts the get issued by user2, and uses user2's certificate to decrypt the symmetric key so that it can decrypt the message data. Daha sonra, AMS adres alanı kullanıcısının anahtar halkasında saklanan user1sertifikasının CA sertifika zincirini kullanarak user1' in imzasını doğrular.

Bu senaryo verilmesine karşın, bir veri koruma ilkesiyle user2 için sertifikalar gerekli olmaz.

To use Advanced Message Security to enqueue messages on IBM MQ-protected queues having a message protection policy of privacy or integrity, Advanced Message Security must have access to these data items:

- The X.509 V2 or V3 certificate and private key for the user enqueuing the message.
- Tüm ileti imzalayıcılarının dijital sertifikalarını imzalamak için kullanılan sertifikalar zinciri.
- Veri koruma ilkesi gizlilikse, amaçlanan alıcıların X.509 V2 ya da V3 sertifikasıdır. Amaçlanan alıcılar, kuyrukla ilişkili Advanced Message Security ilkesinde listelenir.

z/OS'ta çalışan işlemler ve uygulamalar için, Advanced Message Security ' in iki yerde sertifikalara sahip olması gerekir:

- In a SAF-managed key ring associated with the RACF identity of the sending application (the application that enqueues the protected message) or receiving application (if using privacy).

Advanced Message Security ' in ayırdığı sertifika varsayılan sertifikadır ve özel anahtarı içermelidir. Advanced Message Security , gönderme uygulamasının z/OS kullanıcı kimliğini varsayar. Yani, taşıyıcı olarak hareket eder, böylece kullanıcının özel anahtarına erişebilirler.

- AMS adres alanı kullanıcısıyla ilişkili SAF tarafından yönetilen anahtar halkasında.

  Gizlilik ile korunan iletiler gönderirken, bu anahtarlık, ileti alıcılarının genel anahtar sertifikalarını içerir. İleti alınırken, ileti gönderenin imzasının geçerliliğini denetlemek için gereken Sertifika Yetkilisi sertifikalarının zincirini içerir.

Gösterilen önceki örnekler, yerel CA olarak RACF ' yi kullanmış. Ancak, kuruluşunuzda başka bir PKI sağlayıcısı (Certificate Authority) kullanabilirsiniz. If you intend to use another PKI product, remember that the private key and the certificate must be imported into a key ring associated with the z/OS RACF user IDs that originate IBM MQ messages protected by Advanced Message Security.

You can use the RACF RACDCERT command as the mechanism to generate certificate requests, which can be exported and sent to the PKI provider of your choice to be issued.

Sertifilikle ilgili adımların bir özeti şöyledir:

1. RACF yerel CA ' nın olduğu bir sertifika kuruluşu (CA) sertifikası oluşturulmasını ister. Başka bir PKI sağlayıcısı kullanıyorsanız bu adımı atlayın.
2. CA tarafından imzalanmış kullanıcı sertifikaları oluşturun.
3. Kullanıcılar ve Advanced Message Security AMS adres alanı tanıtıcısı için anahtar halkaları oluşturun.
4. Kullanıcı sertifikasını, varsayılan öznitelikle kullanıcı anahtarı halkasına bağlayın.
5. Alıcıların sertifikalarını kullanım (site) özniteliğini kullanarak Advanced Message Security AMS adres alanı kullanıcı anahtarı halkasına bağlayın (Bu adım, yalnızca gizlilik korumalı iletilerin alıcıları olacak kullanıcı sertifikaları için gereklidir).
6. Connect the CA certificate chains for message senders to the Advanced Message Security AMS address space user key ring. (Bu adım yalnızca gönderen imzalarını doğrulayacak AMS görevleri için gereklidir.)

z/OS *z/OS olmayan bir PKI ' nin yapılandırılması*

z/OSiçinAdvanced Message Security , IBM MQ kuyruklarına yerleştirilen ya dareceivedkuyruklarından alınan iletilerin korunması-işlenmesinde X.509 V3 dijital sertifikalarını kullanır. Advanced Message Security bu sertifikaların yaşam döngülerini oluşturmaz ya da yönetmez; bu işlev bir genel anahtar altyapısı (PKI) tarafından sağlanır. Sertifikaların kullanımını gösteren bu yayındaki örnekler, sertifika isteklerini doldurmak için z/OS Security Server RACF ' i kullanmanın bir özelliğini kullandığından emin olun.

z/OS ya daz/OS olmayan bir PKI ' nin kullanılıp kullanılmayacağı, z/OS için AMS yalnızca RACF tarafından yönetilen anahtar halkaları ya da eşdeğeri tarafından yönetilen anahtar halkaları kullanır. These key rings are based on Security Authorization Facility (SAF) and are the repository used by AMS for z/OS to retrieve certificates for originators and recipients of messages placed on or received from IBM MQ queues.

For messages that are originated from z/OS, which are protected by either integrity or encryption policy, the certificate and private key of the originating user ID must be stored in an SAF-managed key ring that is associated with the z/OS user ID of the message originator.

RACF , sertifikaların ve özel anahtarların RACFtarafından yönetilen anahtar halkalarına aktarılmasına ilişkin yeteneği içerir. See the z/OS Security Server RACF publications for the details and examples of how to load certificates to RACF managed key rings.

Kuruluşunuz desteklenen PKI ürünlerinden birini kullanıyorsa, bu ürünleri nasıl devreye alacağına ilişkin bilgi için ürünle birlikte gönderilen yayınlara başvurun.

Advanced Message Security güvenlik ilkelerinin yönetilmesi

Advanced Message Security , kuyruklar boyunca akan iletileri şifrelemek ve doğrulamak için şifreleme şifreleme ve imza algoritmalarını belirtmek üzere güvenlik ilkelerini kullanır.

AMSiçin güvenlik ilkelerine genel bakış

Advanced Message Security güvenlik ilkeleri, bir iletinin şifrelemeyle şifrelenmiş ve imzalanmış olarak nasıl bir ileti olduğunu açıklayan kavramsal nesnelerdir.

Güvenlik ilkesi özniteliklerine ilişkin ayrıntılar için aşağıdaki alt başlıklara bakın:

İlgili kavramlar

“Koruma kalitesi” sayfa 613
Advanced Message Security veri koruma ilkeleri, bir koruma kalitesi (QOP) anlamına gelir.

“AMSiçindeki güvenlik ilkesi öznitelikleri” sayfa 612
Verileri korumak için belirli bir algoritma ya da yöntem seçmek üzere Advanced Message Security ' i kullanabilirsiniz.

AMSiçindeki ilke adları

İlke adı, belirli bir Advanced Message Security ilkesini ve uygulanacağı kuyruğu tanımlayan benzersiz bir addır.

İlke adı, geçerli olduğu kuyruk adıyla aynı olmalıdır. Advanced Message Security (AMS) arasında bire bir eşleme vardır. Bir ilke ve bir kuyruk.

Kuyrukla aynı adı taşıyan bir ilke yaratarak, o kuyruğa ilişkin ilkeyi etkinleştirmenizi sağlar. Eşleşen ilke adlarına sahip olmayan kuyruklar AMStarafından korunmaz.

İlkenin kapsamı, yerel kuyruk yöneticisiyle ve kuyruklarıyla ilişkilidir. Uzak kuyruk yöneticilerinin, yönettikleri kuyruklar için kendi yerel tanımlı ilkelerinin olması gerekir.

AMSiçindeki imza algoritması

İmza algoritması, veri iletilerini imzalarken kullanılması gereken algoritmayı gösterir.

Geçerli değerler şunlardır:

- MD5
- SHA-1
- SHA-2 Yazı Tipi Ailesi:
  - SHA256
  - SHA384 (anahtar uzunluğu alt sınırı kabul edilebilir-768 bit)
  - SHA512 (en az anahtar uzunluğu kabul edilebilir-768 bit)

İmza algoritması belirtmeyen ya da NONEalgoritmasını belirten bir ilke, ilkeyle ilişkili kuyruğa yerleştirilen iletilerin imzalanmadığını belirtir.

Not: İleti koyma ve alma işlevlerinde kullanılan koruma kalitesi eşleşmeli. Kuyrukta kuyrukta ileti ve ileti arasında bir koruma uyuşmazlığı ilkesi varsa, ileti kabul edilmez ve hata işleme kuyruğuna gönderilir. Bu kural hem yerel, hem de uzak kuyruklar için geçerlidir.

AMSiçinde şifreleme algoritması

Şifreleme algoritması, ilkeyle ilişkilendirilmiş kuyruğa veri iletileri şifrelenirken kullanılması gereken algoritmayı gösterir.

Geçerli değerler şunlardır:

- RC2
- DES
- 3DES
- AES128
- AES256

Bir şifreleme algoritması belirtmeyen ya da NONE algoritmasını belirten bir ilke, ilkeyle ilişkili kuyruğa yerleştirilen iletilerin şifrelenmediğini belirtir.

Advanced Message Security şifreli iletileri de imzalandığından, NONE dışındaki bir şifreleme algoritmasını belirten bir ilkenin de en az bir Alıcı DN 'si ve imza algoritması belirtmesi gerektiğini unutmayın.

Önemli: İleti koyma ve alma işlevlerinde kullanılan koruma kalitesi eşleşmeli. Kuyrukta kuyrukta ileti ve ileti arasında bir koruma uyuşmazlığı ilkesi varsa, ileti kabul edilmez ve hata işleme kuyruğuna gönderilir. Bu kural hem yerel, hem de uzak kuyruklar için geçerlidir.

AMS' ta tolerans

Tolerans özniteliği, Advanced Message Security ' in güvenlik ilkesi belirtilmemiş iletileri kabul edip edemeyeceğini belirtir.

İletileri şifrelemek için bir ilkeye sahip bir kuyruktan ileti alınırken, ileti şifrelenmediyse, çağıran uygulamaya döndürülür. Geçerli değerler şunlardır:

0
Hayır (**varsayılan**).

1
Evet.

Tolerans değeri belirtmeyen ya da 0 değerini belirten bir ilke, ilkeyle ilişkilendirilmiş kuyruğa konan iletilerin ilke kurallarıyla eşleşmesi gerektiğini belirtir.

Tolerans isteğe bağlıdır ve konfigürasyonların kuyruklara uygulandığı, ancak bu kuyrukların önceden tanımlanmış bir güvenlik ilkesi olmayan iletiler içerdikleri için, yapılandırma kullanıma hazır olup olmadığını kolaylaştırmak için bu tolerans isteğe bağlıdır.

AMS içinde gönderen ayırt edici adları

Gönderen ayırt edici adları (DN), bir kuyruğa ileti yerleştirme yetkisi olan kullanıcıları tanımlar. Bir gönderen, iletiyi kuyruğa yerleştirmeden önce, iletiyi imzalamak için sertifikasını kullanır.

Advanced Message Security (AMS) İleti alınıncaya kadar, geçerli bir kullanıcı tarafından veri korumalı bir kuyruğa ileti konup konmadığını denetlemez. Şu anda, ilke bir ya da daha fazla geçerli gönderici öngörüyorsa ve iletiyi kuyruğa yerleştiren kullanıcı geçerli gönderenler listesinde değilse, AMS alan uygulamaya bir hata döndürür ve iletiyi AMS hata kuyruğuna yerleştirir.

Bir ilkenin 0 ya da daha fazla gönderen DN 'si belirtilebilir. İlke için gönderici DN ' leri belirtilmezse, gönderenin sertifikasına güvenildiğini belirten veri korumalı iletileri kuyruğa gönderebilir. Gönderenin sertifikası, genel sertifikayı alan uygulamanın kullanabileceği bir anahtar deposuna eklenerek güvenilir.

Gönderen ayırt edici adları aşağıdaki biçimde bulunur:

```
CN=Common Name,O=Organization,C=Country
```

Önemli:

- Tüm DN ' ler büyük harfli olmalıdır. DN ' deki tüm bileşen adı tanıtıcıları, aşağıdaki çizelgede gösterilen sırayla belirtilmelidir:

Bileşen adı	**Değer**
CN	Bir aygıtın tam adı ya da amacı gibi, bu DN ' nin nesnesine ilişkin ortak ad.
Kuruluş Birimi	Ayırt edici ad (DN) nesnesinin bağlı olduğu kuruluş içindeki birim; örneğin, bir kurumsal bölüm ya da bir ürün adı.
O	DN nesnesinin bağlı olduğu kuruluş; örneğin, bir kuruluş.
L	DN nesnesinin bulunduğu yer (şehir ya da belediye).

Bileşen adı	Değer
ST	DN nesnesinin bulunduğu eyaletin ya da bölgenin adı.
C	Ayırt edici ad (DN) nesnesinin bulunduğu ülke.

- İlke için bir ya da daha çok gönderen DN 'si belirtilirse, yalnızca bu kullanıcılar ilkeyle ilişkili kuyruğa ileti yerleştirebilirler.
- Gönderen DN 'leri belirtildiğinde, iletiyi gönderen kullanıcıyla ilişkili sayısal sertifikada bulunan DN' lerle tam olarak eşleşmelidir.
- AMS , yalnızca Latin-1 karakter takımındaki değerleri içeren DN ' leri destekler. Kümenin karakterlerine sahip DN ' ler oluşturmak için öncelikle UTF-8 kodlaması açık ya da **strmqikm** GUI ile UNIX kodlaması kullanılarak UTF-8 kodlamasında oluşturulan bir DN ile bir sertifika oluşturmanız gerekir. Daha sonra, UTF-8 kodlaması açık bir UNIX platformundan bir ilke oluşturmanız ya da IBM MQiçin AMS eklentisini kullanmanız gerekir.
- AMStarafından, gönderenin adını x.509 biçiminden DN biçimine dönüştürmek için kullanılan yöntem, İl ya da İl değeri için her zaman ST = kullanır.
- Aşağıdaki özel karakterler için çıkış karakterleri gerekir:

```
, (comma)
+ (plus)
" (double quote)
\ (backslash)
< (less than)
> (greater than)
; (semicolon)
```

- Ayırt Edici Ad gömülü boşluklar içeriyorsa, DN ' yi çift tırnak işareti içine almanız gerekir.

İlgili kavramlar

“AMSiçindeki alıcı ayırt edici adları” sayfa 611
Alıcı ayırt edici adları (DN), kuyruktan ileti alma yetkisi olan kullanıcıları tanımlar.

AMSiçindeki alıcı ayırt edici adları

Alıcı ayırt edici adları (DN), kuyruktan ileti alma yetkisi olan kullanıcıları tanımlar.

Bir ilkenin sıfır ya da daha fazla alıcı DN 'si belirtilmiş olabilir. Alıcı ayırt edici adları aşağıdaki biçime sahiptir:

```
CN=Common Name,O=Organization,C=Country
```

Önemli:

- Tüm DN ' ler büyük harfli olmalıdır. DN ' deki tüm bileşen adı tanıtıcılarının aşağıdaki çizelgede gösterilen sırayla belirtilmesi gerekir:

Bileşen adı	Değer
CN	Tam ad ya da aygıtın amaçlanan amacı gibi, bu DN ' nin (DN) nesnesi için ortak ad.
OU	DN nesnesinin bağlı olduğu kuruluş içindeki birim (şirket bölümü ya da ürün adı gibi).
O	DN nesnesinin bağlı olduğu kuruluş (örneğin, bir şirket).
L	DN nesnesinin bulunduğu yerellik (şehir ya da belediye).
ST	DN nesnesinin bulunduğu eyalet ya da bölge adı.

Bileşen adı	Değer
C	Ayırt edici ad (DN) nesnesinin bulunduğu ülke.

- İlke için alıcı DN 'si belirlenmediyse, herhangi bir kullanıcı ilkeyle ilişkili kuyruktan ileti alabilir.
- İlke için bir ya da daha çok alıcı DN 'si belirtilirse, yalnızca bu kullanıcılar ilkeyle ilişkili kuyruktan ileti alabilir.
- Alıcı DN 'si, belirtildiğinde, iletiyi alan kullanıcıyla ilişkili sayısal sertifikada yer alan DN ile tam olarak eşleşmelidir.
- Advanced Message Security , yalnızca Latin-1 karakter kümesinden değerleri içeren DN ' leri destekler. To create DNs with characters of the set, you must first create a certificate with a DN that is created in UTF-8 coding using UNIX with UTF-8 coding turned on or with the **strmqikm** GUI. Then you must create a policy from a UNIX platform with UTF-8 coding turned on or use the Advanced Message Security plug-in to IBM MQ.

İlgili kavramlar

“AMS içinde gönderen ayırt edici adları” sayfa 610
Gönderen ayırt edici adları (DN), bir kuyruğa ileti yerleştirme yetkisi olan kullanıcıları tanımlar. Bir gönderen, iletiyi kuyruğa yerleştirmeden önce, iletiyi imzalamak için sertifikasını kullanır.

AMSiçindeki güvenlik ilkesi öznitelikleri

Verileri korumak için belirli bir algoritma ya da yöntem seçmek üzere Advanced Message Security ' i kullanabilirsiniz.

Güvenlik ilkesi, bir iletinin şifrelemeyle şifrelenmiş ve imzalanmış olarak nasıl bir ileti olduğunu tanımlayan kavramsal bir nesnedir.

Çizelge 103. AMSiçindeki güvenlik ilkesi öznitelikleri

Öznitelikler	Tanım
İlke adı	Kuyruk yöneticisine ilişkin ilkenin benzersiz adı.
İmza Algoritması	İletileri göndermeden önce imzalamak için kullanılan şifreleme algoritması.
Şifreleme Algoritması	İletileri göndermeden önce şifrelemek için kullanılan şifreleme algoritması.
Alıcı listesi	Bir iletinin olası alıcılarının sertifika ayırt edici adlarının (DN) listesi.
İmza DN denetim listesi	İleti alma sırasında doğrulanacak imza DN ' lerinin listesi.

Advanced Message Security' ta iletiler bir simetrik anahtarla şifrelenir ve simetrik anahtar, alıcıların genel anahtarlarıyla şifrelenir. Genel anahtarlar, 2048 bit 'e kadar etkili bir uzunluğun anahtarları olan RSA algoritmasıyla şifrelenir. Gerçek asimetrik anahtar şifrelemesi, sertifika anahtarı uzunluğuna bağlıdır.

Desteklenen simetrik anahtar algoritmaları aşağıdaki gibidir:

- RC2
- DES
- 3DES
- AES128
- AES256

Advanced Message Security , aşağıdaki şifreleme karma işlevlerini de destekler:

- MD5
- SHA-1

- SHA-2 Yazı Tipi Ailesi:
  - SHA256
  - SHA384 (anahtar uzunluğu alt sınırı kabul edilebilir-768 bit)
  - SHA512 (en az anahtar uzunluğu kabul edilebilir-768 bit)

Not: İleti koyma ve alma işlevlerinde kullanılan koruma kalitesi eşleşmeli. Kuyrukta kuyrukta ileti ve ileti arasında bir koruma uyuşmazlığı ilkesi varsa, ileti kabul edilmez ve hata işleme kuyruğuna gönderilir. Bu kural hem yerel, hem de uzak kuyruklar için geçerlidir.

Koruma kalitesi

Advanced Message Security veri koruma ilkeleri, bir koruma kalitesi (QOP) anlamına gelir.

Advanced Message Security içindeki üç koruma düzeyi kalitesi, IBM MQ 9.0 ve sonraki bir yayın düzeyinde dördüncü bir düzeyle tamamlanır ve bu, iletiyi imzalamak ve şifrelemek için kullanılan şifreleme algoritmalarına bağlıdır:

- Gizlilik-kuyruğa yerleştirilen iletiler imzalanmış ve şifrelenmelidir.
- Bütünlük-kuyruğa yerleştirilen iletiler gönderici tarafından imzalanmalıdır.
- Gizlilik-kuyruğun üzerine yerleştirilen iletiler şifrelenmelidir. Daha fazla bilgi için bkz. “AMSile sağlanan koruma nitelikleri” sayfa 541
- Yok-veri koruması geçerli değildir.

Bir kuyruğa yerleştirildiğinde iletilerin imzalanmasını öngören bir ilkenin, QOP INTEGRITY olduğunda imzalanmasını öngörüyor. Bir QOP INTEGRITY, bir ilkenin imza algoritmasını öngördüğü, ancak bir şifreleme algoritmasını önlemeyen bir algoritmanın olduğu anlamına gelir. Bütünlük korumalı iletiler de "SIGNED" olarak da anılır.

Bir kuyruğa yerleştirildiğinde iletilerin imzalanmasını ve şifrelenmesi gerektiğini belirten bir ilke, GIZLILIK durumunda bir QOP ' ye sahiptir. Gizlilik QOP, bir ilke imza algoritması ve şifreleme algoritması öngördüğü zaman anlamına gelir. Gizlilik korumalı iletiler "KAPALI" olarak da anılır.

Bir kuyruğa yerleştirildiğinde iletilerin şifrelenmesi gerektiğini öngören bir ilke, GIZLILIK QOP ' ye sahip olmalıdır. QOP GIZLILIK ilkesi, bir ilkenin şifreleme algoritmasını öngördüğü anlamına gelir.

Bir imza algoritması ya da şifreleme algoritması belirtmeyen bir ilke, NONE (YOK) QOP ' ye sahip. Advanced Message Security , QOP NONE ile ilke içeren kuyruklar için veri koruması sağlar.

Güvenlik ilkelerinin yönetilmesi

Güvenlik ilkesi, bir iletinin şifrelemeyle şifrelenmiş ve imzalanmış olarak nasıl bir ileti olduğunu tanımlayan kavramsal bir nesnedir.

Güvenlik ilkeleriyle ilgili tüm denetim görevlerinin çalıştırıldığı konum, kullandığınız altyapıya bağlıdır.

- ULW UNIXve Windowsüzerinde, güvenlik ilkelerinizi yönetmek için DELETE POLICY, DISPLAY POLICYve SET POLD (ya da eşdeğer PCF) komutlarını kullanıyorsunuz.
  - UNIX UNIXüzerinde yönetim görevleri *MQ_INSTALLATION_PATH*/bin' den çalıştırılabilir.
  - Windows On Windows platforms, administrative tasks can be run from any location as the PATH environment variable is updated at the installation.
- IBM i IBM i' ta DSPMQMSPL, SETMQMSPLve WRKMQMSPL komutları, IBM MQ kurulduğunda sistemin birincil diline ilişkin QSYS sistem kitaplığına kurulur.

  Dil özelliği yüklerine göre ek ulusal dil sürümleri QSYS29xx kitaplıklarına kurulur. For example, a machine with US English as the primary language and Korean as the secondary language has the US English commands installed into QSYS and the Korean secondary language load in QSYS2962 as 2962 is the language load for Korean.

- z/OS z/OSüzerinde, yönetimle ilgili komutlar, ileti güvenliği ilkesi yardımcı programı (CSQ0UTIL) kullanılarak çalıştırılır. When policies are created, modified or deleted on z/OS, the changes are not recognized by Advanced Message Security until the queue manager is stopped and restarted, or the z/OS MODIFY command is used to refresh the Advanced Message Security policy configuration. Örneğin:

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

İlgili görevler

"AMSiçinde güvenlik ilkeleri yaratılması" sayfa 614
Güvenlik ilkeleri, ileti konduğunda bir iletinin nasıl korunacağı ya da bir ileti alındığında nasıl korunmuş olması gerektiğini tanımlar.

"AMSiçindeki güvenlik ilkelerinin değiştirilmesi" sayfa 615
Önceden tanımladığınız güvenlik ilkelerinin ayrıntılarını değiştirmek için Advanced Message Security ' u kullanabilirsiniz.

"Displaying and dumping security policies in AMS" sayfa 615
Sağladığınız komut satırı parametrelere bağlı olarak tüm güvenlik ilkelerinin bir listesini ya da adlandırılmış bir ilkeye ilişkin ayrıntıları görüntülemek için **dspmqspl** komutunu kullanın.

"AMSiçindeki güvenlik ilkelerinin kaldırılması" sayfa 617
Advanced Message Securityiçindeki güvenlik ilkelerini kaldırmak için `setmqspl` komutunu kullanmanız gerekir.

ÇalışırkenAdvanced Message Security

İlgili başvurular

İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)

AMSiçinde güvenlik ilkeleri yaratılması

Güvenlik ilkeleri, ileti konduğunda bir iletinin nasıl korunacağı ya da bir ileti alındığında nasıl korunmuş olması gerektiğini tanımlar.

Başlamadan önce

Güvenlik ilkeleri yaratılırken yerine getirilmesi gereken bazı giriş koşulları vardır:

- Kuyruk yöneticisi çalışıyor olmalıdır.
- Güvenlik ilkesinin adı, IBM MQ nesnelerine ilişkin adlandırma kuralları' na uymalıdır.
- Kuyruk yöneticisine bağlanmak ve bir güvenlik ilkesi yaratmak için gereken yetkiye sahip olmalısınız:
  - z/OS z/OS' ta, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)içinde belgelenen yetkiler verin.
  - Multi z/OSdışındaki diğer platformlarda, setmqaut komutunu kullanarak gerekli + connect, + inq ve + chg yetkilerine izin vermeniz gerekir.

  Güvenliğin yapılandırılmasıyla ilgili daha fazla bilgi için bkz. "Güvenliğin ayarlanması" sayfa 121.
- z/OS z/OS'ta, gerekli sistem nesnelerinin CSQ4INSM' deki tanımlamalara göre tanımlandığından emin olun.

Örnek

Here is an example of creating a policy on queue manager QMGR. Bu ilke, iletilerin SHA256 algoritması kullanılarak imzalanacağını ve DN ile sertifikalar için AES256 algoritmasını kullanarak şifreleneceğini belirtir: CN=joe, O=IBM, C=US ve DN: CN=jane, O=IBM, C = TR. Bu ilke `MY.QUEUE` ' e bağlanır:

```
setmqspl -m QMGR -p MY.QUEUE -s SHA256 -e AES256 -r CN=joe,O=IBM,C=US -r CN=jane,O=IBM,C=US
```

Here is an example of creating policy on the queue manager QMGR. Bu ilke, iletilerin DN ' li sertifikalar için 3DES algoritması kullanılarak şifreleneceğini belirtir: CN=john, O=IBM, C=US ve CN=jeff, O=IBM, C=US ve DN ile sertifika için SHA256 algoritmasıyla imzalanmış: CN=phil, O=IBM, C=TR

```
setmqspl -m QMGR -p MY.OTHER.QUEUE -s SHA256 -e 3DES -r CN=john,O=IBM,C=US -r
CN=jeff,O=IBM,C=US -a CN=phil,O=IBM,C=US
```

Not:

- İleti koyma ve alma işlemi için kullanılmakta olan koruma kalitesi eşleşmelidir. İleti için tanımlanan korumanın ilkesi, kuyruk için tanımlanandan daha zayıf ise, ileti hata işleme kuyruğuna gönderilir. Bu ilke hem yerel, hem de uzak kuyruklar için geçerlidir.

İlgili başvurular

setmqspl komut özniteliklerinin listesini tamamla

AMSiçindeki güvenlik ilkelerinin değiştirilmesi

Önceden tanımladığınız güvenlik ilkelerinin ayrıntılarını değiştirmek için Advanced Message Security ' u kullanabilirsiniz.

Başlamadan önce

- Üzerinde işlem yapmak istediğiniz kuyruk yöneticisi çalışıyor olmalıdır.
- Kuyruk yöneticisine bağlanmak ve bir güvenlik ilkesi yaratmak için gereken yetkiye sahip olmalısınız.
  - z/OS z/OS' ta, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)içinde belgelenen yetkiler verin.
  - Multi z/OSdışındaki diğer platformlarda, setmqaut komutunu kullanarak gerekli + connect, + inq ve + chg yetkilerine izin vermeniz gerekir.

  Güvenliğin yapılandırılmasıyla ilgili daha fazla bilgi için bkz. “Güvenliğin ayarlanması” sayfa 121.

Bu görev hakkında

Güvenlik ilkelerini değiştirmek için, yeni öznitelikler sağlayan var olan bir ilkeye `setmqspl` komutunu uygulayın.

Örnek

Here is an example of creating a policy named MYQUEUE on a queue manager named QMGR, specifying that messages are to be encrypted using the 3DES algorithm for authors (**-a**) having certificates with Distinguished Name (DN) of CN=alice,O=IBM,C=US and signed with the SHA256 algorithm for recipients (**-r**) having certificates with DN of CN=jeff,O=IBM,C=US.

```
setmqspl -m QMGR -p MYQUEUE -e 3DES -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Bu ilkeyi değiştirmek için, örneğin, yalnızca değiştirmek istediğiniz değerleri değiştirerek `setmqspl` komutunu tüm özniteliklerle çalıştırın. Bu örnekte, önceden oluşturulan ilke yeni bir kuyruğa eklenmiş ve şifreleme algoritması AES256olarak değiştirilmiştir:

```
setmqspl -m QMGR -p MYQUEUE -e AES256 -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

İlgili başvurular

setmqspl (güvenlik ilkesini ayarla)

Displaying and dumping security policies in AMS

Sağladığınız komut satırı parametrelere bağlı olarak tüm güvenlik ilkelerinin bir listesini ya da adlandırılmış bir ilkeye ilişkin ayrıntıları görüntülemek için **dspmqspl** komutunu kullanın.

Başlamadan önce

- Güvenlik ilkeleri ayrıntılarını görüntülemek için kuyruk yöneticisi var olmalıdır ve çalışır durumda olmalıdır.
- Kuyruk yöneticisine bağlanmak ve bir güvenlik ilkesi yaratmak için gereken yetkiye sahip olmalısınız.
  - z/OS z/OS' ta, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)içinde belgelenen yetkiler verin.
  - Multi z/OSdışındaki diğer platformlarda, setmqaut komutunu kullanarak gerekli + connect, + inq ve + chg yetkilerine izin vermeniz gerekir.

  Güvenliğin yapılandırılmasıyla ilgili daha fazla bilgi için bkz. “Güvenliğin ayarlanması” sayfa 121.

Bu görev hakkında

Aşağıda **dspmqspl** komut işaretlerinin listesi yer alıyor:

*Çizelge 104. **dspmqspl** komut işaretleri.*

Komut işareti	Açıklama
-m	Kuyruk yöneticisi adı (zorunlu).
-p	İlke adı.
-export	Bu işaretin eklenmesi, farklı bir kuyruk yöneticisine kolayca uygulanabilen çıktı oluşturur.

Örnek

Aşağıdaki örnekte, venus.queue.manageriçin iki güvenlik ilkesi nasıl yaratılacağı gösterilmektedir:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s sha256 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s sha256 -a "CN=another signer,O=IBM,C=US"
-e NONE
```

Bu örnek, venus.queue.manager için tanımlanmış tüm ilkelerin ayrıntılarını ve ürettiği çıktıyı gösteren bir komutu gösterir:

```
dspmqspl -m venus.queue.manager

Policy Details:
Policy name: AMS_POL_04_ONE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNs:
  CN=signer1,O=IBM,C=US
Recipient DNs: -
Toleration: 0
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

Bu örnek, venus.queue.manager için tanımlanmış seçilen bir güvenlik ilkesinin ayrıntılarını ve ürettiği çıktıyı gösteren bir komutu gösterir:

```
dspmqspl -m venus.queue.manager -p AMS_POL_06_THREE
```

```
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: SHA256
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

In the next example, first, we create a security policy and then, we export the policy using the **-export** flag:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s SHA256 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export
```

z/OS z/OSüzerinde, dışa aktarılan ilke bilgileri CSQ0UTIL tarafından EXPORT DD ' ye yazılır.

Multi z/OSdışındaki altyapılarda, çıkışı bir dosyaya yeniden yönlendirin; örneğin:

```
dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Bir güvenlik ilkesini içe aktarmak için:

- Windows Windows' ta `policies.bat`komutunu çalıştırın.
- UNIX UNIX'ta:
  1. `mqm` IBM MQ yönetim grubuna ait bir kullanıcı olarak oturum açın.
  2. Issue `. policies.sh`.
- z/OS z/OS üzerinde, dışa aktarılan ilke bilgilerini içeren veri kümesini SYSIN olarak belirterek CSQ0UTIL yardımcı programını kullanın.

İlgili başvurular
dspmqspl komut özniteliklerinin tam listesi

AMSiçindeki güvenlik ilkelerinin kaldırılması

Advanced Message Securityiçindeki güvenlik ilkelerini kaldırmak için `setmqspl` komutunu kullanmanız gerekir.

Başlamadan önce

Güvenlik ilkelerini yönetirken yerine getirilmesi gereken bazı giriş koşulları vardır:

- Kuyruk yöneticisi çalışıyor olmalıdır.
- Kuyruk yöneticisine bağlanmak ve bir güvenlik ilkesi yaratmak için gereken yetkiye sahip olmalısınız.
  - z/OS z/OS' ta, İleti güvenliği ilkesi yardımcı programı (CSQ0UTIL)içinde belgelenen yetkiler verin.
  - Multi z/OSdışındaki diğer platformlarda, setmqaut komutunu kullanarak gerekli + connect, + inq ve + chg yetkilerine izin vermeniz gerekir.

  Güvenliğin yapılandırılmasıyla ilgili daha fazla bilgi için bkz. “Güvenliğin ayarlanması” sayfa 121.

Bu görev hakkında

setmqspl komutunu **-remove** seçeneğiyle birlikte kullanın.

Örnek

Aşağıda, bir ilkenin kaldırılmasına ilişkin bir örnek:

```
setmqspl -m QMGR -remove -p MY.OTHER.QUEUE
```

İlgili başvurular

setmqspl komut özniteliklerinin listesini tamamla

System queue protection in AMS

Sistem kuyrukları, IBM MQ ile yan uygulamaları arasındaki iletişimi etkinleştirir. Bir kuyruk yöneticisi yaratıldığında, IBM MQ iç iletilerini ve verilerini saklamak için bir sistem kuyruğu da yaratılır. Sistem kuyruklarını, yalnızca yetkili kullanıcıların erişebileceği ya da şifresini çözebilmeleri için Advanced Message Security ile koruyabilirsiniz.

Sistem kuyruğu koruması, olağan kuyrukların korunmalarıyla aynı örüntüleri izler. Bkz. "AMSiçinde güvenlik ilkeleri yaratılması" sayfa 614.

Windows To use system queue protection on Windows, copy the `keystore.conf` file to the following directory:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

z/OS On z/OS, to provide protection for `SYSTEM.ADMIN.COMMAND.QUEUE`, the command server must have access to the `keystore` and the `keystore.conf`, which contain keys and a configuration so that the command server can access keys and certificates. `SYSTEM.ADMIN.COMMAND.QUEUE` güvenlik ilkesinde yapılan tüm değişiklikler, komut sunucusunun yeniden başlatılmasını gerektirir.

Komut kuyruğundan gönderilen ve alınan tüm iletiler, ilke ayarlarına bağlı olarak imzalanır ya da imzalanır ve şifrelenir. Bir yönetici yetkili imzalayıcıları tanımlarsa, imzalayıcı Ayırt Edici Ad (DN) denetimini geçmeyen komut iletileri komut sunucusu tarafından yürütülmez ve Advanced Message Security hata işleme kuyruğuna yönlendirilmez. IBM MQ Gezgini geçici dinamik kuyruklarına yanıt olarak gönderilen iletiler, AMStarafından korunmaz.

Güvenlik ilkelerinin aşağıdaki sistem kuyrukları üzerinde bir etkisi yoktur:

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- z/OS SYSTEM.ADMIN.COMMAND.QUEUE
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
- z/OS SYSTEM.BROKER.CLIENTS.DATA
- SYSTEM.BROKER.CONTROL.QUEUE

- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- z/OS SYSTEM.BROKER.SUBSCRIPTIONS.DATA
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- z/OS SYSTEM.CHLAUTH.DATA.QUEUE
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- z/OS SYSTEM.COMMAND.INPUT
- z/OS SYSTEM.DDELAY.LOCAL.QUEUE
- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE
- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
- z/OS SYSTEM.JMS.PS.STATUS.QUEUE
- z/OS SYSTEM.JMS.REPORT.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- z/OS SYSTEM.QSG.CHANNEL.SYNCQ
- z/OS SYSTEM.QSG.TRANSMIT.QUEUE
- z/OS SYSTEM.QSG.UR.RESOLUTION.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- z/OS SYSTEM.RETAINED.PUB.QUEUE
- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

OAM izinlerinin verilmesi

Dosya izinleri, tüm kullanıcıların `setmqspl` ve `dspmqspl` komutlarını yürütmesine izin verir. Ancak, Advanced Message Security , Object Authority Manager (OAM) olanağına dayanır ve bu komutları IBM MQ denetim grubu olan mqm grubuna ait olmayan ya da verilen güvenlik ilkesi ayarlarını okuma iznine sahip olmayan bir kullanıcı tarafından yürütmek için gereken her bir girişimde bir hata ortaya çıktı.

Yordam

Bir kullanıcıya gereken izinleri vermek için şu işlemi çalıştırın:

```
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
```

Not: İstemcileri, kuyruk yöneticisine Advanced Message Security 7.0.1komutunu kullanarak bağlamak istiyorsanız, yalnızca bu OAM yetkilerini ayarlamanız gerekir.

Uyarı: SYSTEM.PROTECTION.POLICY.QUEUE , tüm durumlarda zorunlu değildir. IBM MQ , ilkeleri önbelleğe alarak başarımı en iyi duruma getirir; böylece, SYSTEM.PROTECTION.POLICY.QUEUE (tüm durumlarda kuyruk).

IBM MQ , var olan tüm ilkeleri önbelleğe almaz. Çok sayıda ilke varsa, IBM MQ sınırlı sayıda ilkeyi önbelleğe alır. So, if the queue manager has a low number of policies defined, there is no need to provide the browse option to the SYSTEM.PROTECTION.POLICY.QUEUE.

Ancak, çok sayıda ilke tanımlanmış olması durumunda ya da eski istemciler kullanıyorsanız, bu kuyruğa göz atma yetkisi vermelisiniz. SYSTEM.PROTECTION.ERROR.QUEUE , AMS kodu tarafından oluşturulan hata iletilerini koymak için kullanılır. Bu kuyruğa ilişkin koyma yetkisi yalnızca, kuyruğa bir hata iletisi koyma girişiminde bulunduğunuzda denetlenir. Bir AMS korumalı kuyruğundan ileti koyma ya da alma girişiminde bulunduğunuzda, kuyruğa koyma yetkiniz denetlenmez.

Güvenlik izinlerinin verilmesi

When using command resource security you must set up permissions to allow Advanced Message Security to function. Bu konu, örneklerde RACF komutlarını kullanır. Kuruluşunuz farklı bir dış güvenlik yöneticisi (ESM) kullanıyorsa, bu ESM için eşdeğer komutları kullanmanız gerekir.

Güvenlik izinleri vermenin üç yönü vardır:

- “AMSM adres alanı” sayfa 620
- “CSQ0UTIL” sayfa 621
- “Advanced Message Security ilkesi tanımlanmış kuyrukları kullanma” sayfa 621

Notlar: Örnek komutlar aşağıdaki değişkenleri kullanır.

1. *QMgrName* -kuyruk yöneticisinin adı.

   z/OS z/OSüzerinde, bu değer bir kuyruk paylaşım grubunun adı da olabilir.
2. *username* -bu bir grup adı olabilir.
3. Bu örneklerde MQQUEUE sınıfı gösterilir. Bu, MXQUEUE, GMQQUEUE ya da GMXQUEUE de olabilir. Ek bilgi için “Kuyruk güvenliğine ilişkin profiller” sayfa 190 ' e bakın.

Ayrıca, tanıtım önceden varsa, RDEFE komutunu zorunlu kılmasınız.

AMSM adres alanı

Advanced Message Security adresinin altında çalıştığı kullanıcı adına bazı IBM MQ güvenliği yayınlamanız gerekir.

- Kuyruk yöneticisine toplu bağlantı için, sorun

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
           PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- SYSTEM.PROTECTION.POLICY.QUEUE, sorun:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
           PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

CSQ0UTIL

Kullanıcıların **setmqspl** ve **dspmqspl** komutlarını çalıştırmalarına olanak sağlayan yardımcı program, kullanıcı adının iş kullanıcı kimliği olduğu aşağıdaki izinleri gerektirir:

- Kuyruk yöneticisine toplu bağlantı için şu komutu verin:

```
  RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
             PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- SYSTEM.PROTECTION.POLICY.QUEUE, **setmqpol** komutu için gereklidir.

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
              PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- SYSTEM.PROTECTION.POLICY.QUEUE, **dspmqpol** komutu için gereklidir.

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
                PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

Advanced Message Security ilkesi tanımlanmış kuyrukları kullanma

Bir uygulama, üzerinde ilke tanımlanmış kuyrukları olan herhangi bir iş yaptığında, bu uygulama Advanced Message Security ' in iletileri korumasına izin vermek için ek izinler gerektirir.

Uygulama şunları gerektirir:

- SYSTEM.PROTECTION.POLICY.QUEUE. Bunu şu komutu vererek yapın:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- SYSTEM.PROTECTION.ERROR.QUEUE. Bunu şu komutu vererek yapın:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
            PERMIT QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

IBM i IBM i' ta sertifikalar ve anahtar deposu yapılandırma dosyası ayarlanıyor

Advanced Message Security korumasını ayarlarken ilk göreviniz bir sertifika oluşturmak ve bunu ortamınızla ilişkilendirmeniz. İlişkilendirme, tümleşik dosya sistemi (IFS) içinde tutulan bir dosya aracılığıyla yapılandırılır.

Yordam

1. IBM iile birlikte gönderilen OpenSSL araçlarını kullanarak kendinden onaylı bir sertifika yaratmak için, QShell 'den şu komutu verin:

   ```
   /QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
   $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
   ```

   Bu komut, kendinden onaylı yeni bir sertifika için çeşitli ayırt edici ad öznitelikleri için komut istemleri sağlar:

   - Ortak Ad (CN =)
   - Kuruluş (O =)
   - Ülke (C =)

Bu, PEM (Privacy Enhanced Mail) biçiminde şifrelenmemiş bir özel anahtar ve eşleşen bir sertifika oluşturur.

Basitlik için, yalnızca ortak ad, kuruluş ve ülke değerlerini girin. Bu öznitelikler ve değerler bir ilke oluştururken önemlidir.

Additional prompts and attributes can be customized by specifying a custom openssl configuration file on the command line with the **-config** parameter. Yapılandırma dosyası sözdizimiyle ilgili ayrıntılar için OpenSSL belgelerine bakın.

Örneğin, aşağıdaki komut ek X.509 v3 sertifika uzantılarını ekler:

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048
-keyout $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365 -config myconfig.cnf
```

Burada myconfig.cnf , aşağıdakileri içeren bir ASCII akış dosyasıdır:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = myextensions

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = GB
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Hants
localityName = Locality Name (eg, city)
localityName_default = Hursley
organizationName = Organization Name (eg, company)
organizationName_default = IBM United Kingdom
organizationalUnitName = Organizational Unit Name (eg, department)
organizationalUnitName_default = IBM MQ Development
commonName = Common Name (eg, Your Name)

[myextensions]
keyUsage = digitalSignature,nonRepudiation,dataEncipherment,keyEncipherment
extendedKeyUsage = emailProtection
```

2. AMS , hem sertifika hem de özel anahtarın aynı dosyada tutulmasını gerektirir. Bunu gerçekleştirmek için aşağıdaki komutu verin:

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

The `private.pem` file in $HOME now contains a matching private key and certificate, while the `mycert.pem` file contains all of the public certificates for which you can encrypt messages and validate signatures.

Varsayılan konumunuzda, bir anahtar deposu yapılandırma dosyası (`keystore.conf`) yaratarak, iki dosyanın ortamınızla ilişkilendirilmesi gerekir.

Varsayılan olarak AMS , anahtar deposu yapılandırmasını ana dizininizin bir `.mqs` alt dizininde arar.

3. QShell 'de `keystore.conf` dosyasını oluşturun:

```
mkdir -p $HOME/.mqs
echo "pem.private = $HOME/private.pem" > $HOME/.mqs/keystore.conf
echo "pem.public = $HOME/mycert.pem" >> $HOME/.mqs/keystore.conf
echo "pem.password = unused" >> $HOME/.mqs/keystore.conf
```

IBM i *IBM iüzerinde ilke oluşturma*

Bir ilke yaratmadan önce, korunan iletileri tutmak için bir kuyruk yaratmanız gerekir.

Yordam

1. Komut satırı bilgi isteminde şunu girin;

```
CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
```

Burada mqmname kuyruk yöneticinizin adıdır.

Kuyruk yöneticisinin güvenlik ilkelerini kullanabilecek durumda olup olmadığını denetlemek için DSPMQM komutunu kullanın. **Security Policy Capability** ' in **YES*değerini gösterdiğini doğrulayın.

Tanımlayabileceğiniz en basit ilke, sayısal imza algoritmasıyla bir ilke oluşturularak elde edilen, ancak şifreleme algoritması olmayan bir bütünlük ilkesidir.

İletiler imzalanır, ancak şifrelenmez. İletiler şifrelenecekse, bir şifreleme algoritması ve bir ya da daha fazla istenen ileti alıcıları belirtmeniz gerekir.

Genel anahtar deposunda, amaçlanan bir ileti alıcısına ilişkin bir sertifika ayırt edici bir adla tanıtılır.

2. Display the distinguished names of the certificates in the public keystore, mycert.pem in $HOME, by using the following command in QShell:

```
/QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
```

Ayırt edilmiş bir alıcı olarak ayırt edici adı girmeniz ve ilke adının korunabilmek için kuyruk adı ile eşleşmesi gerekir.

3. Bir CL komut istemi girişte, örneğin:

```
SETMQMSPL POLICY(PROTECTED) MQMNAME (mqmname)SIGNALG(*SHA256) ENCALG(*AES256) RECIP('CN=..,
O=.., C=..')
```

Burada mqmname kuyruk yöneticinizin adıdır.

İlke oluşturulduktan sonra, söz konusu kuyruk adı aracılığıyla çıkarılan, göz atılan ya da yok edici şekilde kaldırılan iletiler, AMS ilkesine tabidir.

İlgili başvurular

İleti Kuyruğu Yöneticisi 'ni Görüntüle (DSPMQM)

MQM Güvenlik İlkesini Ayarla (SETMQMSPL)

IBM i *IBM iüzerindeki ilkenin sınanması*

Güvenlik ilkelerinizi test etmek için ürünle birlikte sağlanan örnek uygulamaları kullanın.

Bu görev hakkında

You can use the sample applications provided with IBM MQ , such as AMQSPUT4, AMQSGET4, AMQSGBR4, and tools such as WRKMQMMSG to put, browse, and get messages using the PROTECTED queue name.

Her şeyin doğru şekilde yapılandırılmış olması durumunda, bu kullanıcı için korunmayan bir kuyruğun uygulama davranışında bir fark olmaması gerekir.

Advanced Message Securityiçin ayarlanmamış bir kullanıcı ya da iletinin şifresini çözmek için gerekli özel anahtara sahip olmayan bir kullanıcı, iletiyi görüntüleyemez. Kullanıcı, MQCC_FAILED (2) ve neden kodu RC2063 (MQRC_SECURITY_ERROR) için eşdeğer bir RCFAIL ' in tamamlanma kodunu alır.

AMS korumasının etkin olduğunu görmek için, örneğin AMQSPUT0' ı kullanarak, bazı sınama iletilerini KORUNAN kuyruğuna (örneğin, KORUNAN) koyun. Daha sonra, dinlenirken işlenmemiş korunan verilere göz atmak için bir diğer ad kuyruğu yaratabilirsiniz.

Yordam

Bir kullanıcıya gereken izinleri vermek için şu işlemi çalıştırın:

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(yourqm)
```

Örneğin, AMQSBCG4 ya da WRKMQMMSG gibi ALIAS kuyruk adı kullanılarak göz atılması, korunan kuyruğun göz atma işlemi için cleartext iletileri gösterdiği daha büyük `scrambled` iletileri ortaya koymalıdır.

Karışık iletiler görünür, ancak bu adla eşleşen AMS için herhangi bir ilke olmadığı için, özgün cleartext ALIAS kuyruğu kullanılarak çözülebilir değil. Bu nedenle, işlenmemiş korunan veriler döndürülür.

İlgili başvurular

MQM Güvenlik İlkesini Ayarla (SETMQMSPL)

MQ iletileriyle çalış (WRKMQMMSG)

Komut ve yapılandırma olayları

Advanced Message Securityile, denetim için ilke değişikliklerinin kaydı olarak günlüğe kaydedilebilir ve hizmet verebilen komut ve yapılandırma olayı iletileri oluşturabilirsiniz.

IBM MQ tarafından oluşturulan komut ve yapılandırma olayları, olayın gerçekleştiği kuyruk yöneticisininde adanmış kuyruklara gönderilen PCF biçiminin iletileridir.

Yapılandırma olayları iletileri SYSTEM.ADMIN.CONFIG.EVENT kuyruğu.

Komut olayları iletileri SYSTEM.ADMIN.COMMAND.EVENT kuyruğu.

Events are generated regardless of tools you are using to manage Advanced Message Security security policies.

Advanced Message Security' ta, güvenlik ilkelerinde farklı işlemler tarafından oluşturulan dört tip olay vardır:

- “AMSiçinde güvenlik ilkeleri yaratılması” sayfa 614, which generate two IBM MQ event messages:
  - Bir yapılandırma olayı
  - Bir komut olayı
- “AMSiçindeki güvenlik ilkelerinin değiştirilmesi” sayfa 615, which generates three IBM MQ event messages:
  - Eski güvenlik ilkesi değerlerini içeren bir yapılandırma olayı
  - Yeni güvenlik ilkesi değerleri içeren bir yapılandırma olayı
  - Bir komut olayı
- “Displaying and dumping security policies in AMS” sayfa 615, which generates one IBM MQ event message:
  - Bir komut olayı
- “AMSiçindeki güvenlik ilkelerinin kaldırılması” sayfa 617, which generates two IBM MQ event messages:
  - Bir yapılandırma olayı
  - Bir komut olayı

Olay günlüğe kaydetmeyi etkinleştirme ve devre dışı bırakma

You control command and configuration events by using the queue manager attributes **CONFIGEV** and **CMDEV**. Bu olayları etkinleştirmek için, uygun kuyruk yöneticisi özniteliğini ENABETLEolarak ayarlayın. Bu olayları geçersiz kılmak için, uygun kuyruk yöneticisi özniteliğini DISABLE(Geçersiz) olarak ayarlayın.

Yordam

Yapılandırma olayları

Yapılandırma olaylarını etkinleştirmek için **CONFIGEV** seçeneğini ETKINolarak ayarlayın. Yapılandırma olaylarını devre dışı bırakmak için **CONFIGEV** seçeneğini DEVRE Dışıolarak ayarlayın. Örneğin, aşağıdaki MQSC komutunu kullanarak yapılanış olaylarını etkinleştirebilirsiniz:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Komut olayları

Komut olaylarını etkinleştirmek için, **CMDEV** seçeneğini ENABETLEolarak ayarlayın. To enable command events for commands except **DISPLAY MQSC** commands and Inquire PCF commands, set the **CMDEV** to DüğüM. Komut olaylarını devre dışı bırakmak için **CMDEV** , DISABLEolarak ayarlayın. Örneğin, aşağıdaki MQSC komutunu kullanarak komut olaylarını etkinleştirebilirsiniz:

```
ALTER QMGR CMDEV (ENABLED)
```

İlgili görevler

Controlling configuration, command, and logger events in IBM MQ

Komut olayı ileti biçimi

Komut olay iletisi, izleyen MQCFH yapısından ve PCF parametrelerinden oluşur.

Seçilen MQCFH değerleri şunlardır:

```
Type = MQCFT_EVENT;
Command = MQCMD_COMMAND_EVENT;
MsgSeqNumber = 1;
Control = MQCFC_LAST;
ParameterCount = 2;
CompCode = MQCC_WARNING;
Reason = MQRC_COMMAND_PCF;
```

Not: ParameterCount değeri iki, MQCFGR tipi (grup) her zaman iki değiştirgesi olduğu için iki değerdir. Her grup, uygun parametrelerden oluşur. Olay verileri iki gruptan (CommandContext ve CommandData) oluşur.

CommandContext şunları içerir

EventUsertanıtıcısı

Açıklama:	Olayı oluşturan komutu ya da çağrıyı yayınlayan kullanıcı kimliği. (Bu kullanıcı kimliği, komutu ya da çağrıyı verme yetkisini denetlemek için kullanılan kullanıcı kimliğidir; bir kuyruktan alınan komutlar için, komut iletisinin MD 'si tarafından da kullanıcı kimliğidir (UserIdentifier).
Tanıtıcı:	MQCACF_EVENT_USER_ID.
Veri tipi:	MQCFST.
Uzunluk üst sınırı:	MQ_USER_ID_LENGTH.
Döndürülen:	Her zaman.

EventOrigin

Açıklama:	Olaya neden olan eylemin kökeni.
Tanıtıcı:	MQIACF_EVENT_ORIGIN.
Veri tipi:	MQCFIN.

Değerler:

MQEVO_CONSOLE
Konsol komutu-komut satırı.

MQEVO_MSG
IBM MQ Explorer eklentisinden komut iletisi.

Döndürülen: Her zaman.

EventQMgr

Açıklama: Komutun ya da çağırmanın girildiği kuyruk yöneticisi. (Komutun yürütüldüğü ve olayı oluşturan kuyruk yöneticisi olay iletisinin MD ' inde yer alıyor).

Tanıtıcı: MQCACF_EVENT_Q_MGR.

Veri tipi: MQCFST.

Uzunluk üst sınırı: MQ_Q_MGR_NAME_LENNGTH.

Döndürülen: Her zaman.

EventAccountingSimgesi

Açıklama: İleti olarak alınan komutlar için (MQEVO_MSG), komut iletisinin MD ' den muhasebe simgesi (AccountingToken).

Tanıtıcı: MQBACF_EVENT_ACCOUNTING_TOKEN.

Veri tipi: MQCFBS.

Uzunluk üst sınırı: MQ_ACCOUNTING_TOKEN_LENGTH.

Döndürülen: Yalnızca EventOrigin MQEVO_MSG ise.

EventIdentityVerileri

Açıklama: Komut iletisi olarak alınan komutlar için (MQEVO_MSG), uygulama kimliği verileri (ApplIdentityData) komut iletisinin MD 'si tarafından alınır.

Tanıtıcı: MQCACF_EVENT_APPL_IDENTITY.

Veri tipi: MQCFST.

Uzunluk üst sınırı: MQ_APPL_IDENTITY_DATA_LENGTH.

Döndürülen: Yalnızca EventOrigin MQEVO_MSG ise.

EventApplTipi

Açıklama: Komut olarak alınan komutlar için (MQEVO_MSG), uygulama tipi (PutApplType), komut iletisinin MD 'inden alınır.

Tanıtıcı: MQIACF_EVENT_APPL_TYPE.

Veri tipi: MQCFIN.

Döndürülen: Yalnızca EventOrigin MQEVO_MSG ise.

EventApplAdı

Açıklama: İleti olarak alınan komutlar için (MQEVO_MSG), komut iletisinin MD ' inden uygulamanın adı (PutApplAd).

Tanıtıcı: MQCACF_EVENT_APPL_ADı.

Veri tipi: MQCFST.

Uzunluk üst sınırı: MQ_APPL_NAME_LEGTH.

Döndürülen: Yalnızca EventOrigin MQEVO_MSG ise.

EventApplBaşlangıç Noktası

Açıklama: İleti olarak alınan komutlar için (MQEVO_MSG), komut iletisinin MD ' den uygulama başlangıç verileri (ApplOriginVerileri).

Tanıtıcı: MQCACF_EVENT_APPL_ORIGIN.

Veri tipi: MQCFST.

Uzunluk üst sınırı: MQ_APPL_ORIGIN_DATA_LENGTH.

Döndürülen: Yalnızca EventOrigin MQEVO_MSG ise.

Komut

Açıklama: Komut kodu.

Tanıtıcı: MQIACF_COMMAND.

Veri tipi: MQCFIN.

Değerler: **MQCMD_INQUIRE_PROT_POLICY sayısal değer 205**
MQCMD_CREATE_PROT_POLICY sayısal değer 206
MQCMD_DELETE_PROT_POLICY sayısal değer 207
MQCMD_CHANGE_PROT_POLICY sayısal değer 208
Bunlar IBM MQ 8.0 `cmqcfc.` hiçinde tanımlanır.

Döndürülen: Her zaman.

CommandData , PCF komutuna sahip PCF öğelerini içerir.

Yapılanış olayı ileti biçimi

Yapılandırma olayları, standart Advanced Message Security biçiminin PCF iletileridir.

MQMD ileti tanımlayıcısına ilişkin olası değerler, Olay iletisi MQMD (ileti tanımlayıcısı)içinde bulunabilir.

Seçilen MQMD değerleri şunlardır:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR           //for both CLI and command server
```

İleti arabelleği, izleyen MQCFH yapısından ve parametre yapısından oluşur. Olası MQCFH değerleri, Olay iletisi MQCFH (PCF üstbilgisinde)içinde bulunabilir.

Seçilen MQCFH değerleri şunlardır:

```
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}
```

MQCFH ' yi izleyen değiştirgeler şunlardır:

EventUserID

Açıklama: Olayı oluşturan komutu ya da çağrıyı yayınlayan kullanıcı kimliği. (Bu kullanıcı kimliği, komutu ya da çağrıyı verme yetkisini denetlemek için kullanılan kullanıcı kimliğidir; bir kuyruktan alınan komutlar için, komut iletisinin MD 'si tarafından da kullanıcı kimliğidir (UserIdentifier).

Tanıtıcı: **MQCACF_EVENT_USER_ID**

Veri tipi: MQCFST.

Uzunluk üst sınırı: MQ_USER_ID_LENGTH.

Döndürülen: Her zaman.

SecurityId

Açıklama: Komut sunucusu iletisi ya da yerel komut için Windows SID olması durumunda MQMD.AccountingToken değeri.

Tanıtıcı: **MQBACF_EVENT_SECURITY_ID**

Veri tipi: MQCBS.

Uzunluk üst sınırı: MQ_SECURITY_ID_LENGTH.

Döndürülen: Her zaman.

EventOrigin

Açıklama: Olaya neden olan eylemin kökeni.

Tanıtıcı: **MQIACF_EVENT_ORIGIN**

Veri tipi: MQCFIN.

Değerler:

MQEVO_CONSOLE
Konsol komutu-komut satırı.

MQEVO_MSG
IBM MQ Explorer eklentisinden komut iletisi.

Döndürülen: Her zaman.

EventQMgr

Açıklama: Komutun ya da çağırmanın girildiği kuyruk yöneticisi. (Komutun yürütüldüğü ve olayı oluşturan kuyruk yöneticisi olay iletisinin MD ' inde yer alıyor).

Tanıtıcı: **MQCACF_EVENT_Q_MGR**

Veri tipi: MQCFST

Uzunluk üst sınırı: MQ_Q_MGR_NAME_LENGH

Döndürülen: Her zaman.

ObjectType

Açıklama: Nesne tipi.

Tanıtıcı: **MQIACF_OBJECT_TYPE**

Veri tipi: MQCFIN

Değer:

MQOT_PROT_POLICY
Advanced Message Security koruma ilkesi. **1019** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlı bir sayısal değer.

Döndürülen: Her zaman.

PolicyName

Açıklama: Advanced Message Security ilkesi adı.

Tanıtıcı: **MQCA_POLICY_NAME**.

Veri tipi: MQCFST.

Değer: **2112** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlı bir sayısal değer.

Uzunluk üst sınırı: MQ_OBJECT_NAME_LENGTH.

Döndürülen: Her zaman.

PolicyVersion

Açıklama: Advanced Message Security ilkesi sürümü.

Tanıtıcı: **MQIA_POLICY_VERSION**

Veri tipi: MQCFIN

Değer **238** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlanan bir sayısal değer.

Döndürülen: Her zaman

TolerateFlag

Açıklama: Advanced Message Security ilke toleransı işareti.

Tanıtıcı: **MQIA_TOLERANTE_KORUMASIZ**

Veri tipi: MQCFIN

Değer **235** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlanan bir sayısal değer.

Döndürülen: Her zaman.

SignatureAlgorithm

Açıklama: Advanced Message Security ilke imza algoritması.

Tanıtıcı: **MQIA_SIGNATURE_ALGORITHM**

Veri tipi: MQCFIN

Değer: **236** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlanan bir sayısal değer.

Döndürülen: Advanced Message Security ilkesinde tanımlanmış bir imza algoritması olduğunda

EncryptionAlgorithm

Açıklama: Advanced Message Security ilke şifreleme algoritması.

Tanıtıcı: **MQIA_ENCRYPTION_ALGORITHM**

Veri tipi: MQCFIN

Değer: **237** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlanan bir sayısal değer.

Döndürülen: IBM MQ ilkesinde tanımlı bir şifreleme algoritması olduğunda

SignerDNs

Açıklama: İzin verilen imzalayıcıların DistinguishedName konusu.

Tanıtıcı: **MQCA_SIGNER_DN**

Veri tipi: MQCFSL

Değer: **2113** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlı bir sayısal değer.

Uzunluk üst sınırı: İlkedeki en uzun imzalayıcı ayırt edici adı (DN), ancak artık MQ_DISTINGUISH_NAME_LENGTH

Döndürülen: IBM MQ ilkesinde tanımlandığında.

RecipientDNs

Açıklama: İzin verilen imzalayıcıların DistinguishedName konusu.

Tanıtıcı: **MQCA_RECIPIENT_DN**

Veri tipi: MQCFSL

Değer: **2114** - IBM MQ 8.0 ya da `cmqc.h` dosyasında tanımlı bir sayısal değer.

Uzunluk üst sınırı: Ilkedeki en uzun alıcı ayırt edici adı (DN), ancak artık MQ_DISTINGUISH_NAME_LENGTH değil.

Döndürülen: IBM MQ ilkesinde tanımlandığında.

Özel notlar

Bu belge, ABD'de kullanıma sunulan ürünler ve hizmetler için hazırlanmıştır.

IBM, bu belgede sözü edilen ürün, hizmet ya da özellikleri diğer ülkelerde kullanıma sunmayabilir. Bulunduğunuz yerde kullanıma sunulan ürün ve hizmetleri yerel IBM müşteri temsilcisinden ya da çözüm ortağından öğrenebilirsiniz. Bir IBM ürün, program ya da hizmetine gönderme yapılması, açık ya da örtük olarak, yalnızca o IBM ürünü, programı ya da hizmetinin kullanılabileceğini göstermez. Aynı işlevi gören ve IBM'in fikri mülkiyet haklarına zarar vermeyen herhangi bir ürün, program ya da hizmet de kullanılabilir. Ancak, IBM dışı ürün, program ya da hizmetlerle gerçekleştirilen işlemlerin değerlendirilmesi ve doğrulanması kullanıcının sorumluluğundadır.

IBM'in, bu belgedeki konularla ilgili patentleri ya da patent başvuruları olabilir. Bu belgenin size verilmiş olması, patentlerin izinsiz kullanım hakkının da verildiği anlamına gelmez. Lisansla ilgili sorularınızı aşağıdaki adrese yazabilirsiniz:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Çift byte (DBCS) bilgilerle ilgili lisans soruları için, ülkenizdeki IBM'in Fikri Haklar (Intellectual Property) bölümüyle bağlantı kurun ya da sorularınızı aşağıda adrese yazın:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japonya

Aşağıdaki paragraf, İngiltere ya da bu tür hükümlerin yerel yasalarla uyuşmadığı diğer ülkelerde geçerli değildir: INTERNATIONAL BUSINESS MACHINES CORPORATION BU YAYINI, HAK İHLALİ YAPILMAYACAĞINA DAİR GARANTİLERLE TİCARİLİK VEYA BELİRLİ BİR AMACA UYGUNLUK İÇİN ZIMNİ GARANTİLER DE DAHİL OLMAK VE FAKS BUNLARLA SINIRLI OLMAMAK ÜZERE AÇIK YA DA ZIMNİ HİÇBİR GARANTİ VERMEKSİZİN "OLDUĞU GİBİ" ESASIYLA SAĞLAMAKTADIR. Bazı ülkeler bazı işlemlerde garantinin açık ya da örtük olarak reddedilmesine izin vermez; dolayısıyla, bu bildirim sizin için geçerli olmayabilir.

Bu yayın teknik yanlışlar ya da yazım hataları içerebilir. Buradaki bilgiler üzerinde düzenli olarak değişiklik yapılmaktadır; söz konusu değişiklikler sonraki basımlara yansıtılacaktır. IBM, önceden bildirimde bulunmaksızın, bu yayında açıklanan ürünler ve/ya da programlar üzerinde iyileştirmeler ve/ya da değişiklikler yapabilir.

Bu belgede IBM dışı Web sitelerine yapılan göndermeler kullanıcıya kolaylık sağlamak içindir ve bu Web sitelerinin onaylanması anlamına gelmez. Bu Web sitelerinin içerdiği malzeme, bu IBM ürününe ilişkin malzemenin bir parçası değildir ve bu tür Web sitelerinin kullanılmasının sorumluluğu size aittir.

IBM'e bilgi ilettiğinizde, IBM bu bilgileri size karşı hiçbir yükümlülük almaksızın uygun gördüğü yöntemlerle kullanabilir ya da dağıtabilir.

(i) Bağımsız olarak yaratılan programlarla, bu program da içinde olmak üzere diğer programlar arasında bilgi değiş tokuşuna ve (ii) değiş tokuş edilen bilginin karşılıklı kullanımına olanak sağlamak amacıyla bu program hakkında bilgi sahibi olmak isteyen lisans sahipleri şu adrese yazabilirler:

IBM Corporation
Yazılım Birlikte Çalışabilirlik Koordinatörü, Bölüm 49XA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Bu tür bilgiler, ilgili kayıt ve koşullar altında ve bazı durumlarda bedelli olarak edinilebilir.

Bu belgede açıklanan lisanslı program ve bu programla birlikte kullanılabilecek tüm lisanslı malzeme, IBM tarafından, IBM Müşteri Sözleşmesi, IBM Uluslararası Program Lisansı Sözleşmesi ya da eşdeğer herhangi bir sözleşmenin kayıt ve koşulları altında sağlanır.

Burada belirtilen performans verileri denetimli bir ortamda elde edilmiştir. Bu nedenle, başka işletim ortamlarında çok farklı sonuçlar alınabilir. Bazı ölçümler geliştirilme düzeyindeki sistemlerde yapılmıştır ve bu ölçümlerin genel kullanıma sunulan sistemlerde de aynı olacağı garanti edilemez. Ayrıca, bazı sonuçlar öngörü yöntemiyle elde edilmiş olabilir. Dolayısıyla, gerçek sonuçlar farklı olabilir. Bu belgenin kullanıcıları, kendi ortamları için geçerli verileri kendileri doğrulamalıdırlar.

IBM dışı ürünlerle ilgili bilgiler, bu ürünleri sağlayan firmalardan, bu firmaların yayın ve belgelerinden ve genel kullanıma açık diğer kaynaklardan alınmıştır. IBM bu ürünleri sınamamıştır ve IBM dışı ürünlerle ilgili performans doğruluğu, uyumluluk gibi iddiaları doğrulayamaz. IBM dışı ürünlerin yeteneklerine ilişkin sorular, bu ürünleri sağlayan firmalara yöneltilmelidir.

IBM'in gelecekteki yönelim ve kararlarına ilişkin tüm bildirimler değişebilir ve herhangi bir duyuruda bulunulmadan bunlardan vazgeçilebilir; bu yönelim ve kararlar yalnızca amaç ve hedefleri gösterir.

Bu belge, günlük iş ortamında kullanılan veri ve raporlara ilişkin örnekler içerir. Örneklerin olabildiğince açıklayıcı olması amacıyla kişi, şirket, marka ve ürün adları belirtilmiş olabilir. Bu adların tümü gerçek dışıdır ve gerçek iş ortamında kullanılan ad ve adreslerle olabilecek herhangi bir benzerlik tümüyle rastlantıdır.

YAYIN HAKKI LİSANSI:

Bu belge, çeşitli işletim platformlarında programlama tekniklerini gösteren, kaynak dilde yazılmış örnek uygulama programları içerir. Bu örnek programları, IBM'e herhangi bir ödemede bulunmadan, örnek programların yazıldığı işletim altyapısına ilişkin uygulama programlama arabirimiyle uyumlu uygulama programlarının geliştirilmesi, kullanılması, pazarlanması ya da dağıtılması amacıyla herhangi bir biçimde kopyalayabilir, değiştirebilir ve dağıtabilirsiniz. Bu örnekler her koşul altında tüm ayrıntılarıyla sınanmamıştır. Dolayısıyla, IBM bu programların güvenilirliği, bakım yapılabilirliği ya da işlevleri konusunda açık ya da örtük güvence veremez.

Bu bilgileri elektronik kopya olarak görüntülediyseniz, fotoğraflar ve renkli resimler görünmeyebilir.

Programlama arabirimi bilgileri

Programlama arabirimi bilgileri (sağlandıysa), bu programla birlikte kullanılmak üzere uygulama yazılımları yaratmanıza yardımcı olmak üzere hazırlanmıştır.

Bu kitap, müşterinin WebSphere MQhizmetlerini edinmek üzere program yazmasına olanak tanıyan, amaçlanan programlama arabirimlerine ilişkin bilgiler içerir.

Ancak, bu bilgiler tanılama, değiştirme ve ayarlama bilgilerini de içerebilir. Tanılama, değiştirme ve ayarlama bilgileri, uygulama yazılımlarınızda hata ayıklamanıza yardımcı olur.

Önemli: Bu tanılama, değiştirme ve ayarlama bilgilerini bir programlama arabirimi olarak kullanmayın; bu, değişiklik söz konusu olduğunda kullanılır.

Ticari Markalar

IBM, IBM logosu, ibm.com, IBM Corporation 'ın dünya çapında birçok farklı hukuk düzeninde kayıtlı bulunan ticari markalarıdır. IBM ticari markalarının güncel bir listesini Web üzerinde "Telif hakkı ve ticari marka bilgileri"www.ibm.com/legal/copytrade.shtmladresinde bulabilirsiniz. Diğer ürün ve hizmet adları IBM'in veya diğer şirketlerin ticari markaları olabilir.

Microsoft ve Windows, Microsoft Corporation'ın ABD ve/veya diğer ülkelerdeki ticari markalarıdır.

UNIX, The Open Group şirketinin ABD ve diğer ülkelerdeki tescilli ticari markasıdır.

Linux, Linus Torvalds'ın ABD ve/ya da diğer ülkelerdeki tescilli ticari markasıdır.

Bu ürün, Eclipse Project (http://www.eclipse.org/) tarafından geliştirilen yazılımları içerir.

Java ve Java tabanlı tüm markalar ve logolar, Oracle firmasının ve/ya da iştiraklerinin markaları ya da tescilli markalarıdır.

Parça numarası:

(1P) P/N: