7.5

IBM WebSphere MQ güvenliğinin sağlanması

Not

Bu bilgileri ve desteklediği ürünü kullanmadan önce, “Özel notlar” sayfa 317 bölümündeki bilgileri okuyun.

Bu basım, yeni basımlarında tersi belirtilmediği sürece, IBM® WebSphere MQ ' ın 7. yayın düzeyi 5 'i ve sonraki tüm yayın ve değişiklik düzeyleri için geçerlidir.

İçindekiler

Güvenlik

Güvenlik, IBM WebSphere MQ uygulamalarının hem geliştiricileri hem de IBM WebSphere MQ yetkilerinin yapılandırıldığı sistem yöneticileri için önemli bir önem gösteridir.

Güvenliğe genel bakış

Bu konu derlemi, IBM WebSphere MQ güvenlik kavramlarını tanıtır.

Güvenlik kavramları ve mekanizmaları, herhangi bir bilgisayar sistemine uygulandıkça, önce bu güvenlik mekanizmalarının bir tartışması ve ardından IBM WebSphere 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 WebSphere MQ installation.

Güvenlik konusunda yaygın olarak kabul edilen noktalar aşağıda verilmiştir:

- “Tanımlama ve kimlik doğrulama” sayfa 5
- “Yetkilendirme” sayfa 6
- “Denetleme” sayfa 6
- “Gizlilik” sayfa 6
- “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 WebSphere 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 45.

İlgili kavramlar

“SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanması” sayfa 199
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 ile çalışma” sayfa 108
These topics give instructions for performing single tasks related to using SSL or TLS with IBM WebSphere MQ.

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 WebSphere MQ environment because IBM WebSphere 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.

IBM WebSphere MQ Advanced Message Security ileIBM WebSphere MQ , temel işlevinin bir parçası olarak itibarlı olmayan bir hizmet sağlamaz. Ancak, bu ürün belgeleri kendi çıkış programlarınızı yazarak bir WebSphere MQ ortamı içinde kendi itibarsız hizmeti nasıl sağlayabileceğinize ilişkin önerileri içerir.

İlgili kavramlar

“IBM WebSphere MQiçinde kimlik doğrulama ve kimlik doğrulama” sayfa 20
IBM WebSphere 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 WebSphere MQiçinde yetki” sayfa 21
IBM WebSphere MQ ortamınızda hangi belirli kişileri ya da uygulamaları yapabilmeyi 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 48 ve ilişkili alt konular.

İlgili kavramlar

“IBM WebSphere MQiçinde denetim” sayfa 21
IBM WebSphere 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, WebSphere MQiçin geçerli olan şifreleme kavramlarını açıklar.

Varlık terimi, bir kuyruk yöneticisine, bir WebSphere MQ MQI istemcisine, tek bir kullanıcıya ya da ileti alışverişi yeteneğine sahip başka bir sisteme gönderme yapmak için kullanılır.

İlgili kavramlar

“IBM WebSphere MQiçinde şifreleme” sayfa 22
IBM WebSphere MQ , Güvenli Yuva Katmanı (SSL) ve İletim Güvenliği Katmanı (TLS) iletişim kurallarını 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*).

Şifrelemenin tanımı için Sözlük ' e bakın.

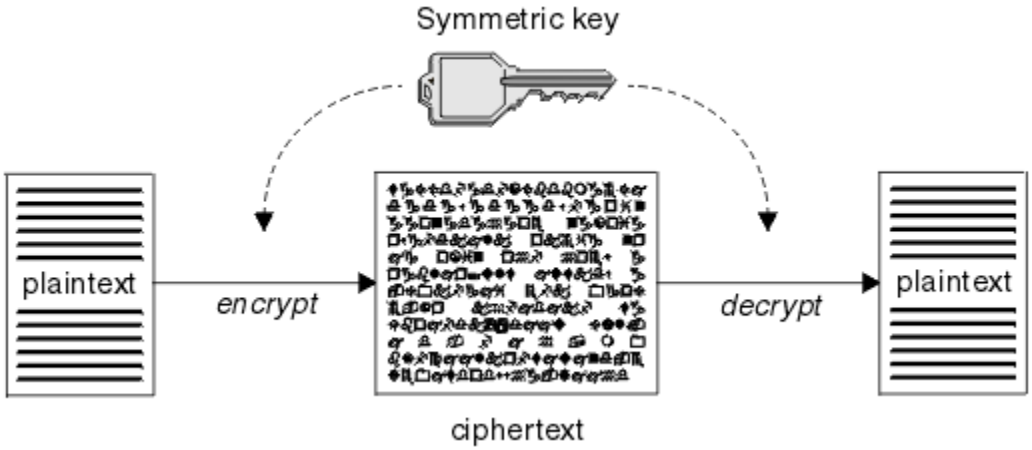
Dönüştürme işlemi, ileti sırasında iletinin görünüşünü değiştiren, ancak içeriği etkilmeyen bir dizi matematiksel işlem içerir. Şifreleme teknikleri, şifreli bir ileti anlaşılabilir olmadığı için, gizliliğin gizliliği ve yetkisiz görüntülere karşı koruma sağlayabilmelerini sağlar. Dijital imzalar, mesaj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

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

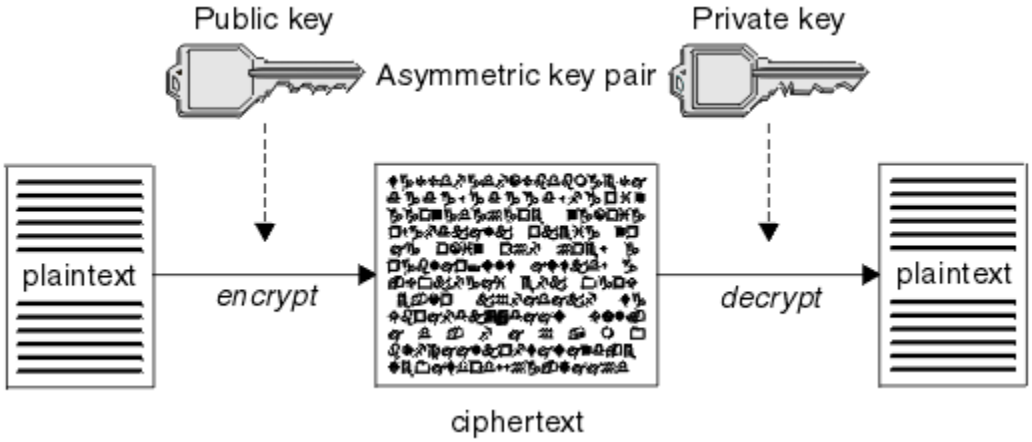
- Her iki tarafın da aynı gizli anahtarı kullanmasını gerektirenler. Paylaşılan anahtar kullanan algoritmalar *simetrik* algoritmalar olarak bilinir. Şekil 1 sayfa 8 simetrik anahtar şifrelemesi gösterir.
- Şifreleme için bir anahtar ve şifre çözme için farklı bir anahtar kullananlar. Bunlardan bir tanesi 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 HASH işleviyle hesaplanan bir iletinin içeriğinin sabit boyutlu sayısal gösterimidir. Bir ileti özeti şifrelenebilir, dijital imza oluşturulabilir.

İletiler doğal olarak değişken olarak değişkendir. İleti özeti, bir iletinin içeriğinin sabit boyutlu sayısal gösterimidir. Bir ileti özeti, iki ölçütü karşılayan bir dönüştürme olan bir HASH işleviyle hesaplanır:

- HASH işlevi tek bir şekilde olmalıdır. 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 ve 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 10içinde açıklandığı şekilde, Sertifika Yetkilisi (CA) olarak adlandırılır.

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

WebSphere MQ tarafından kullanılan sayısal sertifikalar X.509 standartı ile uyumludur. Bu standart, gereken bilgileri ve bunu gönderme biçimini belirtir. 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 algılamazsa 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
WebSphere MQ , X.509 standardına uygun dijital sertifikaları destekler. İstemci kimlik denetimi seçeneğini gerektirir.

IBM WebSphere MQ bir eşdüzey sistem olduğu için, SSL terminolojisinde istemci kimlik doğrulaması olarak görüntülenir. Bu nedenle, SSL kimlik doğrulaması için kullanılan kişisel sertifikalar, istemci kimlik doğrulamasının önemli bir kullanımına izin vermeli. 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 WebSphere MQiçinde sertifika doğrulama ilkeleri hakkında daha fazla bilgi için bkz. “IBM WebSphere MQiçindeki sertifika geçerlilik denetimi ilkeleri” sayfa 33.

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 146
- 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.

DN ' de yaygın olarak aşağıdaki öznitelik tipleri bulunur:

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 WebSphere MQ Yanlış biçimlendirilmiş DN ' leri kabul eder. Daha fazla bilgi için bakınız: WebSphere MQ rules for SSLPEER valules.

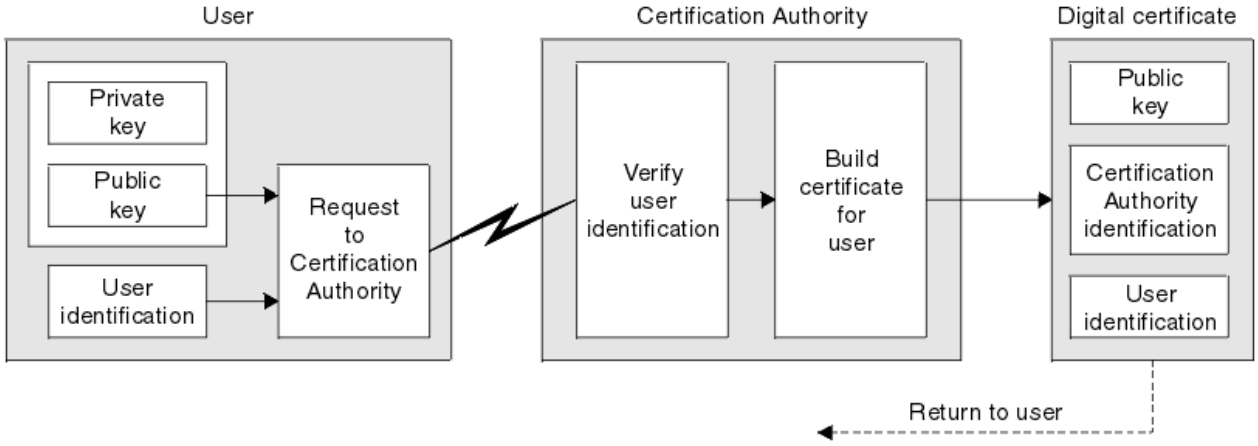
İlgili kavramlar
“Dijital sertifikada ne var?” sayfa 9
Sayısal sertifikalar, X.509 standardı tarafından belirlendiği şekilde, belirli bilgi parçalarını içerir.

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, UNIX, Linux®ve Windows sistemlerinde iKeyman aracı ve z/OSüzerinde RACF tool. 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:

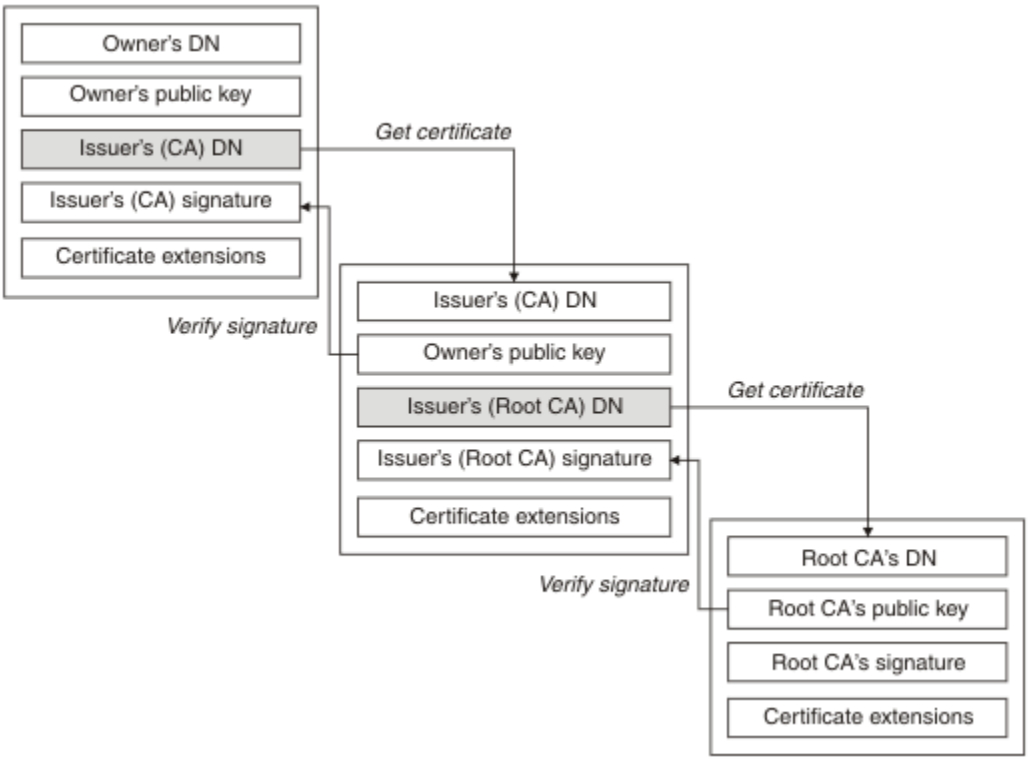
- "Kullanıcı kimliği", Konu Ayırt Edici Ad 'ı içerir.
- "Sertifika Yetkilisi tanıtıcısı", sertifikayı veren CA ' nın Ayırt Edici Adını içerir.
-

Sayısal sertifikalar, çizgede gösterilenler dışında ek alanlar içerir. Dijital sertifikadaki diğer alanlarla ilgili daha fazla bilgi için bkz. “Dijital sertifikada ne var?” sayfa 9.

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.

Sertifika kullanım süresinin dolduğu bir tanım için Sözlük ' e bakın.

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

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

WebSphere MQ , bir Online Certificate Status Protocol (OCSP) responder (yalnızca UNIX, Linux ve Windows sistemlerinde OCSP) yanıtlayıcısı için bir istek gönderilerek sertifikanın iptal edilip edilmediğini denetleyebilir. Alternatif olarak, LDAP sunucusundaki bir CRL ' ye erişebilirler. OCSP iptal ve CRL bilgileri bir Sertifika Yetkilisi tarafından yayınlanır. Daha fazla bilgi için “İptal edilen sertifikalarla çalışma” sayfa 146 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 bilgilerin doğrulandığını 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: SSL ve 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 WebSphere MQ hem SSL, hem de 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 WebSphere MQiçindeki güvenlik protokolleri” sayfa 22
IBM WebSphere MQ , ileti kanalları ve MQI kanalları için bağlantı düzeyinde güvenlik sağlamak üzere TLS (Transport Layer Security; İletim Katmanı Güvenliği) ve SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) protokollerini destekler.

Güvenli Yuva Katmanı (SSL) ve İletim Arabirimi Katmanı Güvenliği (TLS) kavramları

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

SSL ve TLS iletişim kuralları, 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.

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

A full list of CipherSpecs supported by IBM WebSphere MQ is provided at “CipherSpecs ' nin Belirtilmesi” sayfa 211.

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 ya da TLS el sıkışmasına genel bakış

SSL ya da TLS anlaşması, SSL ya da TLS istemcisinin ve sunucusunun, iletişim kurdukları gizli anahtarları oluşturmasını sağlar.

Bu bölümde, SSL ya da TLS istemcisinin ve sunucusunun birbiriyle iletişim kurmasını sağlayan adımlar yer alır.

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

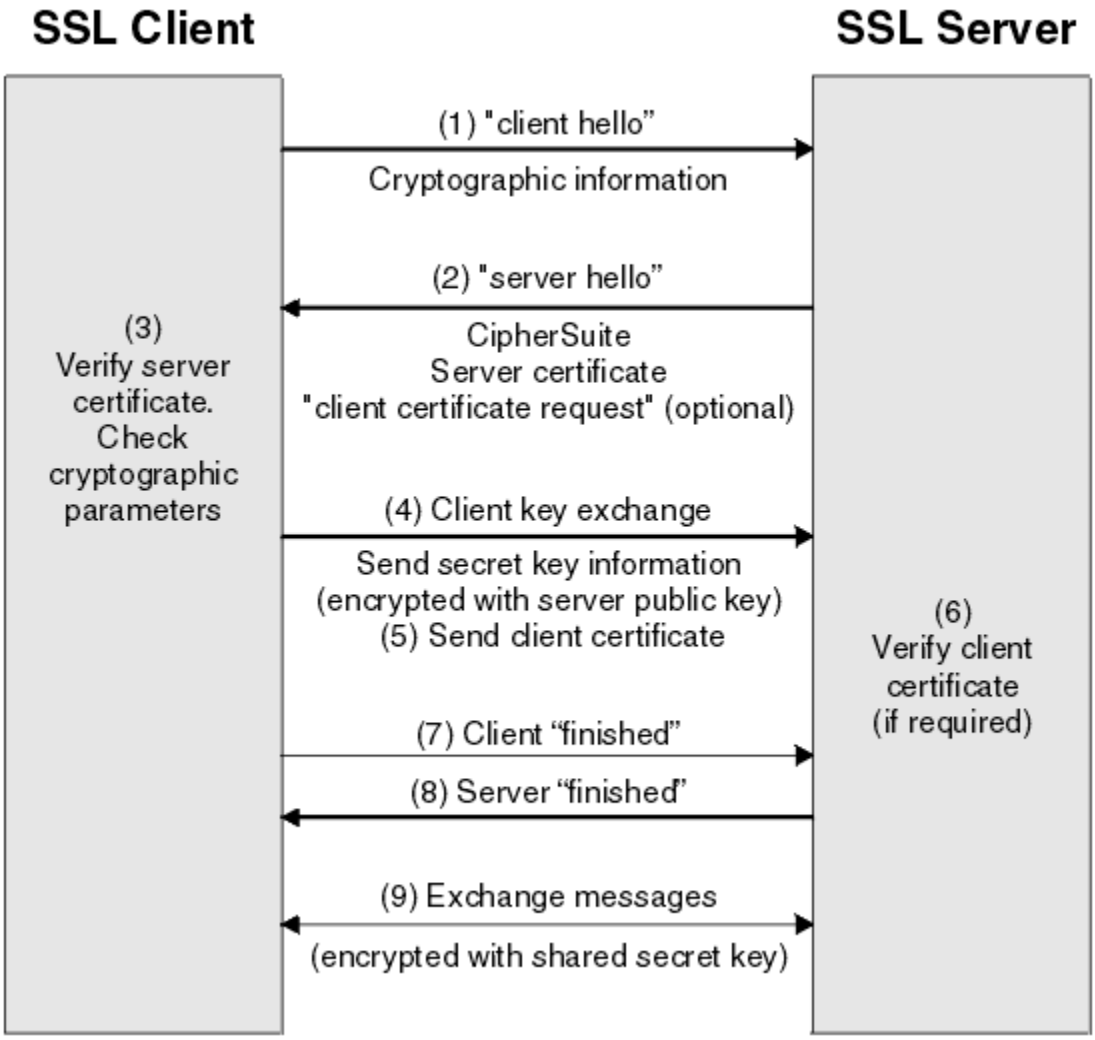
- Anahtar dağıtım sorununu önleyen, paylaşılan bir gizli anahtar oluşturmak için asimetrik şifreleme tekniklerini kullanın. Sonra SSL ya da TLS, asimetrik şifrelemeden daha hızlı olan iletilerin simetrik şifrelemesi için paylaşılan anahtarı kullanır.

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

Genel bakış alanında, SSL el sıkışmasına ilişkin adımlar aşağıdaki gibidir:

1. SSL ya da TLS istemcisi, SSL ya da 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. SSL ya da TLS sunucusu, sunucu tarafından seçilen CipherSuite iletisini, istemci tarafından sağlanan listeden, oturum tanıtıcısını ve başka bir rasgele byte dizesini 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. SSL ya da TLS istemcisi, sunucunun dijital sertifikasını doğrular. Daha fazla bilgi için “SSL ve TLS kimlik doğrulaması, kimlik doğrulama, gizlilik ve bütünlük sağlar” sayfa 16 başlıklı konuya bakın.
4. SSL ya da 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. SSL ya da TLS sunucusu bir "istemci sertifikası isteği"gönderdiyse, istemci, istemcinin sayısal sertifikasıyla birlikte şifrelenmiş bir rasgele byte dizgisi gönderir; istemcinin sayısal sertifikasıyla birlikte bir "dijital sertifika uyarısı yok"ya da.. Bu uyarı yalnızca bir uyarıdır, ancak bazı somutlamalarda, istemci kimlik doğrulaması zorunlu olduğunda tokalaşma başarısız olur.
6. SSL ya da TLS sunucusu, istemcinin sertifikasını doğrular. Daha fazla bilgi için “SSL ve TLS kimlik doğrulaması, kimlik doğrulama, gizlilik ve bütünlük sağlar” sayfa 16 başlıklı konuya bakın.
7. SSL ya da TLS istemcisi, sunucuyu, el sıkışmasının istemci bölümünün tamamlandığını belirten gizli anahtarla şifrelenmiş bir "bitiren" ileti gönderir.
8. SSL ya da TLS sunucusu, istemciyi, el sıkışmasının sunucu parçasının tamamlandığını belirten gizli anahtarla şifrelenmiş bir "bitmiş" ileti gönderir.
9. SSL ya da TLS oturumunun süresi boyunca sunucu ve istemci, paylaşılan gizli anahtarla simetrik olarak şifrelenmiş iletileri değiş tokuş edebilir.

Şekil 5 sayfa 16 , SSL ya da TLS el sıkışmasını gösterir.



Şekil 5. SSL ya da TLS el sıkışmasına genel bakış

SSL ve TLS kimlik doğrulaması, 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 ya da TLS el sıkışmasına genel bakış" sayfa 14.

SSL ve TLS kimlik doğrulaması sağlar

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 değiş tokası (genel bakımda "7" sayfa 15 ve "8" sayfa 15 adımları) kimlik doğrulamasının tamamlandığını onaylamıştır.

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

SSLor 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 , SSL ya da TLS istemcisine sertifika verir ve CA Y sertifikayı SSL ya da TLS sunucusuna gönderir:

Yalnızca sunucu kimlik doğrulaması için, SSL ya da TLS sunucusunun gereksinimleri:

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

ve SSL ya da TLS istemcisi gerekir:

- CA Yiçin CA sertifikası

SSL ya da TLS sunucusu istemci kimlik doğrulaması gerektiriyorsa, sunucu, istemcinin kişisel sertifikasını istemciye veren CA için, bu durumda CA X ' te istemcinin sayısal 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 SSL, hem de TLS sunucusu ve istemcisi, 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, SSL ya da TLS istemcisi sunucunun sertifikasını doğrular ve SSL ya da TLS sunucusu, istemcinin sertifikasını doğrular. Bu doğrulamanın dört yönü vardır:

1. Sayısal imza işaretlendiğinde (bkz. “SSL ve TLS ' de dijital imzalar” sayfa 18).
2. Sertifika zinciri imlenmiş; ara CA sertifikalarının olması gerekir (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 146).

Gizli anahtar ilk durumuna getirildi

SSL ya da TLS anlaşması sırasında, SSL ya da 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. Daha fazla bilgi için bkz. “İleti sindirimi ve dijital imzalar” sayfa 9 .

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.

SSL ve TLS ' nin gizliliği nasıl sağladığı

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

SSL ve TLS ' nin bütünlük sağlama şekli

SSL ve TLS, bir ileti özeti hesaplanarak veri bütünlüğü sağlar. Daha fazla bilgi için bkz. “İletilerin veri bütünlüğü” sayfa 220.

Use of SSL or TLS does ensure data integrity, provided that the CipherSpec in your channel definition uses a hash algorithm as described in the table in “CipherSpecs ' nin Belirtilmesi” sayfa 211.

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 ya da SSL ' nin her iki ucu da, iletişim kurabilmek için bağlantının aynı CipherSpec üzerinde kabul etmesi gerekir.

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

CipherSpecshakkında daha fazla bilgi için bkz. “CipherSpecs ' nin Belirtilmesi” sayfa 211.

CipherSuite , bir SSL ya da 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 ya da SSL bağlantısı için belirtildiğinde yalnızca belirli birleşimler geçerlidir. Geçerli bir CipherSuite adı, kullanılan algoritmaların bileşimini tanımlar. Örneğin, CipherSuite SSL_RSA_WITH_RC4_128_MD5 , şunları belirtir:

- RSA anahtar değiş tokası ve doğrulama algoritması
- 128 bit anahtar kullanan RC4 şifreleme algoritması
- MD5 MAC algoritması

Anahtar değiş tokası ve kimlik doğrulaması için birkaç algoritma vardır, ancak RSA algoritması şu anda en yaygın olarak kullanılan algoritmadır. Şifreleme algoritmalarında ve kullanılan MAC algoritmalarında daha fazla çeşitlilik vardır.

SSL ve TLS ' de dijital imzalar

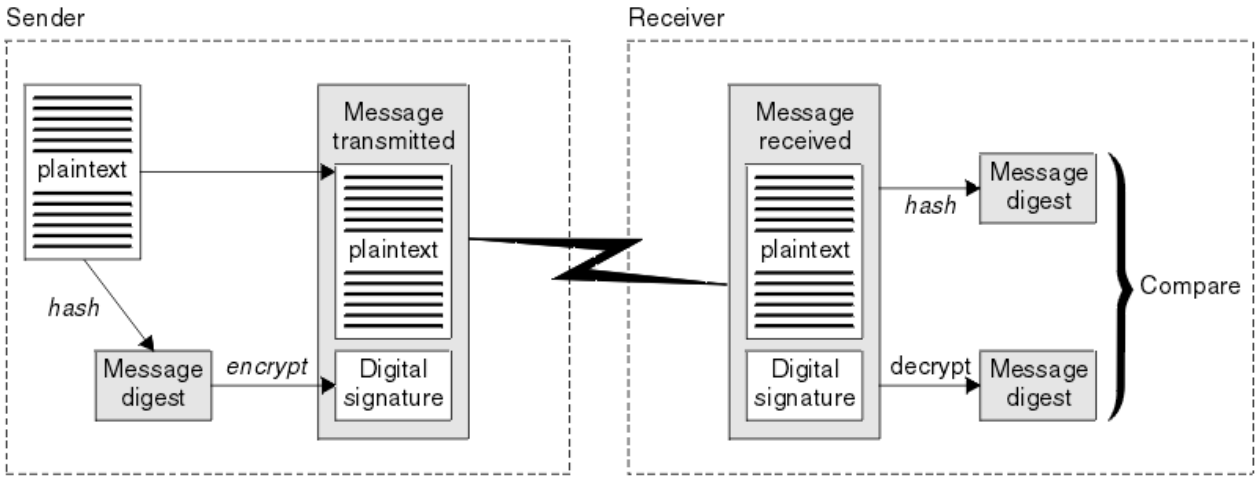
Dijital imza, bir iletinin gösterimini şifreleyerek oluşturulur. Şifreleme, imzaya ilişkin özel anahtarı kullanır ve verimlilik için genellikle iletinin kendisinden ziyade bir ileti özeti üzerinde çalışır.

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 WebSphere 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.

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 sürüm 1.2ile kullanılmak üzere bir Suite B uyumlu profil. Suite B uyumlu işlem için yapılandırıldığında, yukarıda listelenen yalnızca sınırlı şifreleme algoritmaları kümesi kullanılır.
2. TLS sürümü 1.0 ya da TLS sürümü 1.1ile kullanılacak 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.

Windows, UNIX ve Linux sistemlerinde, WebSphere MQ, Suite B uyumlu TLS 1.2 profiline uyumlu olacak şekilde yapılandırılabilir, ancak Suite B geçiş profilini desteklemez. Daha fazla bilgi için bkz. “NSA Suite B Cryptografi (IBM WebSphere MQ)” sayfa 30.

İlgili bilgiler

“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 WebSphere MQ güvenlik mekanizmaları

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

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

IBM WebSphere MQiçinde kimlik doğrulama ve kimlik doğrulama

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

Aşağıda, bir IBM WebSphere 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 5

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 WebSphere MQiçinde yetki

IBM WebSphere MQ ortamınızda hangi belirli kişileri ya da uygulamaları yapabilmeyi sınırlandırmak için yetki kullanabilirsiniz.

Aşağıda, IBM WebSphere MQ ortamında bazı yetki örnekleri bulunur:

- IBM WebSphere MQ kaynaklarını yönetmek için yalnızca yetkili bir yöneticinin komut 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 48 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 WebSphere MQiçinde denetim

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

Aşağıda, bir IBM WebSphere MQ ortamında denetim örnekleri bulunur:

- 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 WebSphere MQ' da gizlilik

İletileri şifreleyerek IBM WebSphere MQ uygulamasında gizliliği uygulayabilirsiniz.

Aşağıda, bir IBM WebSphere MQ ortamında gizliliğin nasıl sağlanabileceğiyle ilgili bazı örnekler bulunmaktadır:

- MCA gönderimi bir iletim kuyruğundan ileti aldıktan sonra, IBM WebSphere MQ iletiyi ağ üzerinden gönderilen MCA ' ya göndermeden önce şifrelemek için SSL ya da TLS kullanır. Kanalın diğer ucunda, MCA ' nın hedef kuyruğuna yerleştirmeden önce iletinin şifresi çözülür.

- İletiler yerel bir kuyruğun üzerinde saklanırken, IBM WebSphere 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 IBM WebSphere MQ Advanced Message Security olanağını kullanabilirsiniz.

İlgili kavramlar

"Gizlilik" sayfa 6
Gizlilik hizmeti, hassas bilgileri yetkisiz açıklamalardan korur.

IBM WebSphere MQiçindeki veri bütünlüğü

Bir iletinin değiştirilip değiştirilmediğini saptamak için veri bütünlüğü hizmetini kullanabilirsiniz.

Aşağıda, bir IBM WebSphere MQ ortamında veri bütünlüğünün nasıl sağlanabileceğiyle ilgili bazı örnekler bulunmaktadır:

- Bir iletinin içeriğinin bir ağ üzerinden iletilirken kasıtlı olarak değiştirilip değiştirilmediğini saptamak için SSL ya da TLS ' yi kullanabilirsiniz. SSL ve TLS ' de, ileti özet algoritmasında, değiştirilen iletilerin aktarmaya ilişkin algılama olanağı sağlanır. Tüm IBM WebSphere MQ CipherSpecs , ileti verisi bütünlüğü sağlamayan TLS_RSA_WIT_NULL_NULL dışında bir ileti özeti algoritması sağlar.
- İletiler yerel bir kuyruğun üzerinde saklanırken, IBM WebSphere 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 IBM WebSphere MQ 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.

İlgili kavramlar

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

IBM WebSphere MQiçinde şifreleme

IBM WebSphere MQ , Güvenli Yuva Katmanı (SSL) ve İletim Güvenliği Katmanı (TLS) iletişim kurallarını kullanarak şifreleme sağlar.

Daha fazla bilgi için bkz. "IBM WebSphere MQiçindeki güvenlik protokolleri" sayfa 22.

İlgili kavramlar

"Şifreleme kavramları" sayfa 7
Bu konu derlemi, WebSphere MQiçin geçerli olan şifreleme kavramlarını açıklar.

IBM WebSphere MQiçindeki güvenlik protokolleri

IBM WebSphere MQ , ileti kanalları ve MQI kanalları için bağlantı düzeyinde güvenlik sağlamak üzere TLS (Transport Layer Security; İletim Katmanı Güvenliği) ve SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) protokollerini destekler.

İleti kanalları ve MQI kanalları, bağlantı düzeyinde güvenlik sağlamak için SSL ya da TLS iletişim kuralını kullanabilir.Çağıran MCA bir SSL ya da TLS istemcisinden ve yanıt veren MCA bir SSL ya da TLS sunucudur. WebSphere MQ supports Version 3.0 of the SSL protocol and Version 1.0 and Version 1.2 of the Transport Layer Security (TLS) protocol. SSL ya da protokol tarafından, kanal tanımlamasının bir parçası olarak bir CipherSpec belirterek kullanılan şifreleme algoritmalarını belirtiyorsunuz.

Bir ileti kanalının her iki ucunda ve bir MQI kanalının sunucu ucunda, MCA bağlı olduğu kuyruk yöneticisi adına hareket eder. SSL ya da TLS anlaşması sırasında MCA, kuyruk yöneticisinin dijital sertifikasını, kanalın diğer ucunda bulunan iş ortağı MCA ' ya gönderir. Bir MQI kanalının istemci ucunda bulunan WebSphere MQ kodu, WebSphere MQ istemcisi uygulamasının kullanıcısı adına hareket eder. SSL ya da TLS anlaşması sırasında, WebSphere MQ kodu, kullanıcının dijital sertifikasını MQI kanalının sunucu ucunda MCA ' ya gönderir.

Kuyruk yöneticileri ve WebSphere MQ istemcisi kullanıcılarının, kanalın sunucu tarafında SSSCUATH (gerekli) belirtilmedikçe, SSL ya da TLS istemcileri olarak işlem yaparken kendileriyle ilişkilendirilmiş kişisel sayısal sertifikalara sahip olmak zorunda değildir.

Dijital sertifikalar bir *anahtar havuzunda* depolanır. The queue manager attribute *SSLKeyRepository* specifies the location of the key repository that holds the queue manager's digital certificate. On a WebSphere MQ client system, the MQSSLKEYR environment variable specifies the location of the key repository that holds the user's digital certificate. Diğer bir seçenek olarak, bir WebSphere MQ istemcisi uygulaması, SSL ve TLS yapılandırma seçenekleri yapısının *KeyRepository* alanında, MQCONNX çağrısında MQSCO ' nun yerini belirleyebilir. Temel havuzlarla ilgili daha fazla bilgi ve konumlarının nasıl belirleneceği hakkında daha fazla bilgi için ilgili konulara bakın.

İlgili kavramlar

"Şifreleme güvenlik iletişim kuralları: SSL ve 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 WebSphere MQ hem SSL, hem de TLS ' yi destekler.

SSL ve TLS içinIBM WebSphere MQ desteği

IBM WebSphere MQ , Güvenli Yuva Katmanı (SSL) iletişim kuralını ve TLS (Transport Layer Security; İletim Katmanı Güvenliği) protokolünü destekler.

SSL ve TLS iletişim kurallarıyla ilgili ek bilgi için ilgili bilgilere bakın.

IBM WebSphere MQ , SSL Sürüm 3.0 ve TLS 1.0 ve TLS 1.2:

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

UNIX, Linux, and Windowsve HP Integrity NonStop Server sistemleri
UNIX, Linux, and Windowsve HP Integrity NonStop Server sistemleri için, SSL ve TLS desteği IBM WebSphere MQile birlikte kurulur.

IBM WebSphere MQ SSL ve TLS desteğine ilişkin önkoşullarla ilgili bilgi için bkz. IBM WebSphere MQiçin Sistem Gereksinimleri.

SSL ya da TLS anahtarı havuzu
Kimliği karşılıklı olarak doğrulanmış bir SSL ya da TLS bağlantısı, bağlantının her ucunda bir anahtar havuzu (farklı platformlarda farklı adlarla bilinebilir) 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. SSL ve TLS ' yi destekleyen altyapılarda ve ortamlarda kullanılan özel mağaza adları şunlardır:

Java ve JMS	anahtar deposu ve güvenilirlik deposu
 Windows , UNIX and Linux sistemleri	anahtar veri tabanı dosyası

Daha fazla bilgi için bkz. "dijital sertifikalar" sayfa 9 ve "Güvenli Yuva Katmanı (SSL) ve İletim Arabirimi Katmanı Güvenliği (TLS) kavramları" sayfa 14.

Kimliği karşılıklı olarak doğrulanmış bir SSL ya da TLS bağlantısı, bağlantının her bir ucunda bir anahtar havuzu gerektirir. Anahtar havuzu şunları 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 WebSphere MQ MQI istemcisi ile ilişkilendirin. Karşılıklı kimlik doğrulaması gerekirse, SSL ya da TLS istemcisinde 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 WebSphere MQ anahtar havuzlarının korunması" sayfa 24.

Anahtar havuzunun yeri, kullanmakta olduğunuz altyapıya bağlıdır:

Windows, UNIX and Linux sistemleri

Windows, UNIX and Linux sistemlerinde 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 WebSphere MQ varsayılan konuma kurulduysa, Pencereler üzerindeki eşdeğer yol `C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\key.kdb`olur.

Windows , UNIX and Linux sistemlerinde, her anahtar veri tabanı dosyasının 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: Windows, UNIX and Linux sistemlerinde, PKCS #11 şifreleme donanım kartları, anahtar veritabanı dosyasında başka bir şekilde tutulan sertifikaları ve anahtarları içerebilir. PKCS #11 kartlarında sertifikalar ve anahtarlar tutulduğunda, WebSphere MQ yine de hem anahtar veritabanı dosyasına hem de parola şifreleme dosyasına erişim gerektirir.

Windows ve UNIX sistemlerinde, anahtar veritabanı, kuyruk yöneticisi ya da WebSphere MQ MQI istemcisiyle ilişkilendirilmiş kişisel sertifika için özel anahtarı da içerir.

IBM WebSphere MQ anahtar havuzlarının korunması

IBM WebSphere 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 WebSphere 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.

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.

Ayrıca, PCF komutlarını ya da WebSphere MQ Explorer olanağını kullanarak bir anahtar havuzunu da yenileyebilirsiniz. For more information, see the MQCMD_REFRESH_SECURITY komutu and the topic *SSL ya da TLS Güvenliği yenileniyor* in the WebSphere MQ Explorer section of this product documentation.

İlgili kavramlar

“İstemcinin SSL anahtar havuzu içerikleri ve SSL ayarlarına ilişkin görünümü yenileniyor” sayfa 25
İstemci uygulamasını anahtar havuzunun yenilenmiş içeriğiyle güncellemek için istemci uygulamasını durdurmanız ve yeniden başlatmanız gerekir.

İstemcinin SSL anahtar havuzu içerikleri ve SSL ayarlarına ilişkin görünümü yenileniyor
İstemci uygulamasını anahtar havuzunun yenilenmiş içeriğiyle güncellemek için istemci uygulamasını durdurmanız ve yeniden başlatmanız gerekir.

Bir WebSphere MQ istemcisinde güvenliği yenileyemezsiniz; ek bilgi için, istemciler için REFRESH SECURITY TYPE (SSL) komutunun eşdeğer bir değeri yoktur (REFRESH SECURITYkonusuna bakın).

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 24
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.

Federal Bilgi İşleme Standartları (FIPS)
Bu konuda, US National Institute of Standards and Technology 'nin Federal Bilgi İşleme Standartları (FIPS) Cryptomol Validation Programı ve SSL ya da TLS kanallarında, Pencereler, UNIX and Linuxve z/OS sistemleri için kullanılabilecek şifreleme işlevleri açıklanmaktadır.

The FIPS 140-2 compliance of an IBM WebSphere MQ SSL or TLS connection on UNIX, Linux, and Windows systems is found here “ UNIX, Linuxve Windows için Federal Bilgi İşleme Standartları (FIPS)” sayfa 26.

Şifreleme donanımı mevcutsa, IBM WebSphere 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 WebSphere MQ en son standardı uygulamak için de güncellenir. Sonuç olarak, bakım uyguladıktan sonra davranışlardaki değişiklikleri görebilirsiniz.

İlgili kavramlar

“MQI istemcisinde çalıştırma sırasında yalnızca FIPS onaylı CipherSpecs ' in kullanıldığını belirtme” sayfa 105
Anahtar havuzlarınızı FIPS uyumlu yazılım kullanarak yaratın ve kanalın FIPS onaylı CipherSpecs' ı kullanması gerektiğini belirtin.

“iKeyman, iKeycmd, runmqakm ve runmqckm komutunu kullanma” sayfa 111
On UNIX, Linux and Pencereler systems, manage keys and digital certificates with the iKeyman GUI or from the command line using iKeycmd or runmqakm.

İlgili görevler

Java için WebSphere MQ sınıflarında SSL ' nin etkinleştirilmesi
JMS için WebSphere MQ sınıflarıyla SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) kullanılıyor

İlgili başvurular

JMS nesnelerinin SSL özellikleri

İlgili bilgiler

“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.

UNIX, Linuxve Windows için Federal Bilgi İşleme Standartları (FIPS)

Windows, UNIX and Linux sistemlerinde bir SSL ya da TLS kanalında şifreleme gerektiğinde, WebSphere 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 geçti.

Windows UNIX and Linux sistemlerinde WebSphere MQ SSL ya da TLS bağlantısının FIPS 140-2 uyumluluğu aşağıdaki gibidir:

- Aşağıdaki koşullar karşılandıysa, tüm IBM WebSphere 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 WebSphere MQ MQI 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.
  - 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 Java uygulamalarına ilişkin IBM WebSphere MQ sınıfları için, bağlantı JRE ' nin SSL ve 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 JMS uygulamalarına ilişkin IBM WebSphere MQ sınıfları için, bağlantı JRE ' nin SSL ve 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 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.
- Yönetilmeyen .NET istemci uygulamaları için, bağlantı GSKit kullanıyor ve aşağıdaki koşullar karşılandığında FIPS uyumludur:

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

Desteklenen tüm AIX, Linux, HP-UX, Solaris, Windowsve z/OS platformları, her bir düzeltme paketinde ya da yenileme paketinde yer alan benioku dosyasında belirtilenler dışında, FIPS 140-2 sertifikalıdır.

GSKit kullanan SSL ve 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 WebSphere 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. 64 bit kod etkilenmediği için, bu sorunu çözmek için FIPS 140-2 uyumluluğunu geçersiz kılın ya da istemci uygulamasını 64 bit yeniden derleyin.

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

WebSphere MQ FIPS 140-2 ile uyumlu çalışacak şekilde yapılandırıldığında, Triple DES (3DES) CipherSpecsile ilgili 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, WebSphere 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 anahtarlarının ilk durumuna getirilmesi” sayfa 217.

WebSphere 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 sırasında yalnızca FIPS onaylı CipherSpecs ' in kullanıldığını belirtme” sayfa 105
Anahtar havuzlarınızı FIPS uyumlu yazılım kullanarak yaratın ve kanalın FIPS onaylı CipherSpecs' ı kullanması gerektiğini belirtin.

“iKeyman, iKeycmd, runmqakm ve runmqckm komutunu kullanma” sayfa 111
On UNIX, Linux and Pencereler systems, manage keys and digital certificates with the iKeyman GUI or from the command line using iKeycmd or runmqakm.

İlgili görevler

WebSphere MQ sınıflarında Java için SSL ' nin etkinleştirilmesi

JMS için WebSphere MQ sınıflarıyla SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) kullanılması

İlgili başvurular

JMS nesnelerinin SSL özellikleri

İlgili bilgiler

“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 WebSphere MQ MQI istemcisine SSL ve TLS
IBM WebSphere MQ , istemcilerde SSL ve TLS ' yi destekler. SSL ya da TLS kullanımını çeşitli şekillerde uyarlayabilirsiniz.

IBM WebSphere MQ , Windows, UNIX and Linux sistemlerindeki IBM WebSphere MQ MQI istemcileri için SSL ve TLS desteği sağlar. If you are using IBM WebSphere MQ classes for Java, see Java için WebSphere MQ sınıflarının kullanılması and if you are using IBM WebSphere MQ classes for JMS, see JMS için WebSphere MQ sınıflarının kullanılması. Bu bölümün geri kalan kısmı Java ya da JMS ortamları için geçerli değildir.

IBM WebSphere MQ istemcisi yapılandırma dosyanızın MQSSLKEYR değeriyle ya da uygulamanızın bir MQCONNX çağrısı yaptığı bir IBM WebSphere MQ MQI istemcisi için anahtar havuzu belirtebilirsiniz. Bir kanalın SSL kullanacağını belirtmek için üç seçeneğiniz vardır:

- Kanal tanımlama çizelgesinin kullanılması
- MQCONNX çağrısında SSL yapılandırma seçenekleri yapısının kullanılması, MQSCO
- Active Directory ' in (Pencereler sistemlerinde) kullanılması

Bir kanala SSL kullanacağını belirtmek için MQSERVER ortam değişkenini kullanamazsınız.

Kanalın diğer ucunda SSL belirtilmediği sürece, var olan IBM WebSphere MQ MQI istemcisi uygulamalarınızı SSL olmadan çalıştırmaya devam edebilirsiniz.

Bir istemci makinesinde SSL Anahtar Havuzu, SSL Anahtar 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 SSL bağlantılarını sona erdirmeniz gerekir. Tüm bağlantılar sona erdikten sonra, SSL kanallarını yeniden başlatın. Tüm yeni SSL ayarları kullanılır. Bu ayarlar, kuyruk yöneticisi sistemlerinde REFRESH SECURITY TYPE (SSL) komutuna göre yenilenenlere benzer.

IBM WebSphere MQ MQI istemciniz bir Windows, UNIX and Linux sisteminde şifreleme donanımıyla çalışıyorsa, bu donanımı MQSSLCRYP ortam değişkeniyle yapılandırırdınız. 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.

SSL gizli anahtarı ilk duruma getirme ve FIPS ' ler IBM WebSphere MQ MQI istemcilerinde desteklenir. Daha fazla bilgi için bkz. “SSL ve TLS gizli anahtarlarının ilk durumuna getirilmesi” sayfa 217 ve “ UNIX, Linuxve Windows için Federal Bilgi İşleme Standartları (FIPS)” sayfa 26.

IBM WebSphere MQ MQI istemcilerine ilişkin SSL desteğine ilişkin ek bilgi edinmek için “IBM WebSphere MQ MQI istemci güvenliğinin ayarlanması” sayfa 105 konusuna bakın.

İlgili görevler

Yapılandırma dosyası kullanarak istemci yapılandırılması

Bir MQI kanalının SSL kullandığını belirtme

Bir MQI kanalının SSL kullanmasını sağlamak için, istemci-bağlantı kanalının *SSLCipherSpec* özniteliğinin değeri, istemci altyapısında IBM WebSphere MQ tarafından desteklenen bir CipherSpec 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 WebSphere MQ MQI istemcisi uygulaması bir MQCONNX çağrısı yayınlandığında.

   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 Pencereler 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.

Örneğin, bir istemci uygulaması MQCONNX çağrısında bir MQCD yapısında istemci bağlantısı kanal tanımlaması sağlıyorsa, bu tanım WebSphere MQ istemcisi tarafından erişilebilen bir istemci kanalı tanımlama çizelgesindeki girişlere tercihte kullanılır.

SSL 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 WebSphere MQ MQI istemcisi için bir CipherSpec belirtme” sayfa 217
Bir IBM WebSphere MQ MQI istemcisi için bir CipherSpec belirtme üç seçeneğiniz vardır.

IBM WebSphere MQiçindeCipherSpecs ve CipherSuites

IBM WebSphere MQ , hem SSL, hem TLS CipherSpecs, hem de RSA ve Diffie-Hellman algoritmalarını destekler.

WebSphere MQ , SSL V3 ve TLS V1.0 ve V1.2 CipherSpecs' ı destekler.

WebSphere MQ , RSA ve Diffie-Hellman anahtar değişimi ve kimlik doğrulama algoritmalarını destekler. SSL el sıkışması 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 WebSphere MQ)
Bu konuda, Windows, Linuxve UNIX sistemlerinde Suite B uyumlu TLS 1.2 profiline uygun olarak IBM WebSphere MQ ' un nasıl yapılandırılacağı hakkında bilgiler yer alır.

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 WebSphere MQ en son standardı uygulamak için de güncellenir. Sonuç olarak, bakım uyguladıktan sonra davranışlardaki değişiklikleri görebilirsiniz. IBM WebSphere MQ Version 7.5 benioku dosyası, her bir ürün bakım düzeyi tarafından uygulanan Suite B ' nin sürümünü listeler. Suite B uyumluluğunu zorunlu kılacak IBM WebSphere MQ ' u yapılandırırsanız, bakım uygulamayı planlarken her zaman benioku dosyasına bakın (bkz. IBM MQ, WebSphere MQve MQSeries ürünleri READMES).

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

Çizelge 1. 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 WebSphere MQ ' in varsayılan davranışı Suite B standardına uymamasına rağmen, IBM WebSphere MQ , Windows, UNIX ve Linux sistemlerinde güvenlik düzeylerine ya da her iki güvenlik düzeyine uyacak şekilde yapılandırılabilir. Following the successful configuration of IBM WebSphere 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.

WebSphere MQ CipherSpecshakkında daha fazla bilgi için bkz. “CipherSpecs ' nin Belirtilmesi” sayfa 211

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. Therefore WebSphere MQ must be configured to use certificates whose digital signature algorithm and public key type are allowed by the configured Suite B security level of the remote partner. 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: iKeycmd ve **iKeyman** araçları, Suite B uyumlu işlem için dijital sertifikaların oluşturulmasını desteklemez.

Dijital sertifikalar yaratılması ve istenmesi

Suite B testine ilişkin kendinden onaylı bir dijital sertifika oluşturmak için bkz. “UNIX, Linux, and Windows sistemlerinde kendinden onaylı bir kişisel sertifika oluşturma” sayfa 119

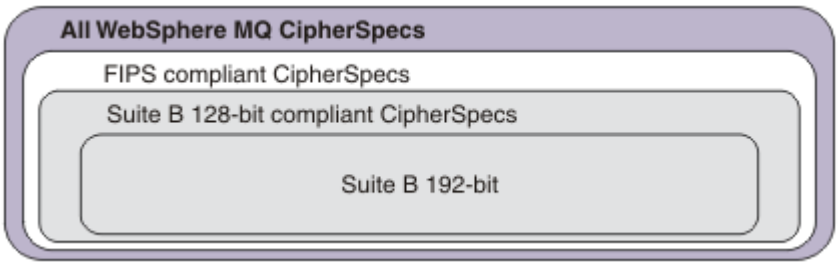
Takım B üretim kullanımı için CA tarafından imzalanmış bir dijital sertifika istemek üzere bkz. “UNIX, Linux, and Windows sistemleri üzerinde kişisel sertifika isteme” sayfa 121.

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 WebSphere MQ is configured for FIPS 140-2 compliant operation. Bu nedenle, WebSphere MQ ' nun hem FIPS hem de Suite B uyumluluğu için aynı anda yapılandırılması mümkündür. Bu durumda, her iki kısıtlama kümesi de geçerlidir.

Aşağıdaki çizge, bu alt kümeler arasındaki ilişkiyi



göstermektedir:

Suite B uyumlu işlem için WebSphere MQ ' un yapılandırılması

For information about how to configure IBM WebSphere MQ on Windows, UNIX and Linux for Suite B compliant operation, see “Suite B için IBM WebSphere MQ ' nin yapılandırılması” sayfa 32.

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

İlgili kavramlar

“MQI istemcisinde çalıştırma sırasında yalnızca FIPS onaylı CipherSpecs ' in kullanıldığını belirtme” sayfa 105

Anahtar havuzlarınızı FIPS uyumlu yazılım kullanarak yaratın ve kanalın FIPS onaylı CipherSpecs' ı kullanması gerektiğini belirtin.

Suite B için IBM WebSphere MQ ' nin yapılandırılması

IBM WebSphere MQ , NSA Suite B standardındaki standart UNIX, Linux, and Windows sistemlerinde çalışmak üzere yapılandırılabilir.

Suite B, güvenli bir güvenlik düzeyi sağlamak için etkinleştirilmiş şifreleme algoritmaları kümesini kısıtlar. IBM WebSphere MQ geliştirilmiş bir güvenlik düzeyi sağlamak üzere Suite B ' ye uygun olarak çalışacak şekilde yapılandırılabilir. Takım B ile ilgili daha fazla bilgi için bkz. “Ulusal Güvenlik Ajansı (NSA) Suite B Cryptography” sayfa 19. Suite B yapılandırması ve bu yapılandırmayla SSL ve TLS kanalları üzerindeki etkisi hakkında daha fazla bilgi için bkz. “NSA Suite B Cryptografi (IBM WebSphere MQ)” sayfa 30.

Kuyruk yöneticisi

For a queue manager, use the command **ALTER QMGR** with the parameter **SUITEB** to set the values appropriate for your required level of security. Ek bilgi için ALTER QMGRbaşlıklı konuya bakın.

You can also use the PCF **MQCMD_CHANGE_Q_MGR** command with the **MQIA_SUITE_B_STRENGTH** parameter to configure the queue manager for Suite B compliant operation

MQI istemcisi

Varsayılan olarak, MQI istemcileri Suite B uyumluluğunu zorunlu kılmaz. Aşağıdaki seçeneklerden birini yürüterek, MQI istemcisine Suite B uyumluluğu için etkinleştirebilirsiniz:

1. Aşağıdaki değerlerden birine ya da birkaçına MQCONNX çağrısında bulunan MQSCO yapısındaki **EncryptionPolicySuiteB** alanı tanımlanarak:
   - MQ_SUITE_B_NONE
   - MQ_SUITE_B_128_BIT
   - MQ_SUITE_B_192_BIT

   Diğer herhangi bir değerle MQ_SUITE_B_NONE kullanılması geçersizdir.
2. MQSUITEB ortam değişkenini aşağıdaki değerlerden birine ya da birkaçına ayarlayarak şunları kullanın:
   - YOK
   - 128_BIT
   - 192_BIT

   Virgülle ayrılmış bir liste kullanarak birden çok değer belirtebilirsiniz. NONE değerini başka bir değerle birlikte kullanmak geçersizdir.
3. MQI istemcisi yapılandırma dosyasının SSL kısmında bulunan **EncryptionPolicySuiteB** özniteliğini aşağıdaki değerlerden birine ya da birkaçına ayarlayın:
   - YOK
   - 128_BIT
   - 192_BIT

   Virgülle ayrılmış bir liste kullanarak birden çok değer belirtebilirsiniz. NONE (Yok) değerinin başka bir değeri kullanılması geçersiz.

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

MQSCO yapısının tam ayrıntıları için bakınız: MQSCO-SSL configuration options.

İstemci yapılandırma dosyasında Suite B ' nin kullanımıyla ilgili daha fazla bilgi için bkz. İstemci yapılandırma dosyasının SSL kısmı .

MQSUITEB ortam değişkeninin kullanımıyla ilgili daha fazla bilgi için Ortam Değişkenleribaşlıklı konuya bakın.

.NET

.NET yönetilmeyen istemciler için **MQC.ENCRYPTION_POLICY_SUITE_B** özelliği, gereken Suite B güvenliğinin tipini belirtir.

.NET için IBM WebSphere MQ sınıflarında kullanılan Suite B ile ilgili bilgi edinmek için bakınız: MQEnvironment .NET class.

IBM WebSphere 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 altyapılarda Java ve JMS uygulamaları için, sertifika geçerlilik denetimi ilkesi Java Runtime Environment 'ın JSSE bileşenine bağlıdır. Sertifika doğrulama ilkesi hakkında daha fazla bilgi için, JRE belgelerinize 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 systems, see “IBM WebSphere MQiçinde sertifika geçerlilik denetimi ilkelerinin yapılandırılması” sayfa 33. Temel ve Standart sertifika doğrulama ilkeleri arasındaki farklar hakkında daha fazla bilgi için bkz. Sertifika doğrulama ve güvenilirlik ilkesi tasarımı UNIX, Linux ve Windows sistemleri .

IBM WebSphere MQiçinde sertifika geçerlilik denetimi ilkelerinin yapılandırılması
Uzak iş ortağı sistemlerinden alınan sayısal sertifikaların geçerliliğini denetlemek için kullanılan SSL/TLS sertifika geçerlilik denetimi ilkesinin kullanılacağını dört şekilde belirleyebilirsiniz.

Kuyruk yöneticisinde, sertifika geçerlilik denetimi ilkesi aşağıdaki şekillerde ayarlanabilir:

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

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

1. İstemci MQSCO yapısındaki *CertificateValPolicy* (CertificateVal) alanını kullanma. Bu alanın kullanılmasına ilişkin ek bilgi için MQSCO-SSL configuration optionsbaşlıklı konuya bakın.
2. İstemci ortam değişkeni *MQCERTVPOL*kullanılıyor. Bu değişkeni kullanma hakkında daha fazla bilgi için bkz. MQCERTVPOL .
3. İstemci SSL stanza ayarlama parametresi ayarı, *CertificateValPolicy*(CertificateVal) ilkesi Bu ayarın kullanılmasıyla ilgili ek bilgi için İstemci yapılanış kütüğünün SSL kısmına bakın .

Sertifika doğrulama ilkeleriyle ilgili daha fazla bilgi için bkz. “IBM WebSphere MQiçindeki sertifika geçerlilik denetimi ilkeleri” sayfa 33.

Digital certificates and CipherSpec compatibility in IBM WebSphere MQ
Bu konuda, IBM WebSphere MQiçindeki CipherSpecs ve dijital sertifikalar arasındaki ilişkiyi sıralayarak uygun CipherSpecs ve güvenlik ilkeniz için dijital sertifikalar nasıl seçileceği hakkında bilgi sağlanmaktadır.

Önceki IBM WebSphere MQyayınlarında, desteklenen tüm SSL ve TLS CipherSpecs , dijital imzalar ve anahtar anlaşması için RSA algoritmasını kullandı. Desteklenen tüm dijital sertifika tipleri, desteklenen tüm CipherSpecsile uyumlu olduğu için, dijital sertifikaları değiştirmeye gerek duymadan herhangi bir kanala ilişkin CipherSpec ' i değiştirmek mümkün oldu.

IBM WebSphere MQ v7.5 'te desteklenen CipherSpecs ' in yalnızca bir alt kümesi, desteklenen tüm sayısal sertifikalar ile kullanılabilir. Bu nedenle, sayısal sertifikanız için uygun bir CipherSpec seçmeniz gerekir. Benzer bir şekilde, kuruluşunuzun güvenlik ilkesi belirli bir CipherSpec kullanmanızı gerektiriyorsa, o CipherSpeciçin uygun bir dijital sertifika edinmeniz gerekir.

MD5 dijital imza algoritması ve TLS 1.2

TLS 1.2 protokolü kullanıldığında, MD5 algoritması kullanılarak imzalanmış dijital sertifikalar reddedilir. Bunun nedeni, şu anda MD5 algoritmasının birçok şifreleme analisti tarafından zayıf kabul edilmesi ve kullanımının genellikle kullanılması önerilmemektedir. TLS 1.2 protokolünde daha yeni CipherSpecs kullanmak istiyorsanız, dijital sertifikaların dijital imzalarında MD5 algoritmasını kullanmadığından emin olun. Older CipherSpecs which use the SSL 3.0 and TLS 1.0 protocols are not subject to this restriction and can continue to use certificates with MD5 digital signatures.

Belirli bir sertifika ilişkin dijital imza algoritmasını görüntülemek için **runmqakm** komutunu kullanabilirsiniz:

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

Burada `cert_label` , görüntülemek için ihtiyacınız olan dijital imza algoritmasının sertifika etiketidir.

Not: Although the **iKeycmd (runmqckm)** tool and the **iKeyman (strmqikm)** GUI can be used to view a selection of digital signature algorithms, the **runmqakm** tool provides a wider range.

runmqakm komutunun yürütülmesi, belirtilen imza algoritmasının kullanımını görüntüleyen çıktı üretecektir:

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

```
    B0 21 0B A8 B2 59 5B 24 59 50 44 89 DC 78 19 51
Trust Status : Enabled
```

`Signature Algorithm` satırı, `MD5WithRSASignature` algoritmasının kullanıldığını gösterir. Bu algoritma MD5 üzerine kuruludur ve bu nedenle bu sayısal sertifika TLS 1.2 CipherSpecsile kullanılamaz.

Eliptik Eğri ve RSA CipherSpecsile birlikte çalışabilirlik

Tüm CipherSpecs , tüm sayısal sertifikalarla birlikte kullanılamaz. CipherSpec ad önekiyle gösterilen üç tip CipherSpecvardır. Her CipherSpec tipi, kullanılabilecek sayısal sertifika tipi üzerinde farklı sınırlamalar ortaya koyar. Bu kısıtlamalar tüm WebSphere MQ SSL ve TLS bağlantıları için geçerlidir, ancak özellikle Eliptik Eğri Şifrelemesi kullanıcıları için geçerlidir.

CipherSpecs ve dijital sertifikalar arasındaki ilişkiler aşağıdaki tabloda özetlenir:

Çizelge 2. CipherSpecs ve dijital sertifikalar arasındaki ilişkiler

Tip	CipherSpec Ad Öneki	Tanım	Gerekli genel anahtar tipi	Dijital imza şifreleme algoritması	Gizli anahtar kuruluş yöntemi
1	ECDHE_ECDSA_	Eliptik Eğri ortak anahtarları, Eliptik Eğri gizli anahtarları ve Eliptik Eğri sayısal imza algoritmaları kullananCipher Specs .	Eliptik Eğrisi	ECDSA	ECDHE
2	ECDHE_RSA_	RSA ortak anahtarları, Eliptik Eğri gizli anahtarları ve Eliptik Eğri sayısal imza algoritmaları kullananCipher Specs .	RSA	RSA	ECDHE
3	(Diğerleri)	RSA genel anahtarlarını ve RSA dijital imza algoritmalarını kullananCipher Specs .	RSA	RSA	RSA

Not: Tip 1 ve 2 CipherSpecs yalnızca, UNIX, Linux, and Windows altyapılarında WebSphere MQ kuyruk yöneticileri ve MQI istemcileri tarafından desteklenir.

Gereken genel anahtar tipi kolonu, kişisel sertifikana ilişkin her CipherSpectipini kullanırken sahip olması gereken genel anahtar tipini gösterir. Kişisel sertifika, kuyruk yöneticisini ya da istemciyi uzak ortağına tanıtan son varlık sertifikasıdır.

Sayısal imza şifreleme algoritması, eşdüzey denetimi doğrulamak için kullanılan şifreleme algoritmasına gönderme yapar. Sayısal imzayı hesaplamak için şifreleme algoritması MD5, SHA-1 ya da SHA-256 gibi bir HASH algoritmasıyla birlikte kullanılır. Kullanılabilecek çeşitli dijital imza algoritmaları vardır; örneğin, "RSA with MD5" ya da "ECDSA with SHA-256". Tabloda ECDSA, ECDSA ' yı kullanan dijital imza algoritmaları kümesini ifade eder; RSA, RSA kullanan dijital imza algoritmaları kümesini belirtir. Belirtilen

şifreleme algoritmasına dayalı olması koşuluyla, sette desteklenen herhangi bir dijital imza algoritması kullanılabilir.

Tip 1 CipherSpecs , kişisel sertifikana bir Eliptik Eğri ortak anahtarı olmasını zorunlu kılmalıdır. Bu CipherSpecs kullanıldığında, bağlantıya ilişkin gizli anahtarı oluşturmak için Eliptik Eğri Diffie Hellman Ephemeral anahtar sözleşmesi kullanılır.

Tip 2 CipherSpecs , kişisel sertifikanda RSA genel anahtarı olmasını gerektirir. Bu CipherSpecs kullanıldığında, bağlantıya ilişkin gizli anahtarı oluşturmak için Eliptik Eğri Diffie Hellman Ephemeral anahtar sözleşmesi kullanılır.

Tip 3 CipherSpecs , kişisel sertifikanda RSA genel anahtarı olması gerektiğini gerektirir. Bu CipherSpecs kullanıldığında, bağlantıya ilişkin gizli anahtarı oluşturmak için RSA anahtar değiş tokası kullanılır.

Bu sınırlamalar listesi ayrıntılı değildir: yapılandırmaya bağlı olarak, birlikte çalışma yeteneğini daha da etkileyebilecek ek kısıtlamalar olabilir. Örneğin, WebSphere MQ , FIPS 140-2 ya da NSA Suite B standartlarına uyacak şekilde yapılandırıldıysa, bu değer izin verilen yapılandırmaların aralığını da sınırlayacaktır. Ek bilgi için aşağıdaki bölüme bakın.

WebSphere MQ kuyruk yöneticisi, kendisini tanımlamak için yalnızca tek bir kişisel sertifika kullanabilir. Bu, kuyruk yöneticisinde bulunan tüm kanalların aynı sayısal sertifikayı kullanacağını ve bu nedenle her kuyruk yöneticisinin aynı anda yalnızca tek bir CipherSpec tipini kullanabileceğini belirtir. Benzer şekilde, bir WebSphere MQ istemcisi uygulaması kendisini tanımlamak için yalnızca tek bir kişisel sertifika kullanabilir. Başka bir deyişle, tek bir uygulama içindeki tüm SSL ve TLS bağlantıları aynı sayısal sertifikayı kullanacaktır ve bu nedenle her istemci uygulaması işlemi aynı anda yalnızca bir CipherSpec tipini kullanabilir.

The three types of CipherSpec do not interoperate directly: this is a limitation of the current SSL and TLS standards. For example, suppose you have chosen to use the ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec for a receiver channel named TO.QM1 on a queue manager named QM1. ECDHE_ECDSA_AES_128_CBC_SHA256 , bir Tip 1 CipherSpecolduğundan, QM1 eliptik bir Eğri anahtarı ve ECDSA tabanlı dijital imzayla kişisel bir sertifikan olmalıdır. Doğrudan QM1 ile iletişim kuran tüm istemcilerin ve diğer kuyruk yöneticilerinin, Tip 1 CipherSpec gereksinimlerini karşılayan dijital sertifikalara sahip olması gerekir. Other channels connecting to queue manager QM1 may use other CipherSpecs (for example ECDHE_ECDSA_3DES_EDE_CBC_SHA256), but they may only use Type 1 CipherSpecs to communicate with QM1.

WebSphere MQ ağlarınızı planlarken, SSL 'nin ya da TLS' nin gerekli olduğu kanalları dikkatli bir şekilde göz önünde bulundurun ve bunların çalıştırılması gereken tüm istemcilerin ve kuyruk yöneticilerinin aynı CipherSpecs tipini ve uygun dijital sertifikaları kullanmalarını sağlayın. The IETF standards RFC 4492, RFC 5246 and RFC 6460 describe the detailed usage of Elliptic Curve CipherSpecs in TLS 1.2.

Sayısal sertifika için dijital 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 görüntülemek için gereksinim duyardığınız sertifikanın etiketidir.

runmqakm komutunun yürütülmesi, Genel Anahtar Tipini görüntüleyen çıktı üretecektir:

```
Label : ibmwebspheremqexample
Key Size : 384
Version : X509 V3
Serial : 9ad5eeef5d756f41
Issuer : CN=Example Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : 21 August 2011 13:10:24 GMT+01:00
Not After : 21 August 2012 13:10:24 GMT+01:00
Public Key
    30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B
    81 04 00 22 03 62 00 04 3E 6F A9 06 B6 C3 A0 11
    F8 D6 22 78 FE EF 0A FE 34 52 C0 8E AB 5E 81 73
    D0 97 3B AB D6 80 08 E7 31 E9 18 3F 6B DE 06 A7
    15 D6 9D 5B 6F 56 3B 7F 72 BB 6F 1E C9 45 1C 46
    60 BE F2 DC 1B AD AC EC 64 4C 0E 06 65 6E ED 93
    B8 F5 95 E0 F9 2A 05 D6 21 02 BD FB 06 63 A1 CC
```

```
    66 C6 8A 0A 5C 3F F7 D3
Public Key Type : EC_ecPublicKey (1.2.840.10045.2.1)
Fingerprint : SHA1 :
    3C 34 58 04 5B 63 5F 5C C9 7A E7 67 08 2B 84 43
    3D 43 7A 79
Fingerprint : MD5 :
    49 13 13 E1 B2 AC 18 9A 31 41 DC 8C B4 D6 06 68
Fingerprint : SHA256 :
    6F 76 78 68 F3 70 F1 53 CE 39 31 D9 05 C5 C5 9F
    F2 B8 EE 21 49 16 1D 90 64 6D AC EB 0C A7 74 17
Signature Algorithm : EC_ecdsa_with_SHA384 (1.2.840.10045.4.3.3)
Value
    30 65 02 30 0A B0 2F 72 39 9E 24 5A 22 FE AC 95
    0D 0C 6D 6C 2F B3 E7 81 F6 C1 36 1B 9A B0 6F 07
    59 2A A1 4C 02 13 7E DD 06 D6 FE 4B E4 03 BC B1
    AC 49 54 1E 02 31 00 90 0E 46 2B 04 37 EE 2C 5F
    1B 9C 69 E5 99 60 84 84 10 71 1A DA 63 88 33 E2
    22 CC E6 1A 4E F4 61 CC 51 F9 EE A0 8E F4 DC B5
    0B B9 72 58 C3 C7 A4
Trust Status : Enabled
```

Bu durumda Genel Anahtar Tipi satırı sertifikana bir Eliptik Eğri ortak anahtarı olduğunu gösterir. Bu durumda imza algoritması satırı, EC_ecdsa_with_SHA384 algoritmasının kullanımda olduğunu gösterir: bu, ECDSA algoritmasına dayalı olur. Bu nedenle, bu sertifika yalnızca Tip 1 CipherSpecsile kullanıma uygundur.

Ayrıca, **iKeycmd (runmqckm)** aracını aynı parametrelerle de kullanabilirsiniz. Ayrıca, anahtar havuzunu açıp sertifikanın etiketini çift tıklatarak sayısal imza algoritmalarını görüntülemek için **iKeyman (strmqikm)** GUI 'si de kullanılabilir. Ancak, daha geniş bir algoritmayı desteklediği için sayısal sertifikaları görüntülemek için **runmqakm** aracını kullanmanız önerilir.

Eliptik Eğri CipherSpecs ve NSA Suite B

WebSphere MQ , Suite B uyumlu TLS 1.2 profiline uyacak şekilde yapılandırıldığında, izin verilen CipherSpecs ve dijital imza algoritmaları “NSA Suite B Cryptografi (IBM WebSphere MQ)” sayfa 30içinde açıklandığı şekilde sınırlandırılmıştır. Buna ek olarak, kabul edilebilir eliptik eğri tuşları aralığı, yapılandırılan güvenlik düzeylerine göre azaltılır.

128-bit Suite B güvenlik düzeyinde, sertifika konularının genel anahtarı NIST P-256 ya da NIST P-384 eliptik eğrisini kullanmak ve NIST P-256 eliptik eğrisi ya da NIST P-384 eliptik eğrisi ile imzalanmalıdır. **runmqakm** komutu, EC_ecdsa_with_SHA256ya da EC_ecdsa_with_SHA384içeren bir -sig_alg değiştirgesi kullanılarak, bu güvenlik düzeyi için sayısal sertifika istemek üzere kullanılabilir.

192-bit Suite B güvenlik düzeyinde, sertifika konularının genel anahtarı NIST P-384 eliptik eğrisini kullanmak ve NIST P-384 eliptik eğrisi ile imzalanmalıdır. **runmqakm** komutu, EC_ecdsa_with_SHA384' un -sig_alg değiştirgesini kullanarak, bu güvenlik düzeyi için sayısal sertifika istemek üzere kullanılabilir.

Desteklenen NIST eliptik eğrileri aşağıdaki gibidir:

Çizelge 3. Desteklenen NIST eliptik eğrileri

NIST FIPS 186-3 eğri adı	**RFC 4492 eğri adı**	**Eliptik Eğri anahtarı büyüklüğü (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 ' nin Belirtilmesi” sayfa 211
DEFINE CHANNEL MQSC komutunda ya da **ALTER CHANNEL** MQSC komutunda **SSLCIPH** değiştirgesini kullanarak CipherSpec belirtin.

“MQI istemcisinde çalıştırma sırasında yalnızca FIPS onaylı CipherSpecs ' in kullanıldığını belirtme” sayfa 105
Anahtar havuzlarınızı FIPS uyumlu yazılım kullanarak yaratın ve kanalın FIPS onaylı CipherSpecs' ı kullanması gerektiğini belirtin.

“NSA Suite B Cryptografi (IBM WebSphere MQ)” sayfa 30
Bu konuda, Windows, Linuxve UNIX sistemlerinde Suite B uyumlu TLS 1.2 profiline uygun olarak IBM WebSphere MQ ' un nasıl yapılandırılacağı hakkında bilgiler yer alır.

“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.

IBM WebSphere MQiçinde desteklenenCipherSpec değerleri
Varsayılan CipherSpecs kümesi, yalnızca şu değerlere izin verir:

TLS 1.0

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

TLS 1.2

- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Kullanımdan kaldırılan CipherSpecs' in etkinleştirilmesi

Varsayılan olarak, kanal tanımlarında kullanımdan kaldırılmış bir CipherSpec belirtmenize izin verilmez. Kullanımdan kaldırılmış bir CipherSpecbelirtmeye çalışırsanız, kuyruk yöneticisine ilişkin hata günlüğünde AMQ9788 iletisini alırsınız.

`qm.ini` dosyasını düzenleyerek, kullanımdan kaldırılan CipherSpecs ' ı yeniden etkinleştirmeniz mümkündür. `qm.ini` dosyasının SSL kısmı içinde, aşağıdaki satırı ekleyin:

```
SSL:
AllowWeakCipherSpec=Yes
```

You can also re-enable one or more of the deprecated CipherSpecs at runtime on the server by setting the environment variable *AMQ_SSL_WEAK_CIPHERENABLE* to any value. Bu ortam değişkeni, `qm.ini` dosyasında belirtilen değerden bağımsız olarak CipherSpecs ' in geçerli olmasına olanak sağlar.

Kanal doğrulama kayıtları

Bir kanal düzeyinde sistemler arasında bağlantı kurmak için verilen erişim üzerinde daha kesin bir denetim yapmak için kanal kimlik doğrulama kayıtlarını kullanabilirsiniz.

İstemcilerin, boş bir kullanıcı kimliği ya da istemcinin istenmeyen işlemler gerçekleştirmesine olanak sağlayacak üst düzey bir kullanıcı kimliği kullanarak, kuyruk yöneticinize bağlanma girişiminde bulunmayı deneyebilirsiniz. Kanal doğrulama kayıtlarını kullanarak bu istemcilere erişimi engelleyebilirsiniz. Diğer bir seçenek olarak, bir istemci, istemci altyapısında geçerli olan, ancak bilinmeyen ya da sunucu altyapısında geçersiz bir biçimde olan bir kullanıcı kimliğini doğrulayabilir. Belirtilen kullanıcı kimliğini geçerli bir kullanıcı kimliğiyle eşlemek için kanal kimlik denetimi kaydını kullanabilirsiniz.

Kuyruk yöneticinize bağlanan ve bir şekilde kötü davranan bir istemci uygulaması bulabilirsiniz. Sunucuyu bu uygulamanın neden olduğu sorunlardan korumak için, güvenlik duvarı kuralları güncellendikçe ya da istemci uygulaması düzeltilinceye kadar istemci uygulamasının açık olduğu IP adresi kullanılarak geçici olarak engellenmiş olması gerekir. İstemci uygulamasının bağlandığı IP adresini engellemek için bir kanal kimlik doğrulaması kaydı kullanabilirsiniz.

IBM WebSphere MQ Explorergibi bir yönetim aracı ve bu belirli kullanım için bir kanal ayarladıysanız, yalnızca belirli istemci bilgisayarlarının bunu kullanabilmelerini sağlamak isteyebilirsiniz. Kanalın yalnızca belirli IP adreslerinden kullanılmasına izin vermek için bir kanal kimlik doğrulaması 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 için kanal kimlik doğrulaması kayıtlarını almak için **ALTER QMGR CHLAUTH(ENABLED)** MQSC komutunu kullanın.

CHLAUTH kuralları, yeni gelen bağlantıya yanıt olarak oluşturulan bir kanal MCA için uygulanır. Kanal MCA ' nın kanala yanıt olarak yerel olarak başlatıldığı bir kanal için, hiçbir **CHLAUTH** kuralı uygulanmaz.

Çizelge 4. Farklı kanal çiftleri için CHLAUTH kurallarının uygulandığı yer

Kanal tipi	**CHLAUTH kurallarının uygulandığı MCA**
SDR-RCVR	RVR
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 SSDR. Geri bildirme bağlantısı için RQSTR.

Kanal doğrulama kayıtları aşağıdaki işlevleri gerçekleştirmek için yaratılabilir:

- Belirli IP adreslerinden gelen bağlantıları engellemek için.
- Belirli kullanıcı kimliklerinden gelen bağlantıları engellemek için.
- Belirli bir IP adresinden bağlantı kuran herhangi bir kanal için bir MCAUSER değeri belirlemek üzere.
- Herhangi bir kanalda belirli bir kullanıcı kimliği için kullanılacak bir MCAUSER değeri belirlemek için.
- Belirli bir SSL ya da TLS Ayırt Edici Adı (DN) içeren herhangi bir kanalda bir MCAUSER değeri belirlemek için kullanılır.
- Belirli bir kuyruk yöneticisinden bağlantı kuran herhangi bir kanal için bir MCAUSER değeri ayarlamak için.
- Belirli bir kuyruk yöneticisinden gelen bağlantıları engellemek için, bağlantı belirli bir IP adresinden gönderilmedikçe.
- Belirli bir SSL ya da TLS sertifikasını sunan bağlantıları engellemek için, bağlantı belirli bir IP adresinden verilinceye kadar.

Bu kullanımlar aşağıdaki bölümlerde daha ayrıntılı olarak açıklanmıştır.

You create, modify, or remove channel authentication records using the MQSC command **SET CHLAUTH** or the PCF command **Set Channel Authentication Record**.

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

Engelleyici IP adresleri

Olağan durumda, belirli IP adreslerinden erişimi önlemek için güvenlik duvarının roldür. Ancak, bağlantı girişimlerini WebSphere MQ sisteminize erişmemesi gereken IP adresinden deneyimlemeniz ve güvenlik duvarının güncellenebilmesi için önce adresi geçici olarak engellemelisiniz. These connection attempts might not even be coming from WebSphere MQ channels, but from other socket applications that are misconfigured to target your WebSphere MQ listener. BLOCKADR tipinde bir kanal kimlik doğrulaması kaydı ayarlayarak IP adreslerini engelle. Joker karakterler de dahil olmak üzere, bir ya da daha çok tek adres, adres aralığı ya da kalıp belirtebilirsiniz.

Bir gelen bağlantı, IP adresi bu şekilde engellendiği için reddedildiğinde, kanal olaylarının etkinleştirilmesi ve kuyruk yöneticisinin çalışması koşuluyla, MQRC_CHANNEL_BLOCKED neden niteleyicisi MQRQ_CHANNEL_BLOCKED_ADDRESS iletisi yayınlandığında bir MQRC_CHANNEL_BLOCKED olay iletisi yayınlanır. Ayrıca, bağlantı engellenen yinelenen girişimlerle dolu olmadığından emin olmak için hata döndürmeden önce 30 saniye açık bir şekilde bağlantı tutulur.

IP adreslerini yalnızca belirli kanallarda engellemek ya da hata bildirilmeden önce gecikmeyi önlemek için, ADDRESSMAP tipinde bir kanal kimlik doğrulaması kaydı olan USERSRC (NOERCESS) parametresiyle bir kanal kimlik doğrulaması kaydı ayarlayın.

Bu neden için bir gelen bağlantı reddedildiğinde, kanal olaylarının etkinleştirilmiş olması ve kuyruk yöneticisinin çalışması koşuluyla MQRC_CHANNEL_BLOCKED neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS ile engellenmiş bir olay iletisi yayınlanır.

Örneğin, “Belirli IP adreslerinin engellenmesi” sayfa 176 başlıklı konuya bakın.

Kullanıcı Kimlikleri Engellenmesi

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

Bu neden için bir gelen bağlantı reddedildiğinde, kanal olaylarının etkinleştirilmesi koşuluyla MQRC_CHANNEL_BLOWKED neden niteleyicisi MQRQ_CHANNEL_BLOCKED_USERID ile engellenmiş bir olay iletisi yayınlanır.

Örneğin, “Belirli kullanıcı kimliklerini engelle” sayfa 178 başlıklı konuya bakın.

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

Bu neden için bir gelen bağlantı reddedildiğinde, kanal olaylarının etkinleştirilmiş olması ve kuyruk yöneticisinin çalışması koşuluyla MQRC_CHANNEL_BLOCKED neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS ile engellenmiş bir olay iletisi yayınlanır.

Örneğin, “İstemci için erişim engelleyici erişim belirtildi kullanıcı kimliği” sayfa 181 başlıklı konuya bakın.

Engelleyici kuyruk yöneticisi adları

Belirtilen bir kuyruk yöneticisinden bağlanan herhangi bir kanalda erişim olmadığını belirtmek için, USERSRC (NOACCESS) parametresiyle QMGRMAP tipinde bir kanal kimlik doğrulaması kaydı ayarlayın. Joker karakterler de dahil olmak üzere tek bir kuyruk yöneticisi adı ya da bir kalıp belirtebilirsiniz. Kuyruk yöneticilerinden erişimi engellemek için BLOCKUSER işlevinin eşdeğer bir işlevi yoktur.

Bu neden için bir gelen bağlantı reddedildiğinde, kanal olaylarının etkinleştirilmiş olması ve kuyruk yöneticisinin çalışması koşuluyla MQRC_CHANNEL_BLOCKED neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS ile engellenmiş bir olay iletisi yayınlanır.

Örneğin, “Uzak kuyruk yöneticisinden erişimin engellenmesi” sayfa 180 başlıklı konuya bakın.

SSL ya da TLS DN ' lerinin engellenmesi

Belirli bir ayırt edici ad içeren bir SSL ya da TLS kişisel sertifikasını sunan herhangi bir kullanıcının erişimi olmadığını belirtmek için, USERSRC (NOERCESS) parametresiyle 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. DN ' lere erişimi engellemek için BLOCKUSER işlevinin eşdeğer bir işlevi yoktur.

Bu neden için bir gelen bağlantı reddedildiğinde, kanal olaylarının etkinleştirilmiş olması ve kuyruk yöneticisinin çalışması koşuluyla MQRC_CHANNEL_BLOCKED neden niteleyicisi MQRQ_CHANNEL_BLOCKED_NOACCESS ile engellenmiş bir olay iletisi yayınlanır.

Örneğin, “SSL Ayırt Edici Adı için erişimin engellenmesi” sayfa 181 başlıklı konuya bakın.

IP adreslerinin kullanılacak kullanıcı kimlikleriyle eşlenmesi

Belirli bir IP adresinden bağlanan herhangi bir kanalın belirli bir MCAUSER kullanmasını belirtmek için, ADDRESSMAP tipinde bir kanal kimlik doğrulaması kaydı ayarlayın. Joker karakterler de dahil olmak üzere tek bir adres, bir adres aralığı ya da bir kalıp belirtebilirsiniz.

Bir bağlantı noktası ileticisi, DMZ oturumu sonu ya da kuyruk yöneticisine sunulan IP adresini değiştiren başka bir ayar kullanırsanız, IP adreslerini eşlemeye gerek kalmaması için uygun olmayabilir.

Örneğin, “Bir IP adresinin MCAUSER kullanıcı kimliği ile eşlenmesi” sayfa 182 başlıklı konuya bakın.

Kuyruk yöneticisi adlarının kullanılacak kullanıcı kimlikleriyle eşlenmesi

Belirli bir kuyruk yöneticisinden bağlanan herhangi bir kanalın belirli bir MCAUSER kullanmak üzere olduğunu belirtmek için, QMGRMAP tipinde bir kanal kimlik doğrulaması kaydı ayarlayın. Joker karakterler de dahil olmak üzere tek bir kuyruk yöneticisi adı ya da bir kalıp belirtebilirsiniz.

Örneğin, “Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi” sayfa 179 başlıklı konuya bakın.

Bir istemci tarafından kullanıcı kimliklerinin kullanılması için kullanıcı kimliklerinin eşlenmesi

Bir WebSphere MQ MQI istemcisinden bir bağlantı tarafından belirli bir kullanıcı kimliği kullanılıp kullanılmadığını belirtmek için, farklı bir MCAUSER değeri kullanılır, USERMAP tipinde bir kanal kimlik doğrulaması kaydı ayarlayın. Kullanıcı kimliği eşlemesi joker karakterler kullanmaz.

Bir örnek için bkz. “İstemcinin değerlendirilen bir kullanıcı kimliğini MCAUSER kullanıcı kimliğiyle eşlenmesi” sayfa 179 .

SSL ya da TLS DN ' lerinin kullanılacak kullanıcı kimliklerine eşlenmesi

Belirli bir DN içeren bir SSL/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.

Örneğin, “SSL ya da TLS Ayırt Edici Adının MCAUSER kullanıcı kimliğine eşlenmesi” sayfa 180 başlıklı konuya bakın.

Eşleme kuyruğu yöneticileri, istemciler ya da SSL ya da TLS DN ' leri IP adresine göre

Bazı durumlarda, bir üçüncü kişinin kuyruk yöneticisi adını bozması mümkün olabilir. Bir SSL ya da TLS sertifikası ya da anahtar veritabanı dosyası da çalınabilir ve yeniden kullanılabilir. Bu tehditlere karşı korunmak için, belirli bir kuyruk yöneticisinden ya da istemcisinden ya da belirli bir DN ' nin kullanılarak belirlenen bir IP adresinden bağlantı kurulması gerektiğini belirtebilirsiniz. USERMAP, QMGRMAP ya da SSLPEERMAP tipinde bir kanal kimlik doğrulaması kaydı belirleyin ve ADDRESS parametresini kullanarak, izin verilen IP adresini ya da IP adreslerini örüntülerini belirtin.

Bir örnek için bkz. “Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi” sayfa 179 .

Kanal doğrulama kayıtları arasındaki etkileşim

Bağlantı yapmaya çalışan bir kanal, birden çok kanal kimlik doğrulama kaydı ile eşleşir ve bu, bunların birbiriyle çelişen etkilerinin olduğunu da sağlar. Örneğin, bir kanal, bir BLOCKUSER kanal kimlik doğrulama kaydı tarafından engellenen, ancak farklı bir kullanıcı kimliği belirleyen bir SSLPEERMAP kaydı ile eşleşen bir SSL ya da TLS sertifikasıyla bir kullanıcı kimliğini doğrulayabilir. Ayrıca, kanal kimlik doğrulaması kayıtları genel arama karakterleri kullanırsa, tek bir IP adresi, kuyruk yöneticisi adı ya da SSL ya da TLS DN birkaç örüntüle eşleşebilir. For example, the IP address 192.0.2.6 matches the patterns 192.0.2.0-24, 192.0.2.*, ve 192.0. * .6. Alınan eylem, aşağıdaki gibi belirlenir.

- Kullanılan kanal kimlik doğrulama kaydı aşağıdaki gibi seçilir:
  - Kanal adıyla eşleşen bir kanal kimlik doğrulaması kaydı, bir genel arama karakteri kullanarak kanal adıyla eşleşen bir kanal kimlik doğrulaması kaydı üzerinden önceliğe sahip olur.
  - Bir SSL ya da TLS DN kullanan bir kanal kimlik doğrulaması kaydı, kullanıcı kimliği, kuyruk yöneticisi adı ya da IP adresi kullanarak bir kayıt üzerinde önceliğe sahip olur.
  - Bir kullanıcı kimliği ya da kuyruk yöneticisi adını kullanan bir kanal kimlik doğrulaması kaydı, bir IP adresini kullanarak bir kayıttan önce önceliklerden yararlanir.
- Eşleşen bir kanal kimlik doğrulaması kaydı bulunursa ve bu kayıt bir MCAUSER belirtiyorsa, bu MCAUSER kanala atanır.
- Eşleşen bir kanal kimlik doğrulaması kaydı bulunursa ve kanalda erişim olmadığını belirtiyorsa, kanala *NOACCESS değerinin bir MCAUSER değeri atanır. Bu değer daha sonra bir güvenlik çıkış programı tarafından değiştirilebilir.
- Eşleşen kanal kimlik doğrulaması kaydı bulunamazsa ya da eşleşen bir kanal kimlik doğrulaması kaydı bulunursa ve kanalın kullanıcı kimliğinin kullanılacağını belirtirse, MCAUSER alanı incelenir.
  - MCAUSER alanı boşsa, istemci kullanıcı kimliği kanala atanmaktadır.
  - MCAUSER alanı boş değilse, kanala atanılır.
- Herhangi bir güvenlik çıkış programı çalıştırılır. Bu çıkış programı, kanal kullanıcı kimliğini belirleyebilir ya da erişimin engellenmiş olacağını belirleyebilir.
- Bağlantı engellenirse ya da MCAUSER için *NOACCESS değeri belirlendiyse, kanal sona erer.
- Bağlantı engellenmezse, bir istemci kanalı dışında herhangi bir kanal için, önceki adımlarda belirlenen kanal kullanıcı kimliği, engellenen kullanıcılar listesine göre işaretlenir.
  - Kullanıcı kimliği engellenen kullanıcılar listesinde yer alıyorsa, kanal sona erer.
  - Kullanıcı kimliği engellenen kullanıcılar listesinde yoksa, kanal çalışır.

Kanal kimlik doğrulama kayıtlarının bir kanal adı, IP adresi, kuyruk yöneticisi adı ya da SSL ya da TLS DN ile eşleştiği yerde, en belirli eşleşme kullanılır. En spesik olarak kabul edilen eşleşme aşağıdaki gibi belirlenir.

- Kanal adı için:
  - En özel eşleşme, genel arama karakteri içermeyen bir addır; örneğin, A.B.C.
  - En soysal eşleşme, tüm kanal adlarıyla eşleşen tek bir yıldız işaretidir (*).
  - Sol üst konumda yıldız imi bulunan bir örüntü, en soldaki konumda tanımlı bir değere sahip bir örüntüden daha genel bir kalıba sahip. Bu nedenle *.B.C A. * ' den daha genel bir değer.
  - İkinci konumdaki yıldız işareti olan bir örüntü, ikinci konumdaki tanımlı bir değere sahip bir örüntüden daha soysal ve sonraki her konum için benzer şekilde. Bu nedenle A. * .C, A.B.*
  - İki ya da daha fazla örüntüde aynı konumda bir yıldız imi varsa, yıldız imi izleyen daha az sayıda düğüm varsa, daha genel bir yıldız olur. Böylece A. * A. * .C ' den daha genel.
- Bir IP adresi için:
  - En özel eşleşme, genel arama karakteri içermeyen bir addır; örneğin, 192.0.2.6.
  - En soysal eşleşme, tüm kanal adlarıyla eşleşen tek bir yıldız işaretidir (*).
  - Sol üst konumda yıldız imi bulunan bir örüntü, en soldaki konumda tanımlı bir değere sahip bir örüntüden daha genel bir kalıba sahip. Bu nedenle *.0.2.6 , 192 'den daha soysal olabilir. *.

- İkinci konumdaki yıldız işareti olan bir örüntü, ikinci konumdaki tanımlı bir değere sahip bir örüntüden daha soysal ve sonraki her konum için benzer şekilde. Böylece 192. *.2.6 , 192.0' dan daha soysal. *.
- İki ya da daha fazla örüntüde aynı konumda bir yıldız imi varsa, yıldız imi izleyen daha az sayıda düğüm varsa, daha genel bir yıldız olur. Böylece 192. * 192. * .2. * * ' den daha genel.
- Kısa çizgi (-) ile gösterilen bir aralık, bir yıldız işaretinden daha özeldir. Bu nedenle 192.0.2.0-24 , 192.0.2' den daha özgüdür. *.
- Bir diğerinin alt kümesi olan bir aralık, daha büyük aralığa göre daha özeldir. Bu nedenle 192.0.2.5-15 , 192.0.2.0-24' ten daha özgüdür.
- Çakışan aralıklara izin verilmez. Örneğin, hem 192.0.2.0-15 hem de 192.0.2.10-20için kanal kimlik doğrulama kayıtları bulunamaz.
- Örüntü, sondaki tek bir yıldız imiyle sona ermedikçe, örüntüde gereken kısımdan az sayıda parça olamaz. Örneğin, 192.0.2 geçersiz, ancak 192.0.2.* geçerlidir.
- A trailing asterisk must be separated from the rest of the address by the appropriate part separator (a dot (.) for IPv4, a colon (:) for IPv6). Örneğin, yıldız işareti kendi parçasında olmadığı için, 192.0* geçerli değildir.
- Bir örüntü, sondaki yıldız işaretinin bitişiğindeki yıldız imi olmayan ek asteriks içerebilir. Örneğin, 192. * .2. * geçerlidir, ancak 192.0' dır. * .* (çizelge adı) geçersiz.
- Sonuçtaki adresin belirsiz olacağı için, bir IPv6 adres kalıbı çift iki nokta üst üste ve sonda yıldız işareti içeremez. Örneğin, 2001:: * 2 0 0 'a kadar genişleyebiliyordu: 0 0 0 0: *, 2001:0000:0000: * ve benzeri

- Kuyruk yöneticisi adı için:
  - En özel eşleşme, genel arama karakteri içermeyen bir addır; örneğin, 192.0.2.6.
  - En soysal eşleşme, tüm kanal adlarıyla eşleşen tek bir yıldız işaretidir (*).
  - Sol üst konumda yıldız imi bulunan bir örüntü, en soldaki konumda tanımlı bir değere sahip bir örüntüden daha genel bir kalıba sahip. Bu nedenle *QUEUEMANAGER, QUEUEMANAGER* ' dan daha soysal.
  - İkinci konumdaki yıldız işareti olan bir örüntü, ikinci konumdaki tanımlı bir değere sahip bir örüntüden daha soysal ve sonraki her konum için benzer şekilde. Bu nedenle Q* MANAGER, QUEUE* ' dan daha soysal.
  - İki ya da daha fazla örüntüde aynı konumda bir yıldız imi varsa, yıldız imi izleyen daha az karakter içeren bir yıldız daha soysal olur. Bu nedenle Q*, Q* MGR ' den daha soysal olur.
- SSL ya da TLS Ayırt Edici Adı (DN) için, alt dizilimlerin öncelik sırası şöyledir:

Çizelge 5. Alt dizelerin öncelik sırası

Sıralama	**DN alt dizgisi**	**Ad**
1	SERIALNUMBER=	Sertifika seri numarası
2	MAIL=	E-posta adresi
3	E=	E-posta adresi (POSTA tercihinde kullanımdan kaldırıldı)
4	UID=, USERID=	Kullanıcı kimliği
5	CN=	Ortak ad
6	T =	Başlık
7	OU=	Kuruluş Birimi
8	DC=	Etki alanı bileşeni
9	O=	Kuruluş
10	SOKAK =	Adres satırı/adres satırı

Çizelge 5. Alt dizelerin öncelik sırası (devamı var)		
Sıralama	**DN alt dizgisi**	**Ad**
11	L=	İlçe
12	ST =, SP=, S=	Eyalet ya da bölge adı
13	PC=	Posta kodu/posta kodu
14	C=	Ülke
15	UNSTRUCTUREDNAME=	Anasistem adı
16	UNSTRUCTUREADDRESS=	IP adresi
17	DNQ=	Ayırt edici ad niteleyicisi

Bu nedenle, bir SSL ya da TLS sertifikası, alt dizeleri içeren bir DN (DN) O=IBM ve C=UK ile sunulursa, WebSphere MQ , her ikisi de mevcutsa, C=UK için bir e-posta adresi olarak O=IBM için bir kanal kimlik doğrulama kaydı kullanır.

Bir DN, önce belirlenen büyük kuruluş birimleriyle sıradüzensel sırada belirtilmesi gereken birden çok kuruluş birimi içerebilir. İki DN, OU değerleri dışında tüm bakımdan eşitse, daha belirgin ayırt edici ad aşağıdaki gibi belirlenir:

1. Farklı OU öznitelikleri varsa, en çok OU değerlerine sahip DN daha özeldir. Bunun nedeni, daha fazla Kuruluş Birimi içeren DN 'nin DN' yi daha ayrıntılı olarak niteleyeceğinden ve daha fazla eşleşme ölçütü sağladığından kaynaklanır. En üst düzey OU genel arama karakteri (OU = *) olsa bile, daha fazla OU içeren DN, genel olarak daha belirgin olarak kabul edilir.
2. Aynı sayıda OU özniteliği varsa, ilgili çift OU değerleri soldan sağa sırayla karşılaştırılır; burada sol en yüksek OU, aşağıdaki kurallara göre en yüksek düzeydir (en yüksek düzeydir).
   a. Genel arama karakteri olmayan bir Kuruluş Birimi (OU), yalnızca tek bir dizgiyle eşleşebileceği için en özeldir.
   b. Başında ya da sonunda (örneğin, OU=ABC* ya da OU= *ABC) tek bir genel arama karakteri olan bir OU 'ya en çok belirli bir OU' ya özgü bir değer girin.
   c. Örneğin, OU= *ABC* gibi iki genel arama karakteri içeren bir OU ' ya daha çok özel bir örnek verilebilir.
   d. Yalnızca yıldız işaretinden (OU = *) oluşan bir OU (OU) en az özeldir.
3. Dizgi karşılaştırması, aynı ayrıntıya sahip iki öznitelik değeri arasında bağlıysa, bundan sonra hangi öznitelik dizgisi daha ayrıntılı olur.
4. Dizgi karşılaştırması, aynı belirtimin ve uzunluğun iki öznitelik değeri arasında bağlıysa, sonuç, DN ' nin genel arama karakterleri hariç olmak üzere, büyük ve küçük harfe duyarsız bir dizgi karşılaştırması tarafından belirlenir.

DC değerleri dışında, iki DN, tüm bakımdan eşitse, DC değerleri dışında en düşük düzeyde DC değeri en düşük düzeydir (en spesik) ve karşılaştırma sıralaması buna göre farklılık gösterirse, aynı eşleştirme kuralları OU ' lar için geçerlidir.

Kanal kimlik doğrulama kayıtlarının görüntülenmesi

To display channel authentication records, use the MQSC command **DISPLAY CHLAUTH** or the PCF command **Inquire Channel Authentication Records**. Sağlanan kanal adıyla eşleşen tüm kayıtları döndürmeyi seçebilir ya da belirtik bir eşleşme seçebilirsiniz. Açık eşleşme, bir kanal belirli bir IP adresinden, belirli bir kuyruk yöneticisinden ya da belirli bir kullanıcı kimliğini kullanarak bağlantı yapma girişiminde bulunduysa ve isteğe bağlı olarak, belirli bir DN ' yi içeren bir SSL/TLS kişisel sertifikasını sunan bir kanal hangi kanal kimlik doğrulama kaydını kullanacağını belirtir.

İlgili kavramlar

“Uzaktan ileti sistemine ilişkin güvenlik” sayfa 54

Bu bölümde, güvenlik ile uzaktan ileti sistemi konuları ele verilmektedir.

IBM WebSphere MQiçinde ileti güvenliği

Message security in IBM WebSphere MQ infrastructure is provided by a separately licensed component IBM WebSphere MQ Advanced Message Security.

IBM WebSphere MQ Advanced Message Security (AMS) expands IBM WebSphere MQ security services to provide data signing and encryption at the message level. 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

"IBM WebSphere MQ Advanced Message Security" sayfa 262
IBM WebSphere MQ Advanced Message Security (AMS) is a separately licensed component of IBM WebSphere MQ Advanced Message Security that provides a high level of protection for sensitive data flowing through the IBM WebSphere MQ Advanced Message Security network, while not impacting the end applications.

Güvenlik gereksinimlerinizin planlanması

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

You can use IBM WebSphere 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.

WebSphere MQ , SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) ve TLS (Transport Layer Security; İletim Katmanı Güvenliği) desteği de içinde olmak üzere, bağlantı düzeyinde bir güvenlik hizmetleri aralığı sağlar.

WebSphereuygulamasını uygularken güvenliğin belirli yönlerini dikkate almanız gerekir. UNIX, Linux ve Windows sistemlerinde, bu yönleri yoksayabilir ve hiçbir şey yapmazsanız, WebSphere MQ' yı kullanamazsınız.

Güvenlikle ilgili önemli noktalar aşağıda açıklanmıştır.

WebSphere MQ' u yönetme yetkisi

WebSphere MQ yöneticilerinin aşağıdakileri yapmak için yetkisi gerekir:

- WebSphere MQ' u denetlemek için komut verme komutları
- IBM WebSphere MQ Gezgini 'ni kullanma

Daha fazla bilgi için bkz.

- "UNIX, Linux, and Windows sistemlerinde IBM WebSphere MQ yönetimi yetkisi" sayfa 191

WebSphere MQ nesneleriyle çalışma yetkisi

Uygulamalar, aşağıdaki WebSphere MQ nesnelerine MQI çağrıları yayınlayarak erişebilirler:

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

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

Daha fazla bilgi için “Authorization for applications to use IBM WebSphere MQ” sayfa 49 başlıklı konuya bakın.

Kanal güvenliği

İleti kanalı aracıları (MCA ' lar) ile ilişkili kullanıcı kimlikleri, çeşitli WebSphere 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 67 başlıklı konuya bakın.

Ek konular

Yalnızca belirli WebSphere MQ işlevini ya da temel ürün uzantılarını kullanıyorsanız, aşağıdaki güvenlik yönlerini göz önünde bulundurmanız gerekir:

- “Kuyruk yöneticisi kümeleri için güvenlik” sayfa 76
- “IBM WebSphere MQ Yayınlama/Abone Olma Güvenliği” sayfa 77
- “IBM WebSphere MQ Internet düzgeçiş güvenliği için güvenlik” sayfa 78

Planlama tanıtıcısı ve kimlik doğrulaması

Kullanılacak kullanıcı kimliklerinin ve kimlik doğrulama denetimlerini uygulamak istediğiniz düzeylere nasıl ve ne kadar düzeyde istediğinizi belirleyin.

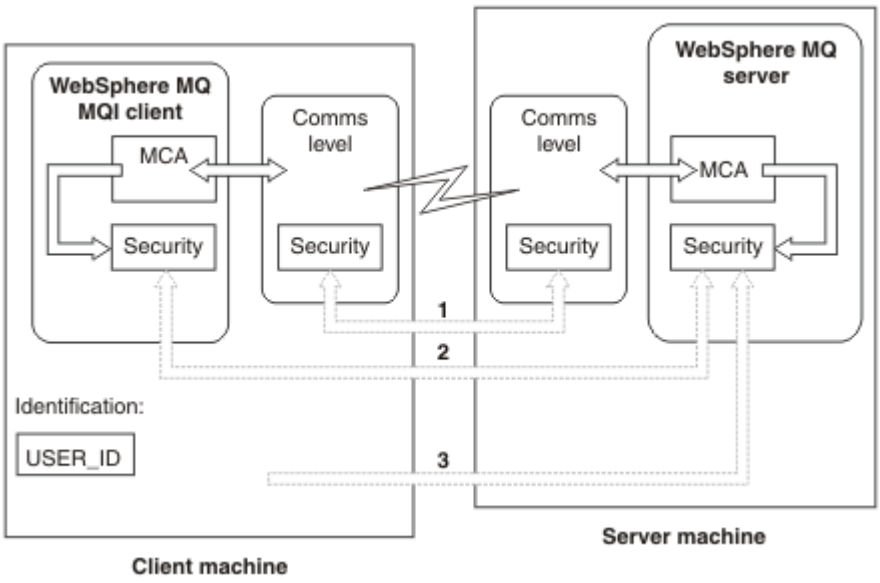
Farklı işletim sistemlerinin kullanıcı kimliklerini farklı uzunluklarda desteklediğine göz önünde olmak üzere, IBM WebSphere MQ uygulamalarınızın kullanıcılarını nasıl tanımlayacağınıza karar vermelisiniz. Kanal doğrulama kayıtlarını, bir kullanıcı kimliğiyle başka bir kullanıcı kimliğiyle eşlemek ya da bağlantının bazı özniteliklerine dayalı olarak bir kullanıcı kimliği belirtmek için kullanabilirsiniz. SSL ya da TLS kullananIBM WebSphere MQ kanalları, tanımlama ve kimlik doğrulaması için bir mekanizma olarak sayısal 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 WebSphere MQuygulamasında kimlik doğrulaması yapmak için hangi dijital sertifikaların kullanılabileceğini belirler. Daha fazla bilgi için bakınız:

- “Uzak kuyruk yöneticisinin MCAUSER kullanıcı kimliğine eşlenmesi” sayfa 179
- “İstemcinin değerlendirilen bir kullanıcı kimliğini MCAUSER kullanıcı kimliğiyle eşlenmesi” sayfa 179
- “SSL ya da TLS Ayırt Edici Adının MCAUSER kullanıcı kimliğine eşlenmesi” sayfa 180
- “Bir IP adresinin MCAUSER kullanıcı kimliği ile eşlenmesi” sayfa 182

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. Bu çizgede, bir sunucuya bağlı olan bir IBM WebSphere MQ MQI istemcisi gösterilir. Güvenlik, aşağıdaki metinde açıklandığı gibi dört düzeyde uygulanır. MCA, Message Channel Agent 'dir.



Şekil 7. İstemci/sunucu bağlantısında güvenlik

1. İletişim düzeyi

   Bkz. ok 1. Güvenlik düzeyini iletişim düzeyinde uygulamak için SSL ya da TLS kullanın. Daha fazla bilgi için, bkz. “Şifreleme güvenlik iletişim kuralları: SSL ve TLS” sayfa 14

2. Kanal doğrulama kayıtları

   Bkz. ok 2 ve 3. Kimlik doğrulama, IP adresi ya da güvenlik düzeyinde SSL/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 38' ta tam açıklama verilir.

3. 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.

4. Kanal güvenlik çıkışa geçilen tanıtıcı

   Bkz. ok 3. İstemcide, iletişim sunucusu iletişimi için kanal güvenliği çıkışlarının bir çift olarak çalışması gerekmez. IBM WebSphere 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.

   HP Integrity NonStop Serveriçin IBM WebSphere MQ istemcisinde kimlik belirlemeye yardımcı olmak için, istemci, istemci uygulamasının çalıştırıldığı OSS Safeguard diğer adını geçirir. This ID is typically of the form <PRIMARYGROUP>.<ALIAS>. Gerekirse, bu kullanıcı kimliğini, kanal kimlik doğrulama kayıtlarını ya da bir güvenlik çıkışını kullanarak kuyruk yöneticisinde alternatif bir kullanıcı kimliğiyle eşleyebilirsiniz. İleti çıkışlarına ilişkin daha fazla bilgi için bkz. “İleti çıkışlarında kimlik eşlemesi” sayfa 144. Kanal kimlik doğrulama kayıtlarının tanımlanmasıyla ilgili daha fazla bilgi için bkz. “İstemcinin değerlendirilen bir kullanıcı kimliğini MCAUSER kullanıcı kimliğiyle eşlenmesi” sayfa 179.

   The values of the user ID and, if available, the security ID, can be used by the server security exit to establish the identity of the IBM WebSphere MQ MQI client.

Kullanıcı Kimlikleri

IBM WebSphere MQ MQI istemcisi Windows 'ta ise ve IBM WebSphere MQ sunucusu da Windows ' daysa ve istemci kullanıcı kimliğinin tanımlı olduğu etki alanına erişiyorsa, IBM WebSphere MQ en çok 20 karakter olan kullanıcı kimliklerini destekler. UNIX and Linux platformlarında ve yapılandırmalarında uzunluk üst sınırı 12 karakterdir.

A WebSphere MQ for Pencereler server does not support the connection of a Pencereler 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_YETKILI) konumunda.

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`.

`UNKNOWN` 'in ayrılmış bir kullanıcı kimliği olduğunu ve `NOBODY` kullanıcı kimliğinin de WebSphere MQ' ya özel anlamları olduğunu unutmayın. `UNKNOWN` ya da `NOBODY` adlı işletim sisteminde kullanıcı kimlikleri yaratılması istenmeyen sonuçlara yol açabilirdi.

Kullanıcı kimlikleri kimlik doğrulaması için kullanılsa da, gruplar, Windows dışında yetkilendirme için kullanılır.

Hizmet hesapları oluşturursanız, gruplara dikkat etmeden ve tüm kullanıcı kimlikleri için farklı bir şekilde yetki verdiyseniz, her kullanıcı diğer her kullanıcının bilgilerine erişebilir.

Planlama yetkilendirmesi

Yönetici yetkisine sahip olacak kullanıcıları planlayın ve bir IBM WebSphere MQ MQI istemcisinden bağlananlar da içinde olmak üzere, uygulamaların kullanıcılarına uygun bir şekilde IBM WebSphere MQ nesnelerini kullanma yetkisi vereceklerini planlayın.

IBM WebSphere MQ' u kullanabilmek için kişilere ya da uygulamalara erişim izni verilmelidir. Gerekli olan erişim, üstlendikleri rollere ve gerçekleştirmeye gereksinim duydukları görevlere bağlıdır. IBM WebSphere MQ içindeki yetki, iki ana kategoriye ayrılabilir:

- Yönetim işlemlerini gerçekleştirme yetkisi
- Authorization for applications to use IBM WebSphere 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 WebSphere MQyönetimi yetkisi

IBM WebSphere MQ denetimcileri, çeşitli işlevleri gerçekleştirmeye ilişkin yetkiye gereksinim duyarlar. Bu yetki farklı platformlarda farklı şekillerde elde edilir.

IBM WebSphere MQ yöneticilerinin aşağıdakileri yapmak için yetkisi gerekir:

- IBM WebSphere MQ' ı yönetmek için komut verme komutları
- Şunu kullanın:IBM WebSphere MQ Explorer

Daha fazla bilgi için işletim sisteminize uygun olan konuya bakın.

UNIX ve Pencereler sistemlerinde IBM WebSphere MQ yönetimi yetkisi

IBM WebSphere MQ yöneticisi, mqm grubunun bir üyesidir. Bu grubun tüm IBM WebSphere MQ kaynaklarına erişimi vardır ve IBM WebSphere MQ denetim komutları yayınlayabilir. Bir yönetici, belirli yetkiler için diğer kullanıcılara yetki verebilir.

UNIX ve Windows sistemlerinde bir IBM WebSphere MQ yöneticisi olmak için, kullanıcının *mqm group*üyesi olması gerekir. Bu grup, WebSphere MQürününü kurduğunuzda otomatik olarak yaratılır. Kullanıcıların denetim komutlarını yayınlamasına izin vermek için bunları mqm grubuna eklemelisiniz. Bu, UNIX sistemlerindeki kök kullanıcıyı içerir.

mqm grubuna üye olmayan kullanıcılar için yönetici ayrıcalıkları verilebilir, ancak IBM WebSphere MQ denetim komutları yayınlayamaz ve yalnızca erişim verilen komutları yürütme yetkisine sahip olur.

Additionally, on Pencereler systems, the SYSTEM and Administrator accounts have full access to IBM WebSphere MQ resources.

Mqm grubunun tüm üyeleri, sistemde çalışan herhangi bir kuyruk yöneticisini yönetebilmek de içinde olmak üzere, sistemdeki tüm WebSphere MQ kaynaklarına erişebilirler. Bu erişim, yalnızca mqm grubundan bir kullanıcı kaldırılarak iptal edilebilir. Windows sistemlerinde, Administrators (Yöneticiler) grubunun üyeleri de tüm WebSphere MQ kaynaklarına erişir.

Yöneticiler, WebSphere 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.

WebSphere MQ Explorer, denetim görevlerini gerçekleştirmek için PCF komutları verir. Denetimciler, yerel sistemdeki bir kuyruk yöneticisini denetlemek için WebSphere MQ Explorer olanağını kullanmak için ek yetkilere gerek duymaz. Bir kuyruk yöneticisini başka bir sistemde denetlemek için WebSphere MQ Explorer kullanılırsa, denetimcilerin, PCF komutlarının uzak kuyruk yöneticisi tarafından işlenmesine ilişkin gerekli yetkileri olmalıdır.

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 WebSphere MQ” sayfa 49.
- Kanallar, kanal başlatıcıları, dinleyiciler ve kümelerde çalışan komutlar için bkz. Kanal güvenliği.

For more information about the authority you need to administer WebSphere MQ on UNIX and Pencereler systems, see the related information.

Authorization for applications to use IBM WebSphere MQ

Uygulamalar nesnelere eriştiğinde, uygulamalara ilişkin kullanıcı kimliklerinin uygun yetkiye gereksinimi vardır.

Uygulamalar, MQI çağrıları yayınlayarak aşağıdaki IBM WebSphere MQ nesnelerine erişebilir:

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

Uygulamalar, IBM WebSphere 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 arasında yer alır.

Java için IBM WebSphere MQ sınıflarını, JMS için IBM WebSphere MQ sınıfları, .NET için IBM WebSphere MQ sınıfları ya da Message Service Clients for C/C++ and .NET kullanan uygulamalar, dolaylı olarak MQI ' yi kullanır.

MCA 'lar ayrıca, bu WebSphere MQ nesnelerine erişmek için MCA' larla ilişkili kullanıcı kimlikleri ve MQI çağrıları da yayınlıyor. Bu kullanıcı kimlikleri ve gerekli yetkiler hakkında daha fazla bilgi için bkz. “Kanal yetkisi” sayfa 67.

Yetki denetimi gerçekleştirildiğinde

Bir uygulama kuyruk yöneticisine, kuyruğa, sürece ya da ad listesine erişmeyi denediğinde, yetki denetimleri gerçekleştirilir.

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 WebSphere MQ' ta oturum açmak zorunda kalmaması gerekir. IBM WebSphere MQ , kullanıcıların temeldeki işletim sisteminde oturum açmakta olduğunu ve bunun için kimlik doğrulaması gerçekleştirdiğini varsayar.

Bir uygulama MQOPEN ya da MQPUT1 çağrısını kullanarak IBM WebSphere 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. UNIX, Linux, and Windows' 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 başvuruda bulunabilir. 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 WebSphere 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 ilişkin ek bilgi için bkz. “İleti bağlamı” sayfa 51.

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.

UNIX, Linux ve Windows sistemlerindeki IBM WebSphere MQ nesneleriyle çalışma yetkisi

IBM WebSphere MQ ile sağlanan yetkilendirme hizmeti bileşeni, *nesne yetkili yöneticisi (OAM)*olarak adlandırılır. Kimlik doğrulama ve yetkilendirme denetimleri aracılığıyla erişim denetimi sağlar.

1. Kimlik doğrulaması.

   The authentication check performed by the OAM provided with IBM WebSphere 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 uygulaması tarafından bir MQCSP yapısı sağlandıysa ve MQCSP yapısındaki *AuthenticationType* özniteliğine MQCSP_AUTH_USER_ID_AND_PWD değeri verilirse, bu denetim OAM tarafından MQZID_AUTHENTICATE_USER işlevinde gerçekleştirilir. Bu denetim öğesidir: MQCSP yapısındaki kullanıcı kimliği, eşleşip eşleşmediklerini belirlemek için *IdentityContext* (MQZIC) içindeki kullanıcı kimliğine göre karşılaştırılır. Eşleşmezse, denetim başarısız olur.

Bu temel denetim, kullanıcının tam kimlik doğrulaması olarak tasarlanmamaktadır. Örneğin, MQCSP yapısında sağlanan parolayı denetleyerek kullanıcının gerçekliğinin denetlenmesine gerek yoktur. Ayrıca, uygulama bir MQCSP yapısını gerçekleştiriyorsa, hiçbir denetim gerçekleştirilmez.

Yetkilendirme hizmeti bileşeni aracılığıyla kuyruk yöneticisinde fuller kimlik doğrulama hizmetleri gerekliyse, IBM WebSphere MQ ile birlikte sağlanan OAM bunu önermez. Yeni bir yetki hizmeti bileşeni yazmalı ya da bir satıcıdan edinmeniz gerekir.

2. 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.

UNIX, Linux ve Windows sistemlerinde, *yetkilendirme hizmeti* , bir uygulama, kuyruk yöneticisi, kuyruk, işlem, konu ya da ad listesi olan bir IBM WebSphere MQ nesnesine erişmek için bir MQI çağrısı yayınlarken erişim denetimini sağlar. Bu, alternatif kullanıcı yetkisi ve bağlam bilgilerini belirleme ya da geçirme yetkisi için denetimleri içerir.

Windowsüzerinde, OAM, UAC etkin olduğunda bile, Yöneticilerin üyelerine tüm IBM WebSphere MQ nesnelerine erişim yetkisi verir.

Ayrıca, Windows sistemlerinde, SYSTEM hesabında IBM WebSphere MQ kaynaklarına tam erişim olanağı bulunur.

Ayrıca, yetki hizmeti, bir PCF komutu bu IBM WebSphere 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.

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 WebSphere MQ ürünleri tarafından sağlanan bileşenleri genişletmeleri ya da değiştirmeleri için bileşenler sunmalarına olanak sağlar.

IBM WebSphere MQ ile sağlanan yetkilendirme hizmeti bileşeni, *nesne yetkili yöneticisi (OAM)*olarak adlandırılır. OAM, yarattığınız her kuyruk yöneticisi için otomatik olarak etkinleştirilir.

OAM, erişimi denetleyen her bir IBM WebSphere 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. Windows sistemlerinde, her iki kullanıcı kimliği ve grup tanıtıcısı bir EDL ' de yer alabilirler. 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 WebSphere MQ , tüm UNIX platformlarında 12 karakterlik bir kısıtlamayı gözlemlemeye devam eder. 12 karakterden uzun bir kullanıcı kimliği kullanırsanız, IBM WebSphere MQ bu değeri "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 WebSphere 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.

UNIX, Linux ve Windows sistemlerinde, denetim komutu **setmqaut** yetkileri verir ve bu yetkileri iptal eder ve EDL ' leri korumak için kullanılır. 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.

Herhangi bir yetki denetimi istemiyorsanız, örneğin, bir test ortamında, OAM ' yi devre dışı bırakabilirsiniz.

OAM komutlarına erişmek için PCF ' nin kullanılması
UNIX, Linux ve Windows sistemlerinde, OAM yönetim komutlarına erişmek için PCF komutlarını kullanabilirsiniz.

PCF komutları ve eşdeğer OAM komutları aşağıdaki gibidir:

Çizelge 6. 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 Giriş başlıklı konuya bakın.

Uzaktan ileti sistemine ilişkin güvenlik

Bu bölümde, güvenlik ile uzaktan ileti sistemi konuları ele verilmektedir.

Kullanıcılara IBM WebSphere 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, SSL ya da 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.

UNIX and Linux sistemlerindeki nesnelerin güvenliği

Bu kimlik IBM WebSphere 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 Linux sistemlerindeki 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.

Pencereler sistemlerindeki nesnelerin güvenliği

Bu kimlik IBM WebSphere MQ denetim komutlarını kullanacaksa, yönetim kullanıcılarının hem mqm grubunun hem de Windows sistemlerindeki denetimciler grubunun bir parçası olması gerekir.

Windows sistemlerindeki kullanıcı kimlikleri

Pencereler 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

Windows dışındaki altyapılar, UNIX and Linux sistemleri, iletilerde kullanıcı kimlikleri için büyük harfli karakterler kullanır.

Pencerelersistemlerinde, 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.

UNIX, Linux ve Windows sistemlerinde başka herhangi bir nedenle ileti çıkışı sağlıyorsanız, otomatik dönüştürmeler gerçekleştirilmez.

Özel bir yetki hizmetinin kullanılması

IBM WebSphere MQ , kurulabilir bir yetkilendirme hizmeti sağlar. Alternatif bir hizmet kurmayı seçebilirsiniz.

IBM WebSphere MQ ile birlikte sağlanan yetkilendirme 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 WebSphere 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 7. 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 57) 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	Herhangi bir başka araç için herhangi bir kullanılan kimlik belirlenmediği zaman 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 57) 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 WebSphere MQ MQI istemcileri için, MQI çağrılarını işleyen süreç sunucu bağlantısı MCA ' dır. 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.

Windows altyapılarında MCAUSER alanının 12 karakterle sınırlı olduğundan emin olun; bunun nedeni, yetki hatalarına yol açabilecek fazladan karakterler kesilecektir.

Bir istemci tarafı güvenlik çıkışı kullanımda olduğunda, IBM WebSphere 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/OSiçin, kanal başlatıcı için atanan kullanıcı kimliği, z/OS başlatma yordamları tablosuna göre görevi başlattı.
- TCP/IP (z/OSdışı) 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 WebSphere MQ varsayılan sunucu bağlantısı kanalı (SYSTEM.DEF.SVRCONN), MCAUSER özniteliği boş olarak ayarlanmış olmalıdır. Yetkisiz erişimi önlemek için, varsayılan tanımın MCAUSER özniteliğini, IBM WebSphere MQ MQ nesnelerine erişimi olmayan bir kullanıcı kimliğiyle güncelleyin.

Kullanıcı Kimlikleri

`runmqsc`ile bir kanal tanımladığınızda, kullanıcı kimliği tek tırnak içine alınmadıkça, MCAUSER özniteliği büyük harfe çevrilir.

UNIX, Linux ve Windows sistemlerinde bulunan sunucular için, istemciden alınan `MCAUserIdentifier` alanının içeriği küçük harfe çevrilir.

IBM iüzerindeki sunucular için, istemciden alınan `LongMCAUserIdentifier` alanının içeriği büyük harfe çevrilir.

UNIX and Linux sistemlerindeki sunucular için, istemciden alınan `LongMCAUserIdentifier` alanının içeriği küçük harfe çevrilir.

Varsayılan olarak, bir 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. SSL ya da TLS kullanmayı seçebilirsiniz, 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 58
Bu konu, bağlantı düzeyi güvenlik ve uygulama düzeyi güvenliğinin çeşitli yönleriyle ilgili bilgileri içerir ve iki güvenlik düzeyini karşılaştırır.

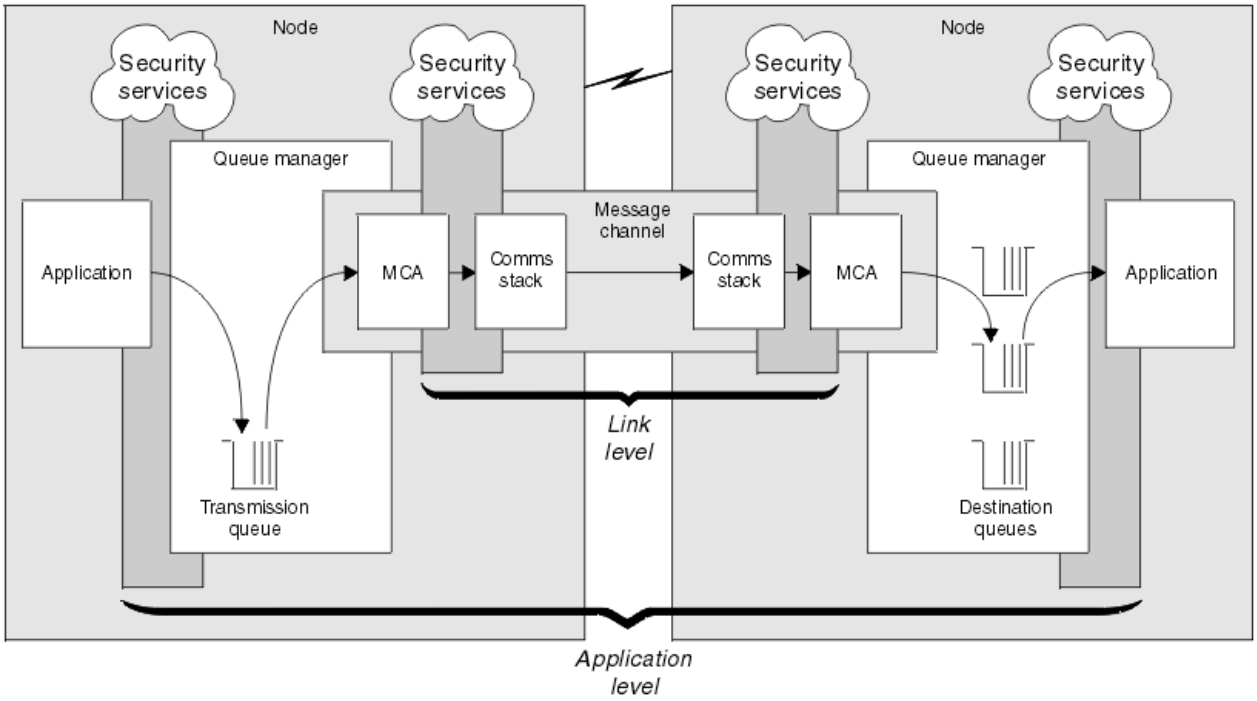
“Kanal çıkış programları” sayfa 63
Kanal çıkış programları , MCA ' nın işlem sırasında tanımlı yerlerde çağrılan programlardır. Kullanıcılar ve satıcılar kendi kanal çıkış programlarını yazabilirler. Bazıları IBMtarafından sağlanır.

“Kanalları SSL ile koruma” sayfa 69
IBM WebSphere MQ ' ta SSL 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 8 sayfa 59içinde gösterilmektedir.



Şekil 8. 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.

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 8 sayfa 59içinde gösterilmektedir.

Denetlenen ve güvenilir ortamlarda çalışmayan kuyruk yöneticileri

Bir kuyruk yöneticisi denetimli ve güvenilir bir ortamda çalıştırılıyorsa, WebSphere MQ tarafından sağlanan erişim denetimi mekanizmaları, kuyruklarda saklanan iletileri korumak için yeterli kabul edilebilir. 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, WebSphere 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 8 sayfa 59içinde 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 WebSphere MQtarafından sağlanan bağlantı düzeyi güvenliği

The primary means of provision of confidentiality and data integrity in IBM WebSphere MQ is by the use of SSL or TLS. IBM WebSphere MQ' ta SSL ve TLS kullanımı hakkında daha fazla bilgi için bkz. “SSL ve TLS içinIBM WebSphere MQ desteği” sayfa 23. For authentication, IBM WebSphere 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, bkz. “Kanal doğrulama kayıtları” sayfa 38.

Kendi bağlantı düzeyi güvenliğinizin sağlanması

Bu konu grubunda, kendi bağlantı düzeyinde güvenlik hizmetlerinizi nasıl sağlayabileceğiniz ele alınmıştır. kendi kanal çıkış programlarınızı yazmak, kendi link seviyesi güvenlik hizmetlerinizi sağlamanın temel yoludur.

Kanal çıkış programları “Kanal çıkış programları” sayfa 63içinde tanıtılır. Aynı konu, Windows için IBM WebSphere MQ ile birlikte sağlanan kanal çıkış programını da açıklar (SSPI kanal çıkış programı). 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, WebSphere MQ' u destekleyen başka bir ürün ya da bu çalışmalardan herhangi birinin bir birleşiminin birlikte çağrılabilir. Uygulama düzeyi güvenlik Şekil 8 sayfa 59' 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.

Gelişmiş İleti Güvenliğiplanlaması

IBM WebSphere MQ Advanced Message Security (AMS) is a separately licensed component of IBM WebSphere MQ that provides a high level of protection for sensitive data flowing through the IBM WebSphere 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 WebSphere MQ. Ancak bu tür çözümler uzman becerilere gereksinim duyar ve bakımı için karmaşık ve pahalı olabilir. IBM WebSphere MQ Advanced Message Security , sanal olarak her tür ticari BT sistemi arasında bilgi taşınırken bu zorlukların ele lanmasına yardımcı olur.

IBM WebSphere MQ Advanced Message Security , IBM WebSphere 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 WebSphere MQ sunucularını, hem de istemcilerini destekler.
- Uçtan uca güvenli ileti sistemi çözümü sağlamak için IBM WebSphere MQ Managed File Transfer ile bütünleştirilir.

Daha fazla bilgi için, bkz. “IBM WebSphere MQ Advanced Message Security” sayfa 262.

Kendi uygulama düzeyinde güvenliğinizin sağlanması
Bu konu grubunda, kendi uygulama düzeyinde güvenlik hizmetlerinizi nasıl sağlayabileceğiniz ele alınmıştır.

Uygulama düzeyinde güvenliği uygulamanıza yardımcı olmak için IBM WebSphere MQ , iki çıkış, API çıkışı ve API geçiş çıkışı sağlar.

Bu çıkışlar, 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 WebSphere 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 WebSphere 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.

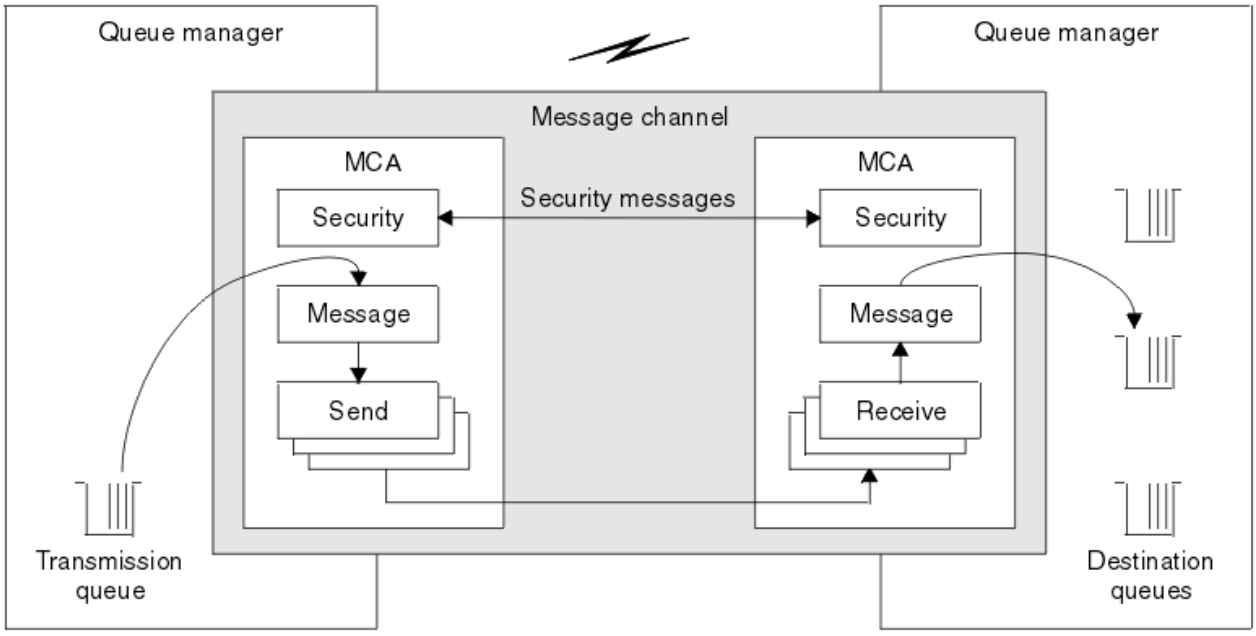
Kanal çıkış programları

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 9 sayfa 64 içinde gösterilmektedir ve aşağıdaki konularda açıklanmaktadır.



Şekil 9. 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 61.

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 WebSphere 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 61.

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 WebSphere 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 WebSphere 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 61.

Planlama verileri bütünlüğü

Verilerinizin bütünlüğünün nasıl korunacağını planlayın.

Veri bütünlüğünü uygulama düzeyinde ya da bağlantı düzeyinde uygulayabilirsiniz.

Uygulama düzeyinde, yetkisiz değişikliklere karşı korumak için iletileri dijital olarak imzalamak için IBM WebSphere MQ Advanced Message Security ' i kullanmayı seçebilirsiniz. Standart tesisler gereksinimlerinizi karşılamazsa, API çıkış programlarını da kullanabilirsiniz.

Bağlantı düzeyinde, SSL ya da TLS kullanmayı seçebilirsiniz, bu durumda dijital sertifikalar kullanımınızı planlamalısınız. Standart tesisler gereksinimlerinizi karşılamazsa, kanal çıkış programlarını da kullanabilirsiniz.

İlgili kavramlar

“Kanalları SSL ile koruma” sayfa 69
IBM WebSphere MQ ' ta SSL desteği, kuyruk yöneticisi kimlik doğrulama bilgileri nesnesini ve çeşitli MQSC komutlarını kullanır. Ayrıca, dijital sertifikalar kullanımınızı da göz önünde bulundurmanız gerekir.

“IBM WebSphere MQiçindeki veri bütünlüğü” sayfa 22
Bir iletinin değiştirilip değiştirilmediğini saptamak için veri bütünlüğü hizmetini kullanabilirsiniz.

“ Gelişmiş İleti Güvenliğiplanlaması” sayfa 62
IBM WebSphere MQ Advanced Message Security (AMS) is a separately licensed component of IBM WebSphere MQ that provides a high level of protection for sensitive data flowing through the IBM WebSphere MQ network, while not impacting the end applications.

İlgili başvurular

API çıkış başvurusu

Kanal-çıkış çağrıları ve veri yapıları

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 WebSphere 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 performans bölümünde yer alıyor.

Denetlenecek veriler

Aşağıdaki bölümlerde açıklandığı gibi, denetlemek için gereksinim duyardığınız veri tiplerini ya da etkinliği göz önünde bulundurun:

IBM WebSphere MQ arabirimlerini kullanarak IBM WebSphere MQ üzerinde yapılan değişiklikler
Özel olarak komut olayları ve yapılandırma olayları olmak üzere, özel işlemden geçirme olaylarını yayınlamak için IBM WebSphere MQ ' i yapılandırın.

IBM WebSphere MQ ' ta denetimin dışında yapılan değişiklikler
Bazı değişiklikler IBM WebSphere MQ ' ın davranışını etkileyebilir, ancak doğrudan IBM WebSphere MQtarafından izlenemez. Bu tür değişikliklere örnek olarak, `mqs.ini`, `qm.ini`ve `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 WebSphere MQ
Kuyruk yöneticilerinin başlatılması ve durdurulması gibi etkinlikleri denetlemek için işletim sistemi araçlarını kullanmak zorunda kalabilirsiniz. Bazı durumlarda, IBM WebSphere MQ , özel işlemden geçirme olaylarını yayınlayabilecek şekilde yapılandırılabilir.

IBM WebSphere MQiçindeki uygulama etkinliği
Uygulamaların eylemlerini denetlemek, örneğin kuyrukların açılması ve iletilerin yerleştirilip alınması, uygun olayları yayınlamak için IBM WebSphere MQ yapılandırmasını yapmak.

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 WebSphere 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 WebSphere 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 WebSphere MQ kaynaklarına erişimi olan bir kullanıcı kimliğine gerek duyarsınız.

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.

WebSphere MQ' da kanallar SSL ya da 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. Ek bilgi için Bağlam için yetkiler başlıklı konuya bakın.

- 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 ilişkilendirilmiş kullanıcı kimliğiyle, iletileri kuyruklara yerleştirmek için hedef kuyrukları açabilirsiniz.

  Bu, Message queuing Interface (MQI) olanağını içerir; bu nedenle, WebSphere MQ Object Authority Manager (OAM) olanağını kullanmadığınızda 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 hesabını kullanacak şekilde, tam yönetim haklarına sahip olacak ve özel yetkiler gerektirmeyecek.

    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.
  - WebSphere yönetim ayrıcalıklarına sahip olmayan bir kullanıcı kimliği kullanırsanız, kanal için, kanala ilişkin dsp ve ctrlx yetkisi, kanal için bu kullanıcı kimliğine çalışabilmelidir. 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. Örneğin, aşağıdaki komutları verin:

```
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 38
Bir kanal düzeyinde sistemler arasında bağlantı kurmak için verilen erişim üzerinde daha kesin bir denetim yapmak için kanal kimlik doğrulama kayıtlarını kullanabilirsiniz.

Kanal kimlik doğrulama kaydı özellikleri

Kanal başlatıcı tanımlarının korunması

Kanal başlatıcılarını yalnızca mqm grubunun üyeleri yönlendirebilir.

IBM WebSphere MQ kanal başlatıcıları IBM WebSphere MQ nesneleri değildir; bunlara erişim OAM tarafından denetlenmez. IBM WebSphere 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 makinede mqm grubunun bir üyesi de 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 yetkilendirme gerektirir; bkz. Çizelge 10 sayfa 88.

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 63 .

Kanalları SSL ile koruma

IBM WebSphere MQ ' ta SSL desteği, kuyruk yöneticisi kimlik doğrulama bilgileri nesnesini ve çeşitli MQSC komutlarını kullanır. Ayrıca, dijital sertifikalar kullanımınızı da göz önünde bulundurmanız gerekir.

SSL desteğine ilişkin komutlar ve öznitelikler

SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) protokolü, dinleme, kurcalama ve kimliğine bürünme karşı koruma sağlayan kanal güvenliği sağlar. SSL içinIBM WebSphere MQ desteği, kanal tanımlamasında, belirli bir kanalda SSL güvenliğini kullanacağını belirtmenizi sağlar. Ayrıca, kullanmak istediğiniz şifreleme algoritması gibi, istediğiniz güvenlik tipine ilişkin ayrıntıları da belirtebilirsiniz.

Aşağıdaki MQSC komutları SSL ' 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 değiştirgeleri SSL ' yi destekler:

SSLCRLNL
SSLCRLNL özniteliği, geliştirilmiş TLS/SSL sertifikası denetlemelerine izin vermek için 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
SSL kullanan bir kanalda SSL bağlantısı kurulamazsa, bir SSL olay iletisinin bildirilip bildirilmeyeceğini belirler.

SLFIPS
Şifreleme donanımında değil, IBM WebSphere MQiçinde 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
Windows,UNIX and Linux sistemlerinde, bir anahtar havuzunu kuyruk yöneticisiyle ilişkilendirir. Anahtar veritabanı, bir *GSKit* anahtar veritabanında tutulur. (The IBM Global Security Kit (GSKit) enables you to use SSL security on Pencereler,UNIX and Linux systems.)

SSLRKEYC
Gizli anahtar yeniden anlaşılmadan önce, SSL etkileşimi içinde gönderilecek ve alınan bayt sayısı. Bayt sayısı, MCA tarafından gönderilen denetim bilgilerini içerir.

Aşağıdaki kanal parametreleri SSL ' yi destekler:

SSLCAUTH
IBM WebSphere MQ ' in SSL istemcisinden bir sertifika gerektirip doğrulamayacağını ve doğrulanıp doğrulamayacağını tanımlar.

SSLCIPH
Şifreleme gücünü ve işlevini belirtir (CipherSpec), örneğin NULL_MD5 ya da RC4_MD5_US. 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 iKeycmd command for managing certificates on UNIX and Linux systems, and the runmqakm tool for managing certificates on UNIX, Linux and Pencereler systems. Aşağıdaki bölümlere bakın:

- setmqaut
- dspmqaut
- dmpmqaut
- rcrmqobj
- rcdmqimg
- dspmqfls
- Anahtarlar ve sertifikaların yönetilmesi

SSL kullanan kanal güvenliğine genel bakış için bkz.

- “SSL ve TLS içinIBM WebSphere MQ desteği” sayfa 23

SSL ile ilişkili MQSC komutlarına ilişkin ayrıntılar için bkz.

- ALTER AUTHORINFO
- DEFINE AUTHINFO
- YAZAR BILGILERINI SIL
- AUTHENTIFO GöRüNTüLE

SSL ile ilişkili PCF komutlarının ayrıntıları için bkz.

- Kimlik Doğrulama Bilgileri Nesnesi Değiştir, Kopyala ve Yarat
- Kimlik Doğrulama Bilgileri nesnesini sil
- Kimlik Doğrulama Bilgileri Nesnesi

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:

UNIX Linux Windows Windows, UNIXve Linux sistemlerinde kendinden onaylı sertifikalar kullanabilirsiniz. Yönergeler için bkz. “UNIX, Linux, and Windows sistemlerinde kendinden onaylı bir kişisel sertifika oluşturma” sayfa 119 .

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, sayısal sertifikanız için uygun bir CipherSpec seçmeniz gerekir. Benzer bir şekilde, kuruluşunuzun güvenlik ilkesi belirli bir CipherSpec kullanılmasını gerektiriyorsa, uygun bir dijital sertifika edinmeniz gerekir.

CipherSpecs ve dijital sertifikalar arasındaki ilişkiyle ilgili daha fazla bilgi için bkz. “Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33

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. WebSphere MQ' da sertifika doğrulama ilkeleri hakkında daha fazla bilgi için bkz. “IBM WebSphere MQiçindeki sertifika geçerlilik denetimi ilkeleri” sayfa 33.

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, WebSphere 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).

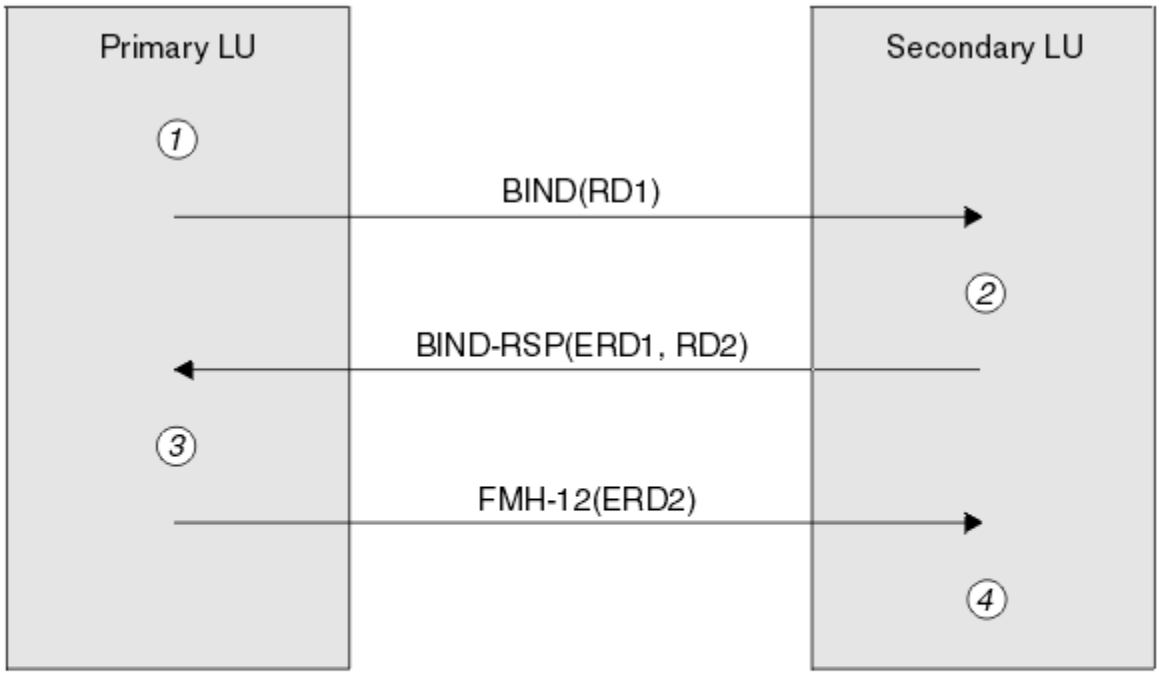
Oturum düzeyi şifrelemesi hakkında daha fazla genel bilgi için bkz. *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

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 10 sayfa 73 , 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 10. Oturum düzeyi kimlik doğrulamasına ilişkin akışlar

Oturum düzeyinde kimlik doğrulamaya ilişkin protokol aşağıdaki gibidir. Yordamlardaki numaralar, Şekil 10 sayfa 73içindeki 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.

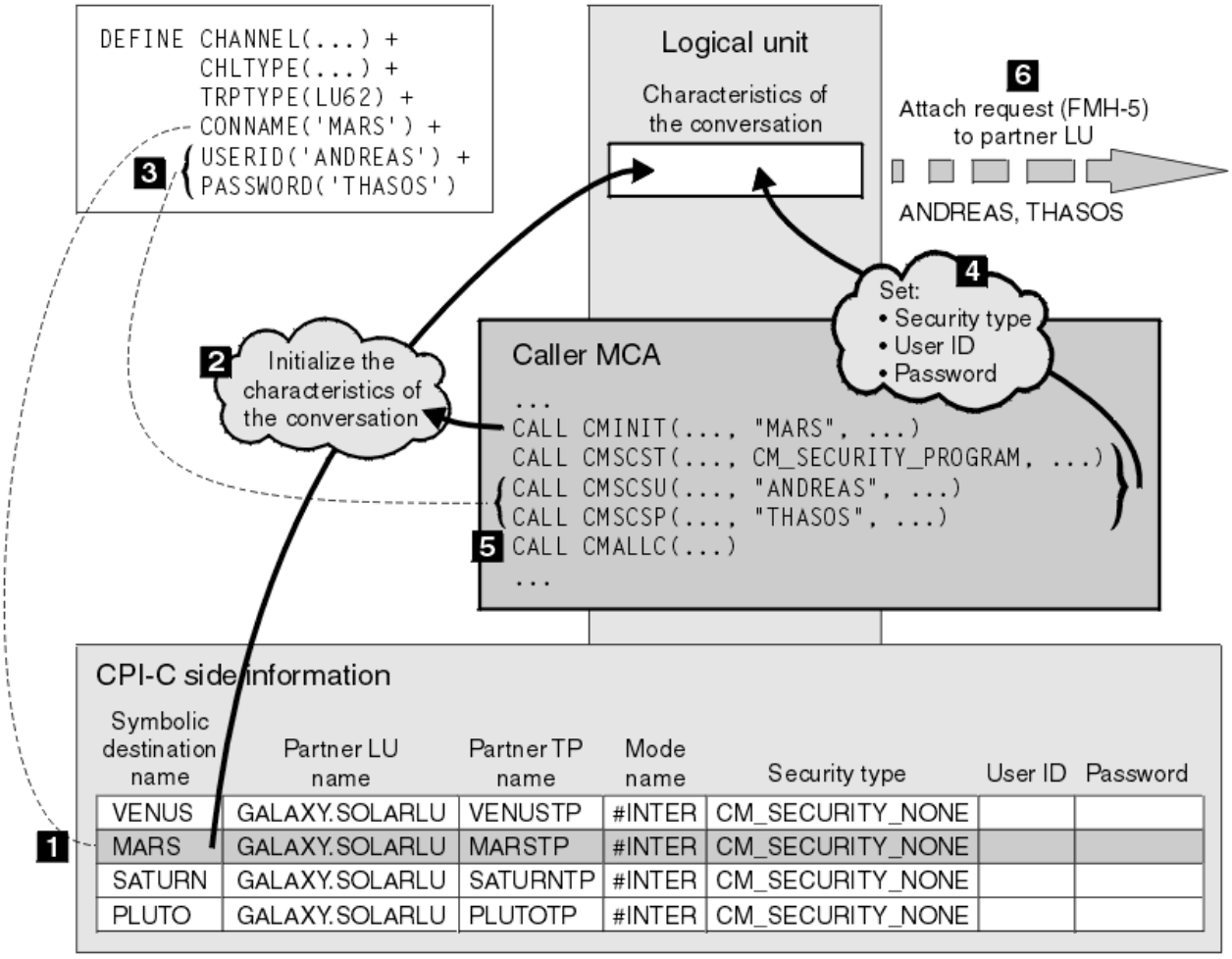
Aşağıdaki konularda, IBM WebSphere MQ ' in etkileşim düzeyi kimlik doğrulaması için destek sağladığı açıklanmaktadır.

Etkileşim düzeyi kimlik doğrulamasıyla ilgili daha fazla bilgi için bkz. *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808. z/OSiçin özel bilgiler için bkz. *z/OS MVS Planning: APPC/MVS Management*, SA22-7599.

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.

UNIX sistemlerinde ve Windows sistemlerinde IBM WebSphere MQ ' ta sohbet düzeyi kimlik doğrulaması desteği
Sohbet düzeyi kimlik doğrulama çalışmalarının UNIX, Linux, and Windows' ta nasıl çalışacağını genel bir bakış elde etmek için bu konuyu kullanın.

The support for conversation level authentication in IBM WebSphere MQ for WebSphere MQ on UNIX systems, and WebSphere MQ for Pencereler is illustrated in Şekil 11 sayfa 75. 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 11. WebSphere MQ etkileşim düzeyi kimlik doğrulaması için destek

IBM i, UNIX sistemleri ve Windows sistemlerinde, 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.

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 WebSphere MQ hangi kuyruk yöneticisinin gönderileceğini karar verir. Birçok uygulama, küme kuyruğuna ileti gönderdiğinde, WebSphere MQ , iş yükünü kuyruğun bir eşgörünümü olan kuyruk yöneticilerinin her birindeki iş yükünü

dengeleir. If one of the systems hosting a cloned queue manager fails, WebSphere 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.

İlgili görevler

“Kuyruk yöneticilerinin ileti alma engellenmesi” sayfa 242
Bir küme kuyruk yöneticisinin çıkış programlarını kullanarak, alma yetkisi olmayan iletileri almasını önleyebilirsiniz.

IBM WebSphere MQ Yayınlama/Abone Olma Güvenliği

IBM WebSphere 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 WebSphere 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 WebSphere 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 WebSphere MQ Multicast.

IBM WebSphere MQ Multicast 'ın yerleşik güvenliği yok. Güvenlik denetimleri, MQOPED zamanındaki kuyruk yöneticisinde işlenir ve MQMD alanı ayarı istemci tarafından işlenir. Ağdaki bazı uygulamalar IBM WebSphere MQ uygulaması olmayabilir (örneğin, LLM uygulamaları, daha fazla bilgi için bkz. WebSphere 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 WebSphere MQ içindeki erişim denetimi kullanıcı kimliklerine dayalıdır. Bu konuyla ilgili daha fazla bilgi için bkz. “İstemciler için erişim denetimi” sayfa 56.

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 WebSphere 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 176.

IBM WebSphere MQ Internet düzgeçiş güvenliği için güvenlik

İnternet üzerinden düzgeçiş, güvenlik duvarından iletişimi basitleştirebilir, ancak bunun güvenlik açısından etkileri vardır.

IBM WebSphere MQ Internet düzgeçişi, SupportPac MS81içinde sağlanan bir IBM WebSphere MQ temel ürün uzantısıdır.

WebSphere MQ Internet düzgeçiş, iki kuyruk yöneticisinin ileti alışverişi için ya da bir WebSphere MQ istemcisi uygulamasının bir kuyruk yöneticisine bağlanmak için, doğrudan TCP/IP bağlantısı gerektirmeden İnternet üzerinden bağlantı kurmasını sağlar. Bir güvenlik duvarının iki sistem arasında doğrudan TCP/IP bağlantısını engelliyorsa, bu olanak yararlı olur. It makes the passage of WebSphere MQ channel protocol flows into and out of a firewall simpler and more manageable by tunnelling the flows inside HTTP or by acting as a proxy. Güvenli Yuva Katmanı 'nın (SSL) kullanılması, Internet üzerinden gönderilen iletileri şifrelemek ve şifrelerini çözmek için de kullanılabilir.

When your WebSphere MQ system communicates with IPT, unless you are using SSLProxyMode in IPT, ensure that the CipherSpec used by WebSphere MQ matches the CipherSuite used by IPT:

- IPT, SSL ya da TLS sunucusu olarak işlev gördüğünde ve WebSphere MQ , SSL ya da TLS istemcisi olarak bağlantı kurduğunda, WebSphere MQ tarafından kullanılan CipherSpec , ilgili IPT anahtar halkasında etkinleştirilmiş bir CipherSuite değerine karşılık gelmelidir.
- IPT, SSL ya da TLS istemcisi olarak hareket ettiğinde ve bir WebSphere MQ SSL ya da TLS sunucusuna bağlandığında, IPT CipherSuite , alan WebSphere MQ kanalında tanımlanan CipherSpec ile eşleşmelidir.

If you migrate from IPT to the integrated WebSphere MQ SSL and TLS support, transfer the digital certificates from IPT Using iKeyman.

Daha fazla bilgi için bkz. WebSphere MQ Internet Pass-Thru (SupportPac MS81).

Güvenliğin ayarlanması

Bu konu derlemi, farklı işletim sistemlerine ve istemcilerin kullanımına özgü bilgileri içerir.

UNIX, Linux, and Windows sistemlerinde güvenliğin ayarlanması

UNIX, Linux, and Windows sistemlerine özgü güvenlik konuları.

IBM WebSphere 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 WebSphere MQ' u yönetebilen
IBM WebSphere MQ' ı denetlemek için komut alabilen kullanıcılar kümesini tanımlayabilirsiniz.

Who can use IBM WebSphere 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 WebSphere 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 WebSphere MQ' e özeldir; MQI kaynaklarına yetki vermek ya da yetkiyi iptal etmek için standart işletim sistemi komutlarını kullanmaz.

Uçbirim Hizmetlerini Kullanarak IBM WebSphere MQ ile bağlantı kurulması

The **Create global objects** user right can cause problems if you are using Terminal Services.

If you are connecting to a Pencereler system by using Terminal Services and you have problems creating or starting a queue manager, this might be because of the user right, **Create global objects**, in recent versions of Pencereler.

Create global objects kullanıcısı, genel ad alanında nesne oluşturmak için yetkilendirilen kullanıcıları sınırlar. In order for an application to create a global object, it must either be running in the global namespace, or the user under which the application is running must have the **Create global objects** user right applied to it.

Administrators have the **Create global objects** user right applied by default, so an administrator can create and start queue managers when connected by using Terminal Services without altering the user rights.

Uçbirim hizmetlerini kullanırken WebSphere MQ yönetim yöntemlerinin çeşitli yöntemleri işe yaramıyorsa, **Create global objects** kullanıcısını doğru olarak ayarlamayı deneyin:

1. Denetim Araçları panosunu açın:

   Windows 2003 ve Windows XP
   Bu panoya **Control Panel** > **Administrative Tools**(Denetim Masası-Yönetim Araçları) seçeneklerini kullanarak erişin

   Windows Vista ve Windows Server 2008
   Bu panoya **Control Panel** > **System and Maintenance** > **Administrative Tools**(Denetim Masası-Sistem ve Bakım-> Yönetim Araçları)
2. **Yerel Güvenlik İlkesi**' ne çift tıklatın.
3. `Local Policies`nesnesini açın.
4. `User Rights Assignment`öğesini tıklatın.
5. Yeni kullanıcıyı ya da grubu **Create global objects** ilkesine ekleyin.

Creating and managing groups on Pencereler

Bu yönergeler, bir iş istasyonundaki ya da üye sunucu makinesinde grupları yönetme işleminde size yol göstermenizi sağlar.

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 üyeliğinde yaptığınız değişiklikler, kuyruk yöneticisi yeniden başlatılıncaya kadar tanınmaz ya da MQSC komutu REFRESH SECURITY (ya da PCF eşdeğeri) komutunu verinceye kadar tanınmaz.

Kullanıcı ve gruplarla çalışmak için Computer Management (Bilgisayar Yönetimi) panosunu kullanın. Oturum açmış olan kullanıcıda yapılan değişiklikler, kullanıcı yeniden oturum açıncaya kadar etkili olmayabilir.

Windows 2003 ve Windows XP
Bu panoya **Control Panel** > **Administrative Tools** > **Computer Management**(Denetim Masası-Yönetim Araçları-Bilgisayar Yönetimi) seçeneklerini

Windows Vista ve Windows Server 2008
Bu panoya erişmek için **Control Panel** > **System and Maintenance** > **Administrative Tools** > **Computer Management**(Denetim Masası-Sistem ve Bakım-> Yönetim Araçları

Windows 7
Bu panoya **Administrative Tools** > **Computer Management**(Yönetim Araçları-Bilgisayar Yönetimi)

Windowsüzerinde 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 'ta Bir Gruba Kullanıcı Eklenmesi

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 'ta 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 'ta Gruptan Bir Kullanıcının Kaldırılması
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.

Creating and managing groups on HP-UX

HP-UX' ta NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için SAM (System Administration Manager; Sistem Denetimi Yöneticisi) olanağını kullanın.

HP-UXüzerinde grup oluşturma
Sistem Denetim Yöneticisi 'ni kullanarak bir gruba kullanıcı ekleme

Yordam

1. System Administration Manager (SAM) olanağından, Kullanıcılar ve Gruplar için Hesapları çift tıklatın.
2. Grupları çift tıklatın.
3. Add a New Group (Yeni Grup Ekle) panosunu görüntülemek için, İşlemler menüsünden Ekle 'yi seçin.
4. Grubun adını girin ve gruba eklemek istediğiniz kullanıcıları seçin.
5. Grubu oluşturmak için Uygula düğmesini tıklatın.

Sonuçlar
Şimdi bir grup oluşturdun.

HP-UXüzerinde bir gruba kullanıcı ekleme
Sistem Denetim Yöneticisi 'ni kullanarak bir kullanıcıyı bir gruba ekleyin.

Yordam

1. System Administration Manager (SAM) olanağından, Kullanıcılar ve Gruplar için Hesapları çift tıklatın.
2. Grupları çift tıklatın.

3. Grubun adını vurgulayın ve Var Olan Bir Grup Değiştir panosunu görüntülemek için İşlemler menüsünden Değiştir 'i seçin.
4. Gruba eklemek istediğiniz bir kullanıcıyı seçin ve Ekle düğmesini tıklatın.
5. Gruba başka kullanıcılar eklemek istiyorsanız, her kullanıcı için 4. adımı yineleyin.
6. Listeye ad eklemeyi bitirdiğinizde Tamam düğmesini tıklatın.

Sonuçlar
Şimdi bir gruba bir kullanıcı eklediniz.

HP-UXüzerinde bir grupta yer alan kişileri görüntüleme
Sistem Denetimi Yöneticisi 'ni kullanarak bir grupta yer alan kişiyi görüntüle

Yordam

1. System Administration Manager (SAM) olanağından, Kullanıcılar ve Gruplar için Hesapları çift tıklatın.
2. Grupları çift tıklatın.
3. Grubun adını vurgulayın ve Gruptaki kullanıcıların bir listesini gösteren, Var Olan Bir Grup Değiştir panosunu görüntülemek için İşlemler menüsünden Değiştir 'i seçin.

Sonuçlar
Grup üyeleri görüntülenir.

HP-UXüzerindeki bir gruptan kullanıcının kaldırılması
Sistem Denetim Yöneticisi 'ni kullanarak bir gruptan bir kullanıcıyı kaldırın.

Yordam

1. System Administration Manager (SAM) olanağından, Kullanıcılar ve Gruplar için Hesapları çift tıklatın.
2. Grupları çift tıklatın.
3. Grubun adını vurgulayın ve Var Olan Bir Grup Değiştir panosunu görüntülemek için İşlemler menüsünden Değiştir 'i seçin.
4. Gruptan kaldırmak istediğiniz kullanıcıyı seçin ve Kaldır düğmesini tıklatın.
5. Gruptan diğer kullanıcıları kaldırmak istiyorsanız, her kullanıcı için 4. adımı yineleyin.
6. Adları listeden kaldırdığınızda Tamam düğmesini tıklatın.

Sonuçlar
Şimdi bir gruptan bir kullanıcıyı kaldırdınız

Creating and managing groups on AIX

AIX' ta, NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için SMITTY özelliğini kullanın.

Grup yaratılması
SMITTY kullanarak bir grup oluşturun.

Yordam

1. SMITTY ' den Güvenlik ve Kullanıcılar seçeneğini belirleyin ve Enter tuşuna basın.
2. Grupları seçin ve Enter tuşuna basın.
3. Add a Group seçeneğini belirleyin ve Enter tuşuna basın.
4. Gruba eklemek istediğiniz grubun adını ve virgülle ayrılmış olarak, gruba eklemek istediğiniz kullanıcıların adlarını girin.
5. Grubu oluşturmak için Enter tuşuna basın.

Sonuçlar
Şimdi bir grup oluşturdun.

Gruba kullanıcı eklenmesi
Bir kullanıcıyı SMITTY kullanarak bir gruba ekleyin.

Yordam

1. SMITTY ' den Güvenlik ve Kullanıcılar seçeneğini belirleyin ve Enter tuşuna basın.
2. Grupları seçin ve Enter tuşuna basın.
3. Grupların özelliklerini değiştir/göster seçeneklerini belirleyin ve Enter tuşuna basın.
4. Grup üyelerinin bir listesini göstermek için grubun adını girin.
5. Gruplara eklemek istediğiniz kullanıcıların adlarını virgüllerle ayırarak ekleyin.
6. Adları gruba eklemek için Enter tuşuna basın.

Gruptaki kişileri görüntüleme
SMITTY kullanan bir grupta yer alan kişiyi görüntüleyin.

Yordam

1. SMITTY ' den Güvenlik ve Kullanıcılar seçeneğini belirleyin ve Enter tuşuna basın.
2. Grupları seçin ve Enter tuşuna basın.
3. Grupların özelliklerini değiştir/göster seçeneklerini belirleyin ve Enter tuşuna basın.
4. Grup üyelerinin bir listesini göstermek için grubun adını girin.

Sonuçlar
Grup üyeleri görüntülenir.

Kullanıcının Gruptan Kaldırılması
Bir kullanıcıyı SMITTY kullanarak gruptan kaldırın.

Yordam

1. SMITTY ' den Güvenlik ve Kullanıcılar seçeneğini belirleyin ve Enter tuşuna basın.
2. Grupları seçin ve Enter tuşuna basın.
3. Grupların özelliklerini değiştir/göster seçeneklerini belirleyin ve Enter tuşuna basın.
4. Grup üyelerinin bir listesini göstermek için grubun adını girin.
5. Gruptan kaldırmak istediğiniz kullanıcıların adlarını silin.
6. Adları gruptan kaldırmak için Enter tuşuna basın.

Sonuçlar
Şimdi bir gruptan bir kullanıcıyı kaldırdınız.

Solaris üzerinde grup yaratılması ve yönetilmesi

Solaris üzerinde, NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için `/etc/group` dosyasını kullanın.

Solaris üzerinde bir grup oluşturma
`groupadd` komutunu kullanarak bir grup oluşturma.

Yordam

Şu komutu yazın: `groupadd` *`group-name`*

Burada *grup-adı* , grubun adıdır.

Sonuçlar
The file `/etc/group` file holds group information.

Solaris üzerinde bir gruba kullanıcı ekleme
usermod komutunu kullanarak bir kullanıcıyı bir gruba ekleyin.

Yordam

Ek bir gruba üye eklemek için, `usermod` komutunu yürütün ve kullanıcının şu anda üyesi olduğu ek grupları ve kullanıcının üyesi olmak için gereken ek grupları listelein.
Örneğin, kullanıcı `groupa`grubunun bir üyesiyse ve `groupb` üyesi olmak ise, şu komutu kullanın: `usermod -G groupa,groupb` *`user-name`* ; burada *kullanıcı-adı* kullanıcı adıdır.

Solaris üzerinde bir grupta kimlerin olduğunu görüntüleme
Bir grubun üyesi olan kişiyi bulmak için, `/etc/group` dosyasında bu grubun girişine bakın.

Solaris üzerindeki bir gruptan bir kullanıcının kaldırılması
usermod komutunu kullanarak bir gruptan bir kullanıcıyı kaldırın.

Yordam

To remove a member from a supplementary group, execute the **usermod** command listing 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 komut kullanılır: `usermod -G groupa,groupb` *`user-name`*; burada *`user-name`* , kullanıcı adıdır.

Creating and managing groups on Linux

Linux' ta NIS ya da NIS + kullanmayasınız, gruplarla çalışmak için `/etc/group` dosyasını kullanın.

Linuxüzerinde bir grup oluşturma
groupadd komutunu kullanarak bir grup oluşturun.

Yordam

Yeni bir grup oluşturmak için şu komutu yazın: `groupadd -g` *`group-ID group-name`*
Burada *grup-tnt* , grubun sayısal tanıtıcısıdır ve *grup-adı* , grubun adıdır.

Sonuçlar
The file `/etc/group` file holds group information.

Linuxüzerinde bir gruba kullanıcı ekleme
usermod komutunu kullanarak bir kullanıcıyı bir gruba ekleyin.

Yordam

Ek bir gruba üye eklemek için, `usermod` komutunu yürütün ve kullanıcının şu anda üyesi olduğu ek grupları ve kullanıcının üyesi olmak için gereken ek grupları listelein.
Örneğin, kullanıcı `groupa`grubunun bir üyesiyse ve `groupb` üyesi olmak ise, şu komut kullanılır: `usermod -G groupa,groupb` *`user-name`*.
, burada *`user-name`* kullanıcı adıdır.

Linux' da bir grupta kimlerin yer aldiğini görüntüleme

getent komutunu kullanarak bir grupta yer alan kişileri görüntüleyin.

Yordam

Bir grubun üyesi olan kişiyi görüntülemek için şu komutu yazın: `getent group` *`group-name`*

Burada *grup-adı* , grubun adıdır.

Kullanıcının Gruptan Kaldırılması

usermod komutunu kullanarak bir gruptan bir kullanıcıyı kaldırın.

Yordam

To remove a member from a supplementary group, execute the **usermod** command listing 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 komut kullanılır: `usermod -G groupa,groupb` *`user-name`*

Burada *kullanıcı-adı* kullanıcı adıdır.

Yetkilendirmeler 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 için 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.

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, açılmakta olan nesnenin adı ya da adlarında değil, bir ad çözüldükten sonra elde edilen nesne adı üzerinde 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 8 sayfa 87, Çizelge 9 sayfa 87, Çizelge 10 sayfa 88ve Çizelge 11 sayfa 88 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 8. MQCONN çağrıları için güvenlik yetkisi gerekli

Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 88)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQCONN	Burada geçerli değil	Burada geçerli değil	MQZAO_CONNECT

Çizelge 9. MQOPEN çağrıları için güvenlik yetkisi gerekli

Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 88)**	**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 89)**	MQZAO_INPUT	Burada geçerli değil	Burada geçerli değil
MQOO_OUTPUT (Olağan kuyruk) **(“3” sayfa 89)**	MQZAO_OUTPUT	Burada geçerli değil	Burada geçerli değil
MQOO_PASPAS_ IDENTITY_CONTEXT **(“4” sayfa 89)**	MQZAO_PASPAS_ IDENTITY_CONTEXT	Burada geçerli değil	Denetim yok
MQOO_PASS_ALL_ CONTEXT **(“4” sayfa 89, “5” sayfa 89)**	MQZAO_PASS _ALL_CONTEXT	Burada geçerli değil	Denetim yok
MQOO_SET_ IDENTITY_CONTEXT **(“4” sayfa 89, “5” sayfa 89)**	MQZAO_SET_ IDENTITY_CONTEXT	Burada geçerli değil	MQZAO_SET_ IDENTITY_CONTEXT **(“6” sayfa 89)**
MQOO_SET_ ALL_CONTEXT **(“4” sayfa 89, “7” sayfa 89)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **(“6” sayfa 89)**

Çizelge 9. MQOPEN çağrıları için güvenlik yetkisi gerekli (devamı var)			
Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 88)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQOO_OUTPUT (İletim kuyruğu) **(“8” sayfa 89)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **(“6” sayfa 89)**
MQOO_SET	MQZAO_SET	Burada geçerli değil	Denetim yok
MQOO_ALTERNATE_ USER_AUTHORITY	**(“9” sayfa 89)**	**(“9” sayfa 89)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“9” sayfa 89, “10” sayfa 89)**

Çizelge 10. MQPUT1 çağrıları için güvenlik yetkilendirmesi gerekiyor			
Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 88)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQPMO_PASPAS_ IDENTITY_CONTEXT	MQZAO_PASPAS_ IDENTITY_CONTEXT **(“11” sayfa 89)**	Burada geçerli değil	Denetim yok
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASPAS_ ALL_CONTEXT **(“11” sayfa 89)**	Burada geçerli değil	Denetim yok
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **(“11” sayfa 89)**	Burada geçerli değil	MQZAO_SET_ IDENTITY_CONTEXT **(“6” sayfa 89)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **(“11” sayfa 89)**	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **(“6” sayfa 89)**
(İletim kuyruğu) **(“8” sayfa 89)**	MQZAO_SET_ ALL_CONTEXT	Burada geçerli değil	MQZAO_SET_ ALL_CONTEXT **(“6” sayfa 89)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**(“12” sayfa 89)**	Burada geçerli değil	MQZAO_ALTERNATE_ USER_AUTHORITY **(“10” sayfa 89)**

Çizelge 11. MQCLOSE çağrıları için güvenlik yetkisi gerekli			
Yetki için gerekli yetki:	**Kuyruk nesnesi (“1” sayfa 88)**	**Süreç nesnesi**	**Kuyruk yöneticisi nesnesi**
MQCO_DELETE	MQZAO_DELETE **(“13” sayfa 89)**	Burada geçerli değil	Burada geçerli değil
MQCO_DELETE _PURGE	MQZAO_DELETE **(“13” sayfa 89)**	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 89).
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 her ikisinin de doğru olması durumunda gerçekleştirilir:

    - Kalıcı bir dinamik kuyruk kapatılmakta ve silinmektedir.
    - Kuyruk, kullanılmakta olan nesne tanıtıcı değeri döndüren MQOPEN çağrısı tarafından yaratılmadı.

    Yoksa, kontrol falan yok.

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 *nesne*

Nesne	**Yetki gerekiyor**
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE
Süreç	MQZAO_CHANGE
Kuyruk yöneticisi	MQZAO_CHANGE
Ad Listesi	MQZAO_CHANGE

Nesne	Yetki gerekiyor
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 *nesne* NOREPLACE (“1” sayfa 94)

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CREATE **(“2” sayfa 94)**
Konu	MQZAO_CREATE **(“2” sayfa 94)**
Süreç	MQZAO_CREATE **(“2” sayfa 94)**
Kuyruk yöneticisi	Burada geçerli değil
Ad Listesi	MQZAO_CREATE **(“2” sayfa 94)**
Kimlik doğrulama bilgileri	MQZAO_CREATE **(“2” sayfa 94)**
Kanal	MQZAO_CREATE **(“2” sayfa 94)**
İstemci bağlantı kanalı	MQZAO_CREATE **(“2” sayfa 94)**
Dinleyici	MQZAO_CREATE **(“2” sayfa 94)**
Hizmet	MQZAO_CREATE **(“2” sayfa 94)**
İletişim bilgileri	MQZAO_CREATE **(“2” sayfa 94)**

DEFINE *nesne* REPLACE (“1” sayfa 94, “3” sayfa 94)

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

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

Nesne	Yetki gerekiyor
İstemci bağlantı kanalı	MQZAO_GÖRÜNTÜLE
Dinleyici	MQZAO_GÖRÜNTÜLE
Hizmet	MQZAO_GÖRÜNTÜLE
İletişim bilgileri	MQZAO_GÖRÜNTÜLE

BAşLAT *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

DURUN *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 KANALI	Kanal	MQZAO_CONTROL
KANALı	Kanal	MQZAO_CONTROL_EXTENDED

Komut	Nesne	Yetki gerekiyor
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	

Komut	Nesne	Yetki 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 yetki yaratma yetkisi verilir.
3. Bu, değiştirilecek nesnenin önceden var olması durumunda geçerlidir. Değilse, bu denetim DEFINE *object* NOREPLACE için olur.

İlgili bilgiler

Kümeleme: REFRESH CLUSTER en iyi uygulamaları kullanma

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 *nesne*

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

Nesne	Yetki gerekiyor
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)**
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 100)**

Copy *nesne* (with replace) (1, 4)

Nesne	Yetki gerekiyor
Kuyruk	MQZAO_CHANGE
Konu	MQZAO_CHANGE

Nesne	Yetki gerekiyor
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* (başkasıyla değiştirilmeden) yarat (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)**
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

Nesne	Yetki gerekiyor
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

Sorgu *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

Inquire *nesne* names

Nesne	Yetki gerekiyor
Kuyruk	Denetim yok
Konu	Denetim yok
Süreç	Denetim yok
Kuyruk yöneticisi	Denetim yok
Ad Listesi	Denetim yok

Nesne	Yetki gerekiyor
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	
Küme Sıfırlama	'mqm' grup üyeliği gerekiyor	
Kuyruk Yöneticisi Kümesini Askıya Al	'mqm' grup üyeliği gerekiyor	
Sürdürme Kuyruğu Yöneticisi Kümesi	'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 yetki 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.

Pencerelerüzerinde güvenlik için özel dikkat edilmesi gereken noktalar

Bazı güvenlik işlevleri Pencereler' un farklı sürümlerinde farklı davranır.

IBM WebSphere MQ güvenliği, kullanıcı yetkileri ve grup üyeliklerine ilişkin bilgi için işletim sistemi API ' larına çağrılara dayanır. Bazı işlevler Windows sistemlerinde aynı şekilde işlev görmez. Bu konu topluluklarında, IBM WebSphere MQ ' u bir Windows ortamında çalıştırırken bu farklılıkların IBM WebSphere MQ güvenliğini nasıl etkileyebileceğinin açıklamaları yer alır.

SSPI kanal çıkış programı

Pencereler için WebSphere MQ , 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, Pencereler 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 desteği 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, WebSphere MQ Sürüm 7.0tarafından desteklenen tüm Windows altyapılarında desteklenir.

Bu hizmet genellikle bir MQI kanalında, sunucu kuyruk yöneticisinin bir WebSphere MQ MQI istemci 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 , WebSphere MQ Sürüm 7.0tarafından desteklenen tüm Windows altyapılarında 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 yöneticisinin ve WebSphere MQ MQI istemcisi 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'da bir' grup bulunamadı ' hatası elde ettiğinde

Windows sunucuları, etki alanı denetleyicilerine yükseltildiğinde ya da alan denetleyicilerinden indirgendiğinde, WebSphere MQ yerel mqm grubuna erişimi kaybettiğinden bu sorun oluşabilir. Bu sorunu gidermek için yerel mqm grubunu yeniden yaratın.

Bu belirti, yerel bir mqm grubunun eksikliğini gösteren bir hatadır; örneğin:

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

Altering the state of a machine between server and domain controller can affect the operation of WebSphere MQ, because WebSphere MQ uses a locally-defined mqm group. 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 sorunu gidermek için, standart Windows yönetim araçlarını kullanarak yerel mqm grubunu yeniden yaratın. Tüm grup üyeliği bilgileri kaybolduğundan, yeni oluşturulan yerel mqm grubundaki ayrıcalıklı WebSphere MQ kullanıcılarını yeniden yürürlüğe getirmeniz gerekir. Makine bir etki alanı üyesiyse, ayrıcalıklı etki alanı WebSphere MQ kullanıcı kimlikleri gereken yetki düzeyini vermek için, etki alanı mqm grubunu yerel mqm grubuna da eklemelisiniz.

Windows' da IBM WebSphere MQ ve etki alanı denetleyicileriyle ilgili sorunlarda bulunduğunuzda

Certain problems can arise with security settings when Pencereler servers are promoted to domain controllers.

Etki alanı denetleyicilerine Pencereler 2000, Pencereler 2003 ya da Pencereler Server 2008 sunucuları yükseltilirken, kullanıcı ve grup izinleriyle ilgili varsayılan ya da varsayılan olmayan bir güvenlik ayarı seçme seçeneği sunulur. Bu seçenek, rasgele kullanıcıların etkin dizinden grup üyeliklerini alabildiğini denetler. Because WebSphere MQ relies on group membership information to implement its security policy, it is important that the user ID that is performing WebSphere MQ operations can determine the group memberships of other users.

Windows 2000 'de, varsayılan güvenlik seçeneği kullanılarak bir etki alanı yaratıldığında, kuruluş işlemi sırasında WebSphere MQ tarafından yaratılan varsayılan kullanıcı kimliği, zorunlu olarak diğer kullanıcılara ilişkin grup üyeliklerini elde edebilir. Ürün daha sonra olağan biçimde kurulur, varsayılan nesneler yaratır ve kuyruk yöneticisi gerekiyorsa, yerel ve etki alanı kullanıcılarının erişim yetkisini saptayabilir.

Windows 2000 'de, varsayılan güvenlik seçeneği kullanılarak bir etki alanı yaratıldığında varsayılan olmayan güvenlik seçeneği kullanılarak bir etki alanı yaratıldığında ya da Windows 2003 ve Windows Server 2008 'de bir etki alanı yaratıldığında, kuruluş sırasında WebSphere MQ tarafından yaratılan kullanıcı kimliği, her zaman gerekli olan grup üyeliklerini saptayamaz. Bu durumda bilmeniz gerekir:

- Varsayılan değer olarak, varsayılan değer olan Pencereler 2003 ve Pencereler Server 2008 ile Pencereler 2000, güvenlik izinleri de nasıl davranır
- Etki alanı mqm grubu üyelerinin grup üyeliklerini okumasına nasıl izin verileceği
- How to configure an IBM WebSphere MQ Windows service to run under a domain user

Varsayılan değer olan Pencereler 2003 ve Pencereler Server 2008 etki alanına sahip Pencereler 2000 etki alanı, güvenlik izinleri

WebSphere MQ kuruluşu, yerel kullanıcının ya da etki alanı kullanıcısının kuruluşu gerçekleştirmesine bağlı olarak, bu işletim sistemlerinde farklı bir şekilde davranır.

Bir **yerel** kullanıcı WebSphere MQ' yı kurarsa, Prepare WebSphere MQ Wizard, IBM WebSphere MQ Windows hizmeti için oluşturulan yerel kullanıcının, kuran kullanıcının grup üyeliği bilgilerini alabileceğini algılar. The Prepare WebSphere MQ Wizard asks the user questions about the network configuration to determine whether there are other user accounts defined on domain controllers running on Pencereler 2000 or later. Böyle bir durumda, IBM WebSphere MQ Windows hizmetinin belirli ayarları ve yetkileri olan bir etki alanı kullanıcı hesabı altında çalışması gerekir. Prepare WebSphere MQ Wizard, kullanıcıya bu kullanıcının hesap ayrıntıları için bilgi isteminde bulunur. Çevrimiçi yardımı, etki alanı yöneticisine gönderilebilir olan etki alanı kullanıcı hesabının ayrıntılarını sağlar.

Bir **etki alanı** kullanıcısı WebSphere MQ' yı kurarsa, Prepare WebSphere MQ Wizard, IBM WebSphere MQ Windows hizmeti için oluşturulan yerel kullanıcının kuruluş kullanıcısının grup üyeliği bilgilerini alamıyor olduğunu algılar. Bu durumda, Prepare WebSphere MQ Sihirbazı her zaman kullanıcıya, kullanılacak IBM WebSphere MQ Windows hizmeti için etki alanı kullanıcı hesabının hesap ayrıntılarının girmesini ister.

When the IBM WebSphere MQ Windows service needs to use a domain user account, WebSphere MQ cannot operate correctly until this has been configured using the Prepare WebSphere MQ Wizard. Prepare WebSphere MQ Wizard, Windows hizmeti uygun bir hesapla yapılandırılıncaya kadar, kullanıcının diğer görevlerle devam etmesini sağlar.

Bir Windows 2000 etki alanı varsayılan olmayan güvenlik izinleriyle yapılandırıldıysa, WebSphere MQ ' un doğru şekilde çalışması için olağan çözüm, yukarıda açıklandığı gibi, bunu uygun bir etki alanı kullanıcı hesabıyla yapılandırmasıdır.

Ek bilgi için WebSphere MQ için etki alanı hesaplarının yaratılması ve ayarlanmasıSeekonusuna bakın.

Configuring IBM WebSphere MQ Services to run under a domain user on Windows
Etki alanı kullanıcı hesabının hesap ayrıntılarına girmek için Prepare IBM WebSphere MQ sihirbazını kullanın. Diğer bir seçenek olarak, kuruluşa özgü IBM WebSphere MQ Hizmeti için **Oturum Aç** ayrıntılarını değiştirmek üzere Computer Management (Bilgisayar Yönetimi) panosunu kullanabilirsiniz.

Daha fazla bilgi için bkz. IBM WebSphere MQ Windows hizmeti kullanıcı hesabının parolasının değiştirilmesi

Güvenlik şablonu dosyalarının Windows 'a uygulanması

Bir şablon uygulandığında, WebSphere MQ dosyaları ve dizinlerine uygulanan güvenlik ayarları etkilenebilir. If you use the highly secure template, apply it before installing WebSphere MQ.

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. Özellikle, 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, WebSphere MQ dosyaları ve dizinlerine uygulanan güvenlik ayarlarını etkileyebilir. If you want to use the Highly Secure template, configure your machine before you install WebSphere MQ.

Yüksek düzeyde güvenli şablonu, WebSphere MQ ' un kurulu olduğu bir makineye uygulıyorsanız, WebSphere MQ dosyaları ve dizinlerinde ayarladığınız tüm izinler kaldırılır. Bu izinler kaldırıldığı için, *Yönetici*, *mqm*ve uygun olduğunda *Herkes* grup erişimini hata dizinlerinden kaybedersiniz.

İçiçe gruplar

İçiçe yerleşimli grupların kullanımına ilişkin kısıtlamalar vardır. Bu sonuç kısmen etki alanı işlevsel düzeyinden ve kısmen de WebSphere 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 düzeyinde yer alıyor. (Windows server 2003, Windows XP, Windows Vista ve Windows Server 2008, 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, WebSphere MQtarafından kullanılan tanıtıcılar için ek sınırlamalar da uygulanır. WebSphere MQ tarafından kullanılan ağ API ' leri, etki alanı işlevsel düzeyi tarafından desteklenen tüm yapılandırmaları desteklemez. Sonuç olarak, WebSphere MQ , bir Etki Alanı Yerel grubunda bulunan herhangi bir Etki Alanı Tanıtıcılarının grup üyeliklerini sorgulamayamaz; bu grup, yerel bir grupta içiçe yerleştirilmiş olan bir Etki Alanı Yerel grubunda yer alan grup üyeliklerini sorgulamaz. Ayrıca, genel ve evrensel grupların birden çok içiçe yerleştirilmesi desteklenmez. Ancak, hemen iç içe geçmiş genel gruplar ya da genel gruplar desteklenir.

IBM WebSphere MQ' a bağlanan Windows uygulamaları için ek yetki yapılandırılması

Uygulama süreçlerine erişim izni verilebilmesi için IBM WebSphere MQ işlemlerinin çalıştırıldığı hesabın ek yetkilendirmeye gereksinim duyabilir.

You might experience problems if you have Pencereler applications, for example ASP pages, connecting to IBM WebSphere MQ that are configured to run at a security level higher than usual.

IBM WebSphere MQ , belirli eylemleri koordine etmek için uygulama süreçlerine erişim için SENKRONIZE erişimi gerektirir. APAR IC35116 , uygun ayrıcalıkların belirtilebilmesi için IBM WebSphere MQ ' yi değiştirdi. However, the account under which IBM WebSphere MQ processes run might need additional authorization before the requested access can be granted.

Bir sunucu uygulaması ilk kez bir kuyruk yöneticisine bağlanmayı denediğinde IBM WebSphere MQ , IBM WebSphere MQ denetimcileri için uyumlulaştırma yetkisi vermek üzere süreci değiştirir. IBM WebSphere MQ işlemlerinin çalıştırıldığı kullanıcı kimliği için ek yetki yapılandırmak için aşağıdaki adımları tamamlayın:

1. Yerel Güvenlik İlkesi aracını başlatın, Güvenlik Ayarları-> Yerel İlkeler-> Kullanıcı Sağ Atamaları seçeneklerini tıklatın ve "Hata Ayıklama Programları" seçeneğini tıklatın.
2. "Hata Ayıklama Programlarını" çift tıklatın, daha sonra IBM WebSphere 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.

HP Integrity NonStop Serverüzerinde güvenliğin ayarlanması

HP Integrity NonStop Server sistemlerine özgü güvenlik konuları.

HP Integrity NonStop Server için IBM WebSphere MQ istemcisi, bir kuyruk yöneticisine bağlarken bağlantı düzeyinde güvenlik sağlamak için hem Transport Layer Security (TLS) hem de Secure Sockets Layer (SSL) protokollerini destekler. Bu protokoller, OpenSSLuygulamasının bir somutlaması kullanılarak desteklenir. OpenSSL , güçlü şifreleme işlemleri sağlamak için rasgele veri kaynağı gerektirir.

OpenSSL

HP Integrity NonStop Serveriçin IBM WebSphere MQ istemcisi içinOpenSSL güvenliğine genel bakış.

OpenSSL araç takımı, bir ağ üzerinden güvenli iletişim için Güvenli Yuva Katmanı (SSL) ve İletim Arabirimi Katmanı Güvenliği (TLS) protokollerinin açık kaynaklı bir uygulamasıdır.

Araç takımı OpenSSL Project tarafından geliştirilir. OpenSSL Projesiyle ilgili daha fazla bilgi için bkz. https://www.openssl.org. IBM WebSphere MQ client for HP Integrity NonStop Server contains modified versions of the OpenSSL libraries and the **openssl** command. Kitaplıklar ve **openssl** komutu OpenSSL araç takımı 1.0.1ciçinden raporlanır ve yalnızca nesne kodu olarak sağlanır. Kaynak kod sağlanmadı.

OpenSSL kitaplıkları, gerektiği şekilde dinamik olarak IBM WebSphere MQ istemci uygulama programları tarafından yüklenir. Yalnızca IBM WebSphere MQ tarafından sağlanan OpenSSL kitaplıkları, IBM WebSphere MQ istemci uygulamalarıyla birlikte kullanılmak üzere desteklenir.

Sertifika yönetimi amacıyla kullanılabilecek **openssl** komutu, `opt_installation_path/opt/mqm/bin`OSS dizinine kurulur.

openssl komutunu kullanarak, çeşitli ortak veri biçimleriyle anahtarlar ve sayısal sertifikalar yaratabilir ve bunları yönetebilir ve basit sertifika yetkilisi (CA) görevlerini gerçekleştirebilirsiniz.

OpenSSL tarafından işlenen anahtar ve sertifika verileri için varsayılan biçim Privacy Enhanced Mail (PEM) biçimidir. PEM biçimindeki veriler base64 ile kodlanmış ASCII veridir. Bu nedenle, veriler, e-posta gibi metin tabanlı sistemler kullanılarak aktarılabilir ve metin düzenleyicileri ve web tarayıcıları kullanılarak kesilebilir ve yapıştırılabilir. PEM, metin tabanlı kriptografik alışverişler için bir İnternet standardır ve 1421, 1422, 1423 ve 1424 Internet RFC ' lerinde belirtilir. IBM WebSphere MQ , uzantısı `.pem` olan bir dosyanın PEM biçiminde veri içerdiğini varsayar. PEM biçimindeki bir dosya, birden çok sertifika ve diğer kodlanmış nesneler içerebilir ve açıklamaları içerebilir.

Diğer işletim sistemlerinde IBM WebSphere MQ SSL desteği, Dosyalarda anahtar ve sertifika verilerinin Ayırt Edici Kodlama Kuralları (DER) kullanılarak şifrelenmesi için gerekli olabilir. DER, güvenli iletişimde ASN.1 gösteriminin kullanılmasıyla ilgili bir kodlama kuralları kümesidir. DER kullanılarak kodlanan veriler ikili verilerdir ve DER kullanılarak kodlanan anahtar ve sertifika verilerinin biçimi de PKCS#12 ya da PFX olarak da bilinir. Bu verileri, genel olarak `.p12` ya da `.pfx`uzantısını içeren bir dosya içerir. **openssl** komutu, PEM ile PKCS#12 biçimi arasında dönüştürme yapabilir.

Entropi Cini

OpenSSL , güçlü şifreleme işlemleri sağlamak için rasgele veri kaynağı gerektirir. Rasgele sayı oluşturma, genellikle işletim sistemi ya da sistem genelinde yardımcı program işlemi tarafından sağlanan bir yetenektir. HP Integrity NonStop Server işletim sistemi, işletim sistemi içinde bu yeteneği sağlamaz.

HP Integrity NonStop Serveriçin IBM WebSphere MQ istemcisiyle birlikte sağlanan SSL ve TLS desteğini kullanırken, rasgele veri kaynağını sağlamak için entropi yardımcı programı adı verilen bir işlem gerekir.

SSL ya da TLS gerektiren bir istemci kanalı başlattığınızda, OpenSSL , bir entropi yardımcı programının çalışır durumda olmasını ve hizmetlerinin OSS dosya sisteminde bulunan bir yuvaya `/etc/egd-pool`' de sağlanmasını bekler.

An entropy daemon is not provided by IBM WebSphere MQ client for HP Integrity NonStop Server. HP Integrity NonStop Server için IBM WebSphere MQ istemcisi aşağıdaki entropi yardımcı programı ile sınanmaktadır:

- amqjkdm0 (IBM WebSphere MQ 5.3 sunucusu tarafından sağlandığı gibi)
- `/usr/local/bin/prngd` (Sürüm 0.9.27, HP Integrity NonStop Server Open Source Technical Library tarafından sağlandığı gibi)

IBM WebSphere MQ MQI istemci güvenliğinin ayarlanması

İstemci uygulamalarının sunucudaki kaynaklara sınırsız erişimi olmadığından, IBM WebSphere MQ MQI istemci 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.

  SSL ya da TLS içinde karşılıklı kimlik doğrulaması kullanmanız gerekir. Daha fazla bilgi için bkz. “SSL ya da TLS ile çalışma” sayfa 108
- 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 154.

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. “İstemcinin değerlendirilen bir kullanıcı kimliğini MCAUSER kullanıcı kimliğiyle eşlenmesi” sayfa 179.

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 38.

MQI istemcisinde çalıştırma sırasında yalnızca FIPS onaylı CipherSpecs ' in kullanıldığını belirtme

Anahtar havuzlarınızı FIPS uyumlu yazılım kullanarak yaratın ve kanalın FIPS onaylı CipherSpecs' ı kullanması gerektiğini belirtin.

Çalıştırma zamanında FIPS uyumlu olmak için, anahtar havuzları, -fips seçeneğiyle runmqakm gibi yalnızca FIPS uyumlu yazılım kullanılarak oluşturulmuş ve yönetilmelidir.

Bir SSL ya da TLS kanalının yalnızca FIPS onaylı CipherSpecs ' i öncelik sırasına göre üç şekilde kullanması gerektiğini belirtebilirsiniz:

1. MQSCO yapısındaki FipsRequired alanını MQSSL_FIPS_YES olarak ayarlayın.
2. MQSSLFIPS ortam değişkenini YES olarak ayarlayın.
3. İstemci yapılandırma dosyasında SSLFipsRequired özniteliğini YES olarak ayarlayın.

Varsayılan olarak, FIPS onaylı CipherSpecs gerekli değildir.

Bu değerler, ALTER QMGR SSLFIPS ' deki eşdeğer parametre değerleriyle aynı anlamlara sahiptir (bkz. ALTER QMGR). İstemci işleminin etkin SSL ya da TLS bağlantısı yoksa ve SSL MQCONNX üzerinde bir FipsRequired değeri geçerli olarak belirtilirse, bu işlemle ilişkili sonraki tüm SSL bağlantılarında yalnızca bu değerle ilişkili CipherSpecs ' i kullanmalıdır. Bu, bu ve diğer tüm SSL ya da TLS bağlantıları duruncaya kadar geçerli olur; bu aşamada sonraki bir MQCONNX, FipsRequirediçin yeni bir değer sağlayabilir.

Şifreleme donanımı varsa, WebSphere MQ tarafından kullanılan şifreleme modülleri, donanım ürünü tarafından sağlanan modüller olacak şekilde yapılandırılabilir ve bunlar belirli bir düzey için FIPS onaylı olabilir. Yapılandırılabilir modüller ve bunların FIPS onaylı olup olmadıkları donanım ürününe bağlı olarak değişir.

Mümkün olduğunda, FIPS-only CipherSpecs yapılandırıldıysa, MQI istemcisi, MQRC_SSL_INITIALIZATION_ERROR ile FIPS dışı bir CipherSpec belirten bağlantıları reddeder. WebSphere MQ , bu tür bağlantıların tümünü reddetmeyi garanti etmez ve WebSphere MQ yapılanışınızın FIPS-uyumlu olup olmadığını belirlemek sizin sorumluluğunuzda.

İlgili kavramlar

“ UNIX, Linuxve Windows için Federal Bilgi İşleme Standartları (FIPS)” sayfa 26
Windows, UNIX and Linux sistemlerinde bir SSL ya da TLS kanalında şifreleme gerektiğinde, WebSphere 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 geçti.

İstemci yapılandırma dosyasının SSL kısmı

İlgili başvurular

FipsRequired (MQlong)

MQSSLFIPS

SSL ya da TLS istemcisi uygulamalarının, AIXüzerinde GSKit V8.0 birden çok kuruluşuyla çalıştırılması

SSL or 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 kuruluşu olan bir AIX sisteminde istemci uygulamaları çalıştırırken, istemci bağlanma çağrıları SSL ya da TLS kullanıldığında 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 WebSphere MQ istemcisinin iki farklı GSKit V8.0 kuruluşundan karışık bir kitaplık kümesi yüklemesine neden olmuştur. Db2 ortamında birIBM WebSphere MQ istemcisi uygulamasının yürütülmesi bu hataya neden olabilir.

Bu hatayı önlemek için, kitaplık yolunun önüne IBM WebSphere MQ kitaplık dizinlerini ekleyin; böylece, IBM WebSphere MQ kitaplıkları öncelik kazanır. 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 (set WebSphere MQ ortamı)

UNIX, Linux, and Windows sistemlerinde SSL ya da TLS ' ye ilişkin iletişimlerin ayarlanması

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.

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 Windows sistemlerinde SSL ya da TLS ile çalışma” sayfa 111.

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 WebSphere MQ uygulaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

UNIX, Linux ve Windows sistemlerinde, SSL ya da TLS istemcisi, yalnızca doğru IBM WebSphere 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 WebSphere MQ istemcisi için `ibmwebspheremq` , ardından oturum açma kullanıcı kimliğiniz küçük harfe çevrilerek değiştirildi; örneğin, `ibmwebspheremqmyuserid`.

IBM WebSphere 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, bkz. “SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanması” sayfa 199.

SSL ya da TLS ile çalışma

These topics give instructions for performing single tasks related to using SSL or TLS with IBM WebSphere MQ.

Bunlardan çoğu, aşağıdaki bölümlerde açıklanan üst düzey görevlerde adım olarak kullanılır:

- “Kullanıcıların tanımlanması ve kimlik doğrulaması” sayfa 140
- “Nesnelere erişim yetkisi verme” sayfa 154
- “İletilerin gizliliği” sayfa 199
- “İletilerin veri bütünlüğü” sayfa 220
- “Kümeleri güvenli tutma” sayfa 238

Working with SSL or TLS on HP Integrity NonStop Server

Güvenlik hizmetleri, bileşenler, desteklenen iletişim kuralı sürümleri, desteklenen CipherSpecsve desteklenmeyen güvenlik işlevselliği dahil olmak üzere HP Integrity NonStop Server OpenSSL güvenlik uygulaması için IBM WebSphere MQ istemcisini açıklar.

IBM WebSphere MQ SSL ve TLS desteği, istemci kanalları için aşağıdaki güvenlik hizmetlerini sağlar:

- Sunucunun kimlik doğrulaması ve isteğe bağlı olarak, istemcinin kimlik doğrulaması.
- Bir kanalda akan verilerin şifrelenmesi ve şifresinin çözülmesi.
- Bütünlük, bir kanalda akan verilerde denetler.

HP Integrity NonStop Server için IBM WebSphere MQ istemcisiyle birlikte sağlanan SSL ve TLS desteği aşağıdaki bileşenlerden oluşur:

- OpenSSL kitaplıkları ve **`openssl`** komutu.
- IBM WebSphere MQ parola şifreleme komutu, **`amqrsslc`**.

SSL ya da TLS istemci kanalı işlemi için gerekli olan aşağıdaki bileşenler, HP Integrity NonStop Serveriçin IBM WebSphere MQ istemcisiyle birlikte sağlanmaz:

- OpenSSL şifrelemesi için rasgele veri kaynağı sağlayan bir entropi yardımcı programı.

Desteklenen protokol sürümleri

HP Integrity NonStop Server için IBM WebSphere MQ istemcisi aşağıdaki iletişim kuralı sürümlerini destekler:

- SSL 3.0
- TLS 1.0
- TLS 1.2

Desteklenen CipherSpecs

HP Integrity NonStop Server için IBM WebSphere MQ istemcisi aşağıdaki CipherSpecs sürümlerini destekler:

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

Desteklenmeyen güvenlik işlevi

HP Integrity NonStop Server için IBM WebSphere MQ istemcisi şu anda desteklenmiyor:

- PKCS#11 Şifreleme donanımı desteği
- LDAP Sertifikası İptal Listesi denetimi
- OCSP Çevrimiçi Sertifika Durumu İletişim Kuralı denetimi
- FIPS 140-2, NSA SUIT B şifreleme takımı denetimleri

Sertifika yönetimi

Sayısal sertifika ve sertifika iptal bilgilerini saklamak için bir dosya kümesi kullanın.

IBM WebSphere MQ SSL ve TLS desteği, sayısal sertifika ve sertifika iptal bilgilerini saklamak için bir dosya kümesi kullanır. These files are located in a directory specified either programmatically by way

of the KeyRepository field in the MQSCO structure passed on the MQCONNX call, by the *MQSSLKEYR* environment variable, or, in the SSL stanza of the `mqclient.ini` using the SSLKeyRepository attribute.

MQSCO yapısı, ini dosyası stanza değerine göre öncelik veren MQSSLKEYR ortam değişkenine göre önceliklidir.

Önemli: Anahtar havuzu konumu, HP Integrity NonStop Server platformunda bir dosya adı değil, bir dizin konumunu belirtir.

HP Integrity NonStop Server için IBM WebSphere MQ istemcisi, anahtar havuzu konumundaki aşağıdaki, büyük/küçük harf duyarlı dosyaları kullanır:

- "Kişisel sertifika deposu" sayfa 110
- "Sertifika güvenilirlik deposu" sayfa 110
- "Tümcecik parola saklama dosyası" sayfa 110
- "Sertifika iptal listesi dosyası" sayfa 111

Kişisel sertifika deposu
Kişisel sertifika deposu dosyası (`cert.pem`).

Bu dosya, kişisel sertifikasını ve istemcinin PEM biçiminde kullanması için şifrelenmiş özel anahtarı içerir. SSL ya da TLS kanallarını istemci kimlik doğrulaması gerektirmeyen TLS kanalları kullanıyorsanız, bu dosyanın varlığı isteğe bağlıdır. Kanal tanımında istemci kimlik denetiminin gerektirdiği durumlarda ve SSLCAUTH (gerekli), bu dosyanın var olması ve hem sertifika hem de şifrelenmiş özel anahtarı içermemesi gerekir.

Sertifika deposunun sahibine okuma erişimine izin vermek için dosya izinlerinin bu dosyada ayarlanması gerekir.

Doğru biçimlendirilmiş bir `cert.pem` dosyası, aşağıdaki üstbilgiler ve altbilgiler ile tam olarak iki bölüm içermelidir:

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

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

Şifrelenmiş özel anahtara ilişkin geçiş tümcecik, " `Stash.sth`" geçiş tümcecik parola saklama dosyasında saklanır.

Sertifika güvenilirlik deposu
Sertifika güvenilirlik deposu dosyası (`trust.pem`).

Bu dosya, istemcinin BEM biçiminde bağlandığı kuyruk yöneticileri tarafından kullanılan kişisel sertifikaların doğrulanması için gerekli olan sertifikaları içerir. Sertifika güvenilirlik deposu, tüm SSL ya da TLS istemci kanalları için zorunludur.

Dosya izinlerinin bu dosyaya yazma erişimini sınırlamak için ayarlanması gerekir.

Doğru biçimlendirilmiş bir `trust.pem` dosyası, aşağıdaki üstbilgileri ve altbilgileri içeren bir ya da daha fazla bölüm içermelidir:

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

Tümcecik parola saklama dosyası
Geçiş tümcecik parola şifreleme dosyası (`Stash.sth`).

Bu dosya, IBM WebSphere MQ için özel bir ikili biçimdir ve `cert.pem` dosyasında tutulan özel anahtara erişirken kullanılmak üzere şifrelenmiş geçiş tümcecisini içerir. Özel anahtarın kendisi `cert.pem` sertifika deposunda saklanır.

Bu dosya, **-s** parametresiyle IBM WebSphere MQ **amqrsslc** komut satırı aracı kullanılarak oluşturulur ya da değiştirilir. Örneğin, `/home/alice` dizininin bir `cert.pem` dosyası içerdiği durumlarda:

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

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

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

İlgili kişisel sertifika deposunun sahibine okuma erişimine izin vermek için dosya izinlerinin bu dosyada ayarlanması gerekir.

Sertifika iptal listesi dosyası
Sertifika iptal listesi dosyası (`crl.pem`).

Bu dosya, müşterinin PEM biçiminde dijital sertifikaları doğrulamak için kullandığı sertifika iptal listelerini (CRL ' ler) içerir. Bu dosyanın varlığı isteğe bağlıdır. Bu dosya yoksa, sertifikaları doğrularken herhangi bir sertifika iptal denetimi gerçekleştirilir.

Dosya izinlerinin bu dosyaya yazma erişimini sınırlamak için ayarlanması gerekir.

Doğru biçimlendirilmiş bir `crl.pem` dosyası, aşağıdaki üstbilgileri ve altbilgileri içeren bir ya da daha fazla bölüm içermelidir:

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

UNIX, Linux, and Windows sistemlerinde SSL ya da TLS ile çalışma

UNIX, Linux ve Windows sistemlerinde, Secure Sockets Layer (SSL) desteği IBM WebSphere MQile kurulur.

Sertifika doğrulama ilkeleriyle ilgili daha ayrıntılı bilgi için Sertifika doğrulama ve güvenilirlik ilkesi tasarımıbaşlıklı konuya bakın.

iKeyman, iKeycmd, runmqakm ve runmqckm komutunu kullanma

On UNIX, Linux and Pencereler systems, manage keys and digital certificates with the iKeyman GUI or from the command line using iKeycmd or runmqakm.

- **UNIX and Linux** sistemleri için:
  - iKeyman GUI 'sini başlatmak için **strmqikm** komutunu kullanın.
  - Use the **runmqckm** command to perform tasks with the iKeycmd command line interface.
  - Runmqakm komut satırı arabirimiyle görevleri gerçekleştirmek için **runmqakm** komutunu kullanın. **runmqakm** için komut sözdizimi, **runmqckm**ile ilgili sözdizimiyle aynıdır.

    SSL 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.

JRE 'nin ürünün önceki sürümlerinde 32 bit olduğu, ancak 64 bit yalnızca IBM WebSphere MQ Version 7.5sürümünde olduğu aşağıdaki platformlarda, **iKeyman** ve **iKeycmd** JRE' nin adresleme kipi için uygun olan ek PKCS#11 sürücülerini kurmanız gerekebilir. Bunun nedeni, PKCS#11 sürücüsünün JRE ile aynı adresleme kipini kullanması gerektiğinden kaynaklanır. Aşağıdaki tabloda, IBM WebSphere MQ Version 7.5 JRE adresleme kipleri gösterilmektedir.

Çizelge 12. IBM WebSphere MQ Version 7.5 JRE adresleme kipleri

Altyapı	**JRE Adresleme Kipi**
Windows (32 bit ya da 64 bit)	32
System x 32 bit içinLinux	32
System x 64 bit içinLinux	64
System p içinLinux	64
System z içinLinux	64
HP-UX	64
Solaris Sparc	64
Solaris x86-64	64
AIX	64

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.

    SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, **runmqckm** ya da **strmqikm** komutları yerine **runmqakm** komutunu kullanın.

UNIX, Linux ya da Windows sistemlerinde SSL izleme isteğinde bulunmaya ilişkin bilgi için bkz. strmqtrc.

İlgili başvurular

runmqckm ve runmqakm komutları

UNIX, Linux, and Windows sistemlerinde anahtar havuzu ayarlama

iKeyman kullanıcı arabirimini kullanarak ya da **iKeycmd** ya da **runmqakm** komutlarını kullanarak bir anahtar havuzu ayarlayabilirsiniz.

Bu görev hakkında

SSL ya da TLS bağlantısı, bağlantının her iki ucunda bir *anahtar havuzu* gerektirir. Her IBM WebSphere MQ kuyruk yöneticisinin ve IBM WebSphere MQ MQI client ' in bir anahtar havuzuna erişimi olması gerekir. Daha fazla bilgi için “SSL ya da TLS anahtarı havuzu” sayfa 23 başlıklı konuya bakın.

UNIX, Linux, and Windows sistemlerinde, sayısal sertifikalar, **iKeyman** kullanıcı arabirimi kullanılarak ya da **iKeycmd** ya da **runmqakm** komutları kullanılarak yönetilen bir anahtar veritabanı dosyasında saklanır.

Bu dijital sertifikaların etiketleri var. Belirli bir etiket, bir kuyruk yöneticisiyle ya da IBM WebSphere MQ MQI clientile kişisel bir sertifikayı ilişkilendirir. SSL ve TLS, kimlik doğrulama amacıyla bu sertifikayı kullanır. UNIX, Linux, and Windows sistemlerinde, IBM WebSphere MQ , diğer ürünlere ilişkin sertifikalarla karışıklığı önlemek için etiket öneki olarak `ibmwebspheremq` ' yi kullanır. Önek, kuyruk yöneticisi ya da IBM WebSphere MQ MQI client kullanıcı oturum açma kimliği adı ve ardından küçük harfe çevrilir. Sertifika etiketinin tamamını küçük harfli olarak belirtmeye dikkat edin.

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 *MQ_INSTALLATION_PATH*`\Qmgrs\`*queue_manager_name*`\ssl`olur; burada *MQ_INSTALLATION_PATH* , IBM WebSphere MQ ' nin kurulu olduğu dizindir. Örneğin, `C:\program files\IBM\WebSphere 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 WebSphere 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 dosyası adının denetlenmesine ve belirtilmesine ilişkin bilgi için bkz. “UNIX, Linux ya da Windows sistemlerindeki bir kuyruk yöneticisine ilişkin anahtar havuzu yerinin değiştirilmesi” sayfa 117 . Anahtar veri tabanı kütüğünü yaratmadan önce ya da sonra, anahtar veri tabanı dosyası adını belirtebilirsiniz.

iKeyman ya da **iKeycmd** 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, **iKeyman** ya da **iKeycmd** çalıştırdığınız kullanıcı kimliğinin mqm grubunun bir üyesi olması gerekir. For a IBM WebSphere MQ MQI client, if you run **iKeyman** or **iKeycmd** from a user ID different from that under which the client runs, you must alter the file permissions to enable the IBM WebSphere MQ MQI client to access the key database file at run time. Daha fazla bilgi için bkz. “ Pencerelerüzerindeki anahtar veri tabanı dosyalarınıza erişilmesi ve güvenceye alınması” sayfa 115 ya da “UNIX and Linux sistemlerindeki anahtar veritabanı dosyalarınızın erişilmesi ve güvenliğini sağlama” sayfa 115.

iKeyman ya da **iKeycmd** sürümünde 7.0sürümünde, yeni anahtar veritabanları otomatik olarak önceden tanımlanmış bir sertifika yetkilisi (CA) sertifikasına sahip olur. **iKeyman** ya da **iKeycmd** sürümünde 8.0sürümünde, anahtar veritabanı dosyanızın yalnızca istediğiniz sertifika kuruluşu (CA) sertifikalarını içerdiğiniz için, anahtar veritabanları otomatik olarak doldurulmaz, çünkü ilk kurulumu daha güvenli hale getirilir.

Not: CA sertifikalarıyla sonuçlanan GSKit sürüm 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. “GSKit sürüm 8.0içeren UNIX, Linux, and Windows sistemlerinde varsayılan CA sertifikalarının boş bir anahtar havuzuna eklenmesi” sayfa 116.

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:

   - UNIX, Linux, and Windows sistemlerinde:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - runmqakm komutunu kullanarak:

     ```
     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 WebSphere MQiçin, `cms`olmalıdır.)

   -stash
   Anahtar veritabanı parolasını bir dosyaya kaydeder.

   -fips.
   BSafe şifreleme kitaplığı kullanımını devre dışı bırakır. Yalnızca 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, **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, 0x20 - 0x7Earalığında, standart ASCII yazdırılabilir karakter takımında 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 iKeyman 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:\Program Files\IBM\WebSphere MQ\qmgrs\QM1\ssl` (Windows sistemlerinde).

  Yol, kuyruk yöneticisinin **SSLKeyRepository** özniteliğinin değeriyle eşleşmelidir.
- Bir IBM WebSphere MQ istemcisi için: `/var/mqm/ssl` (UNIX and Linux sistemlerinde) ya da `C:\mqm\ssl` (Windows sistemlerinde).

8. **Aç**'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 alamayacakları için, SSL ya da TLS kanallarını başlatma girişimleri başarısız olur.
11. **Tamam**'ı tıklatın.

    Kişisel Sertifikalar penceresi açılır.
12. Set the access permissions as described in “ Pencerelerüzerindeki anahtar veri tabanı dosyalarınıza erişilmesi ve güvenceye alınması” sayfa 115 or “UNIX and Linux sistemlerindeki anahtar veritabanı dosyalarınızın erişilmesi ve güvenliğini sağlama” sayfa 115.

Pencerelerüzerindeki 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.

UNIX and Linux sistemlerindeki anahtar veritabanı dosyalarınızın erişilmesi ve güvenliğini sağlama
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.

GSKit sürüm 8.0içeren UNIX, Linux, and Windows sistemlerinde varsayılan CA sertifikalarının boş bir anahtar havuzuna eklenmesi
GSKit sürüm 8 ile boş bir anahtar havuzuna varsayılan CA sertifikalarından birini ya da birkaçını eklemek için bu yordamı izleyin.

GSKit sürüm 7.0' da, yeni bir anahtar havuzu oluştururken davranış, genel olarak kullanılan Sertifika Yetkilileri için varsayılan CA sertifikalarının bir kümesini otomatik olarak eklemekten geçmektedir. 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.

iKeyman' ın Kullanılması

CA sertifikasını eklemek istediğiniz makine üzerinde aşağıdaki adımları gerçekleştirin:

1. **strmqikm** komutunu (UNIX, Linux ve Windows sistemlerinde) kullanarak iKeyman GUI 'sini başlatın.
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 iKeycmdkullanarak 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 WebSphere 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.

UNIX, Linux, and Windows sistemlerindeki 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 WebSphere 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 sistemlerinde: `/var/mqm/qmgrs/QM1/ssl/key`; burada `/var/mqm/qmgrs/QM1/ssl` yolu ve `key` kök adıdır.

   b. Windows' ta: *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl\key`; burada *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl` yol, `key` kök adıdır. *MQ_INSTALLATION_PATH* WebSphere MQ ' un kurulu olduğu üst düzey dizini temsil eder.

UNIX, Linux ya da Windows sistemlerindeki 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 Linux sistemlerinde:

```
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 sistemlerinde:

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\Mykey')
```

Anahtar veritabanı dosyası tam olarak nitelenmiş dosya adına sahip: `C:\Program Files\IBM\WebSphere 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.

You can also alter your queue manager's attributes using the WebSphere MQ Explorer or PCF commands.

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 Windows sistemlerindeki bir anahtar havuzuna aktarılması” sayfa 130.

UNIX, Linux, and Windows sistemlerinde bir IBM WebSphere MQ MQI istemcisi için anahtar havuzunun bulunması

Anahtar havuzunun yeri MQSSLKEYR değişkeniyle verilir ya da MQCONNX çağrısında belirtilir.

IBM WebSphere MQ MQI istemcisinin anahtar veritabanı kütüğünüzün yerini almak için MQSSLKEYR ortam değişkenini inceleyin. Örneğin:

```
echo $MQSSLKEYR
```

Ayrıca, anahtar veritabanı dosyası adının bir MQCONNX çağrısında da (“UNIX, Linux, and Windows sistemlerinde bir IBM WebSphere MQ MQI istemcisi için anahtar havuzu yerini belirtme” sayfa 118) açıklandığı şekilde ayarlanabileceği için uygulamanızı da denetleyin. Bir MQCONNX çağrısındaki değer kümesi, MQSSLKEYR değerini geçersiz kılar.

UNIX, Linux, and Windows sistemlerinde bir IBM WebSphere MQ MQI istemcisi için anahtar havuzu yerini belirtme

Bir IBM WebSphere MQ MQI istemcisi için varsayılan anahtar havuzu yoktur. Konumunu iki şekilde belirtebilirsiniz. Diğer sistemlere yetkisiz kopyalamayı önlemek için anahtar veritabanı dosyasına yalnızca amaçlanan kullanıcılar ya da denetimciler tarafından erişilebildiğinden emin olun.

IBM WebSphere MQ MQI istemcisinin anahtar veri tabanı dosyasının yerini aşağıdaki iki yoldan belirleyebilirsiniz:

- MQSSLKEYR ortam değişkeni ayarlanıyor. Örneğin, UNIX and Linux sistemlerinde:

  ```
  export MQSSLKEYR=/var/mqm/ssl/key
  ```

  Anahtar veri tabanı dosyası, tam olarak nitelenmiş dosya adını içerir:

  ```
  /var/mqm/ssl/key.kdb
  ```

  Windows sistemlerinde:

  ```
  set MQSSLKEYR=C:\Program Files\IBM\WebSphere MQ\ssl\key
  ```

  Anahtar veri tabanı dosyası, tam olarak nitelenmiş dosya adını içerir:

  ```
  C:\Program Files\IBM\WebSphere 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 MQSCO başlıklı konuya bakın.

Sertifikalar üzerindeki değişiklikler ya da sertifika deposu UNIX, Linux ya da Windows sistemlerinde 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 ilk olarak bir SSL kanalı çalıştırdığında.
- Yeni bir gelen TCP/IP tek kanal işlemi, önce bir SSL kanalı başlatmak için bir istek alır.
- MQSC komutu REFRESH SECURITY TYPE (SSL) komutu, Websphere MQ SSL ortamını yenilemek için verilir.
- İstemci uygulaması işlemleri için, süreçteki son SSL bağlantısı kapatılır. Sonraki SSL 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 bir SSL kanalı çalıştırılır. Süreç

havuzlama işlemi önceden bir SSL kanalı çalıştırdıysa 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 SSL kanalı çalıştırılır. Kanal başlatıcı işlemi önceden bir SSL kanalı 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 önce bir SSL kanalı başlatmak için bir istek alır. Dinleyici zaten bir SSL kanalı çalıştırdıysa ve değişikliğin hemen yürürlüğe girmesini istiyorsanız, MQSC komutunu REFRESH SECURITY TYPE (SSL) komutunu çalıştırın.

Ayrıca, IBM WebSphere MQ Explorer ya da PCF komutlarını kullanarak WebSphere MQ SSL ortamını da yenileyebilirsiniz.

UNIX, Linux, and Windows sistemlerinde kendinden onaylı bir kişisel sertifika oluşturma

iKeyman, iKeycmdya da runmqakm komutunu kullanarak kendinden onaylı bir sertifika yaratabilirsiniz.

Not: IBM WebSphere 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.

Kendinden onaylı sertifikaları neden kullanmak isteyebileceğiyle ilgili daha fazla bilgi için bkz. “İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için kendinden onaylı sertifikaların kullanılması” sayfa 200.

Tüm dijital sertifikalar tüm CipherSpecsile kullanılamaz. Kullanmanız gereken CipherSpecs ile uyumlu bir sertifika oluşturduğunuzdan emin olun. WebSphere MQ supports three different types of CipherSpec. Ayrıntılar için “Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33 başlıklı konudaki “Eliptik Eğri ve RSA CipherSpecsile birlikte çalışabilirlik” sayfa 35 başlıklı konuya bakın. 1 numaralı CipherSpecs (adları ECDHE_ECDSA_) kullanmak için, sertifikayı oluşturmak için **runmqakm** komutunu kullanmanız ve bir Eliptik Eğrisi ECDSA imza algoritması parametresi belirtmeniz gerekir; örneğin, **-sig_alg** EC_ecdsa_with_SHA384 .

iKeyman' ın Kullanılması

iKeyman FIPS uyumlu bir seçenek sunmaz. SSL ya da TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Kuyruk yöneticiniz ya da WebSphere MQ MQI istemcisi için kendinden onaylı bir sertifika edinmek için aşağıdaki yordamı kullanın:

1. **strmqikm** komutunu kullanarak iKeyman GUI 'sini 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 kaydetmek 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. **Yarat** menüsünden, **Kendinden onaylı yeni sertifika**öğesini tıklatın. Yeni Kendinden Onaylı Sertifika Yarat penceresi görüntülenir.
9. **Key Label** (Anahtar Etiketi) alanına şunu yazın:

- Kuyruk yöneticisi için `ibmwebspheremq` , ardından kuyruk yöneticinizin adı küçük harfe katlandı. Örneğin, `QM1`, `ibmwebspheremqqm1`ya da,
- Bir WebSphere MQ istemcisi için, `ibmwebspheremq` oturum açma kullanıcı kimliğiniz küçük harfe (örneğin, `ibmwebspheremqmyuserid`) katlandı.

10. **Distinguished name**' daki herhangi bir alan ya da **Subject alternative name** alanlarından herhangi biri için bir değer yazın ya da bir değer 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.

Komut satırını kullanma

iKeycmd ya da runmqakm komutunu kullanarak kendinden onaylı bir kişisel sertifika yaratmak için aşağıdaki komutları kullanın:

- UNIX, Linux ve Windows sistemlerinde iKeycmd komutunu kullanma:

```
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_dsname` *DNS_names* , `-san_emailaddr` *email_addresses* ya da `-san_ipaddr` *IP_addresses* ' yi kullanabilirsiniz.

- runmqakm komutunu kullanarak:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days

        -fips -sig_alg algorithm
```

`-db` *filename*	Bir CMS anahtar veri tabanının tam olarak nitelenmiş dosya adı.
`-pw` *password*	CMS anahtar veri tabanına ilişkin parola.
`-label` *label*	Sertifikaya eklenen anahtar etiketi.
`-dn` *distinguished_name*	Çift tırnak işareti içine alınmış X.500 ayırt edici adı. En az bir öznitelik gerekli. Birden çok OU ya da DC özniteliği sağlayabilirsiniz.
`-size` *key_size*	Anahtar boyutu. iKeycmdiçin değer 512 ya da 1024 olabilir. Runmqakm için değer 512, 1024, 2048 ya da 4096 olabilir.
`-x509version` *version*	Yaratılacak X.509 sertifikasının sürümü. Değer 1, 2 ya da 3 olabilir. Varsayılan 3'tür.
`-expire` *days*	Sertifikana ilişkin geçerlilik süresi (gün olarak) Varsayılan değer, sertifika için 365 gündür.
`-fips`	Komutun FIPS kipinde çalıştırıldığını belirtir. Bu kip, BSafe şifreleme kitaplığı kullanımını devre dışı bırakır. Yalnızca 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, **runmqakm** komutu başarısız olur.

`-sig_alg`	Runmqakm için, kendinden onaylı bir sertifika yaratma sırasında kullanılan karma algoritma. Bu hash algoritması, yeni yaratılan kendinden onaylı sertifikayla ilişkilendirilmiş imzayı yaratmak için kullanılır. Değer, `md5`, `MD5_WITH_RSA`, `MD5WithRSA`, `SHA_WITH_DSA` , `SHA_WITH_RSA`, `sha1`, `SHA1WithDSA` olabilir. `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` ya da `EC_ecdsa_with_SHA512`. Varsayılan değer `SHA1WithRSA`' dır.
`-sig_alg`	iKeycmdiçin, girişin anahtar çiftinin yaratılması için kullanılan asimetrik imza algoritması kullanılır. Bu değer, `MD2_WITH_RSA`, `MD2WithRSA`, `MD5_WITH_RSA` , `MD5WithRSA`, `SHA1WithDSA`, `SHA1WithRSA`, `SHA256_WITH_RSA`, `SHA256WithRSA` olabilir, `SHA2WithRSA`, `SHA384_WITH_RSA`, `SHA384WithRSA`, `SHA512_WITH_RSA`, `SHA512WithRSA`, `SHA_WITH_DSA`, `SHA_WITH_RSA` , `SHAWithDSA`ya da `SHAWithRSA`. Varsayılan değer `SHA1WithRSA`' dır.
`-san_dnsname` *`DNS_names`*	Yaratılmakta olan girişle ilgili DNS adlarının virgülle ya da boşlukla ayrılmış bir listesi.
`-san_emailaddr` *`email_addresses`*	Yaratılmakta olan girdiye ilişkin e-posta adreslerinin virgülle ya da boşlukla ayrılmış bir listedir.
`-san_ipaddr` *`IP_addresses`*	Yaratılmakta olan girişe ilişkin IP adreslerinin virgülle ya da boşlukla ayrılmış bir listesi.

distributed *UNIX, Linux, and Windows sistemleri üzerinde kişisel sertifika isteme*

You can request a personal certificate by using the **strmqikm** (iKeyman) GUI, or from the command line using the **runmqckm** or **runmqakm** commands. SSL ya da TLS sertifikalarını FIPS-uyumlu bir şekilde yönetmeniz gerekiyorsa **runmqakm** komutunu kullanın.

Bu görev hakkında

Kişisel bir sertifikayı iKeyman grafik kullanıcı arabirimini kullanarak ya da komut satırından aşağıdaki noktalara dikkat ederek isteyebilirsiniz:

- WebSphere 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.
- Tüm dijital sertifikalar tüm CipherSpecsile kullanılamaz. Kullanmanız gereken CipherSpecs ile uyumlu bir sertifika istediğinizden emin olun. WebSphere MQ supports three different types of CipherSpec. Ayrıntılar için “Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33 başlıklı konudaki “Eliptik Eğri ve RSA CipherSpecsile birlikte çalışabilirlik” sayfa 35 başlıklı konuya bakın.
- 1 numaralı CipherSpecs Tip 1 'i (adları `ECDHE_ECDSA_` başında) 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`.
- Yalnızca runmqakm komutu FIPS uyumlu bir seçenek sağlar.
- Şifreleme donanımı kullanıyorsanız, bkz. “PKCS #11 donanımınıza ilişkin kişisel bir sertifika istenmesi” sayfa 137.

iKeyman kullanıcı arabiriminin kullanılması

Bu görev hakkında

iKeyman FIPS uyumlu bir seçenek sunmaz. SSL ya da 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 iKeyman 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) alanında aşağıdaki etiketleri girin:
   - Kuyruk yöneticisi için, kuyruk yöneticinizin adını izleyen `ibmwebspheremq` yazın küçük harfe çevrilecek. For example, for a queue manager called `QM1`, enter `ibmwebspheremqqm1`.
   - IBM WebSphere MQ MQI clientiçin, oturum açma kullanıcı kimliğinizin ardından `ibmwebspheremq` girin; tümü küçük harfli olarak; örneğin, `ibmwebspheremqmyuserid` .
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 122adımında seçtiğiniz dosyada saklanır.
14. 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:

- **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 kullanarak:

```
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.

-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.

-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. Bu kip, BSafe şifreleme kitaplığı kullanımını devre dışı bırakır. Yalnızca 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, **runmqakm** komutu başarısız olur.

-sig_alg
runmqckmiçin, girişin anahtar çiftinin oluşturulması için kullanılan asimetrik imza algoritmasını belirtir. Değer, 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, SHAWithDSAya da SHAWithRSA . Varsayılan değer SHA1WithRSAdeğeridir.

-sig_alg
runmqakmiçin, bir sertifika isteğinin oluşturulması sırasında kullanılan HASH algoritmasını belirtir. Bu hash algoritması, yeni yaratılan sertifika isteğiyle ilişkilendirilmiş imzayı yaratmak için kullanılır. Değer, md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA , SHA_WITH_RSA, sha1, SHA1WithDSA olabilir. 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 ya da 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.

UNIX, Linux, and Windows sistemlerinde var olan bir kişisel sertifikana ilişkin yenileme

iKeyman kullanıcı arabirimini kullanarak ya da **iKeycmd** ya da **runmqakm** komutlarını kullanarak kişisel bir sertifikayı yenileyebilirsiniz.

Başlamadan önce

Kişisel sertifikalarınız için daha büyük anahtar boyutları kullanma zorunluluğunuz varsa, yeniden yaratılan sertifika isteği var olan bir anahtardan üretildiğinden, aşağıda açıklanan yenileme adımları işe yaramaz.

Gereksinim duyduğunuz anahtar boyutlarını kullanarak yeni bir sertifika isteği oluşturmak için "UNIX, Linux, and Windows sistemleri üzerinde kişisel sertifika isteme" sayfa 121 içinde açıklanan adımları izleyin. Bu işlem, varolan anahtarınızın yerini alır.

Bu görev hakkında

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.

iKeyman kullanıcı arabiriminin kullanılması

Bu görev hakkında

iKeyman FIPS uyumlu bir seçenek sunmaz. SSL ya da 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. UNIX, Linux, and Windows sistemlerinde **strmqikm** komutunu kullanarak iKeyman 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 Yarat ...**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 124adımında seçtiğiniz dosyada saklanır.
12. Yeni kişisel sertifikayı, dosyayı sertifika yetkilisine (CA) göndererek ya da dosyayı CA için web sitesindeki istek formuna kopyalayarak isteyin.

Yordam

Use the following commands to request a personal certificate by using either the **iKeycmd** or **runmqakm** command:

- UNIX, Linux, and Windows sistemlerinde **iKeycmd** komutunu kullanma:

```
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 ve Windows sistemlerindeki bir anahtar havuzuna alınması” sayfa 125içinde açıklanan adımları kullanarak bunu anahtar veritabanınıza ekleyebilirsiniz.

Kişisel sertifikaların UNIX, Linux ve Windows sistemlerindeki 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.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

İçe aktarılacak sertifika dosyasının yürürlükteki kullanıcı için yazma iznine sahip olduğundan emin olun ve bir kuyruk yöneticisi ya da bir WebSphere MQ MQI istemcisi için anahtar veritabanı dosyasına kişisel sertifika almak için aşağıdaki yordamı kullanın:

1. **strmqikm** komutunu (Windows UNIX and Linux üzerinde) kullanarak iKeyman GUI 'sini başlatın.
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

iKeycmd kullanarak bir anahtar veritabanı dosyasına kişisel sertifika eklemek için aşağıdaki komutları kullanın:

- UNIX, Linux ve Windows' ta aşağıdaki komutu verin:

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

Burada:

`-file filename`	kişisel sertifikayı içeren dosyanın tam olarak nitelenmiş dosya adıdır.
`-db filename`	CMS anahtar veri tabanının tam olarak nitelenmiş dosya adıdır.
`-pw password`	CMS anahtar veri tabanının parolasıdır.
`-format ascii`	sertifikının biçimidir. The value can be `ascii` for Base64-encoded ASCII or `binary` for Binary DER data. Varsayılan değer `ascii` ' dir.

Şifreleme donanımı kullanıyorsanız, bkz. “Kişisel sertifikanızı PKCS #11 donanımınıza alma” sayfa 139.

Anahtar havuzundan bir CA sertifikasının çekilmesi

CA sertifikasını almak için bu yordamı izleyin.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

CA sertifikasını almak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. **`strmqikm`** komutunu kullanarak iKeyman GUI 'sini başlatın.
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

Use the following commands to extract a CA certificate using iKeycmd :

- UNIX, Linux ve 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.

UNIX, Linux ve Windows sistemlerindeki bir anahtar havuzundan, kendinden onaylı sertifikana ilişkin genel parçanın çekilmesi

Kendinden onaylı sertifikana ilişkin genel bölümü çıkarmak için bu yordamı izleyin.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

Kendinden imzalı bir sertifikana ilişkin genel kısmını çıkarmak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. **`strmqikm`** komutunu (UNIX, Linux ve Windowsüzerinde) kullanarak iKeyman GUI 'sini başlatın.
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. **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 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 iKeycmd or runmqakm:

- UNIX, Linux ve 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.

UNIX, Linux, and Windows sistemlerinde CA sertifikası (ya da kendinden onaylı bir sertifikenin genel bölümü) bir anahtar havuzuna eklenmesi

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: Eklemek istediğiniz sertifika bir sertifika zincirinde varsa, zincirin üstünde olan tüm sertifikaları da eklemeniz gerekir. Sertifikenin ASCII (UTF-8) ya da ikili (DER) kodlamalarında olduğundan emin olmalısınız; çünkü IBM Global Secure Toolkit (GSKit), diğer kodlama türleriyle sertifikaları desteklemiyor. Sertifikaları, kökten başlayarak kesinlikle alçalan düzende eklemeniz gerekir, ardından da zincirin hemen altındaki CA sertifikasına sahip olun.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

CA sertifikasını eklemek istediğiniz makine üzerinde aşağıdaki adımları gerçekleştirin:

1. **strmqikm** komutunu (UNIX, Linux ve Windows sistemlerinde) kullanarak iKeyman GUI 'sini başlatın.
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. **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

iKeycmd komutunu kullanarak bir CA sertifikası eklemek için aşağıdaki komutları kullanın:

- UNIX, Linux ve Windows' ta aşağıdaki komutu verin:

```
runmqckm -cert -add -db filename -pw password -label label -file 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.
`-file filename`	Sertifikayı içeren dosyanın adı.
`-format ascii`	sertifikının biçimidir. The value can be `ascii` for Base64-encoded ASCII or `binary` for Binary DER data. Varsayılan değer `ascii`' dir.

Kişisel bir sertifikenin anahtar havuzundan dışa aktarılması

Kişisel bir sertifikayı dışa aktarmak için bu yordamı izleyin.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

Kişisel sertifikayı dışa aktarmak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. **strmqikm** komutunu (Windows UNIX and Linux üzerinde) kullanarak iKeyman GUI 'sini başlatın.
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

iKeycmdkomutunu kullanarak kişisel bir sertifikayı dışa aktarmak için aşağıdaki komutları kullanın:

- UNIX, Linux ve 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.
`-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.

Kişisel bir sertifikin UNIX, Linux, and Windows sistemlerindeki 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. “UNIX, Linux, and Windows sistemlerinde CA sertifikası (ya da kendinden onaylı bir sertifikenin genel bölümü) bir anahtar havuzuna eklenmesi” sayfa 128) geçerli olan CA sertifikalarının tam geçerli zincirini eklemelisiniz.

PKCS #12 dosyaları, kullanıldıktan sonra geçici olarak dikkate alınmalı ve silinmelidir.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS-uyumlu bir biçimde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

Kişisel sertifikayı içe aktarmak istediğiniz makinede aşağıdaki adımları gerçekleştirin:

1. **strmqikm** komutunu kullanarak iKeyman GUI 'sini 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. Bu pencere, örneğin, hedef anahtar veritabanında aynı etikete sahip bir sertifika varsa, içe aktarılmakta olan sertifikaların etiketlerinin değiştirilmesine olanak sağlar. Sertifika etiketlerinin değiştirilmesi, sertifika zinciri doğrulaması üzerinde bir etki göstermez. Bu, sertifikayı belirli bir kuyruk yöneticisi ya da istemciyle (örneğin,`ibmwebspheremqqm1`) ilişkilendirmek için kişisel sertifika etiketini WebSphere MQ tarafından gerekli olan kişisel sertifika etiketini değiştirmek için kullanılabilir.
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, doğru etiketlenmiş sertifikalarla güncellenen **Kişisel Sertifikalar** ve **İmzalayıcı sertifikaları** alanlarıyla yeniden görüntülenir.
19. Sertifika, hedef anahtar veritabanına içe aktarılır.

Komut satırını kullanma

Kişisel bir sertifikayı iKeycmdkullanarak içe aktarmak için aşağıdaki komutları kullanın:

- UNIX, Linux ve 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.

iKeycmd , sertifika etiketlerini doğrudan değiştirmek için bir komut sağlamaz. 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.

Microsoft .pfx dosyasından içe aktarma

Bu yordamı, iKeymankullanarak bir Microsoft .pfx dosyasından mport 'a düşürün. Bir .pfx dosyasını içe aktarmak için runmqakm olanağını kullanamazsınız.

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 (Linux, UNIX ya da Windowsüzerinde) kullanarak iKeyman GUI 'sini 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. Kullanımı kolay ad, `ibmwebspheremq`biçiminde olmalı ve kuyruk yöneticisi adı ya da WebSphere MQ MQI istemcisi kullanıcı oturum açma kimliği küçük harfli olmalıdır.
21. **Tamam** düğmesini tıklatın. Etiketleri Değiştir penceresi kaldırılır ve özgün IBM Anahtar Yönetimi penceresi, Kişisel Sertifikalar ve İmzalayıcı Sertifikaları panoları ile birlikte güncellenen kişisel sertifikalarla birlikte yeniden görüntülenir.
22. pfx kişisel sertifikası artık (hedef) veritabanına içe aktarılmaktadır.

Bir sertifika etiketinin iKeycmd kullanılarak değiştirilmesi mümkün değildir.

Bir PKCS #7 kütüğünden içe aktarma

iKeyman ve iKeycmd araçları, PKCS #7 (.p7b) dosyalarını desteklemez. Bir PKCS #7 kütüğünden sertifikaları içe aktarmak için runmqckm aracını kullanın.

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.

Deleting a certificate from a key repository on UNIX, Linux, and Windows systems

Kişisel ya da CA sertifikalarını kaldırmak için bu yordamı kullanın.

iKeyman' ın Kullanılması

SSL sertifikalarını FIPS ile uyumlu bir şekilde yönetmeniz gerekiyorsa, runmqakm komutunu kullanın. iKeyman FIPS uyumlu bir seçenek sunmaz.

1. **strmqikm** komutunu (UNIX, Linux ve Windows sistemlerinde) kullanarak iKeyman GUI 'sini başlatın.
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 sertifikenin anahtar havuzundan dışa aktarılması” sayfa 129).
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

iKeycmd ya da runmqakm komutunu kullanarak bir sertifikayı silmek için aşağıdaki komutları kullanın:

- UNIX, Linux ve 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. Bu kip, BSafe şifreleme kitaplığı kullanımını devre dışı bırakır. Yalnızca 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, **runmqakm** komutu başarısız olur.

Anahtar havuzu koruması için güçlü parolalar oluşturma

You can generate strong passwords for key repository protection using the **runmqakm** command.

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:

```
!   \   "    '
```

runmqckm, **runmqakm** ya da iKeyman GUI 'sindeki bir bilgi istemine yanıt olarak parola girerken, parolayı tırnak içine almak ya da bu parolayı almak gerekli değildir. İşletim sistemi kabuğu bu vakalardaki veri girişini etkilmediği için bu gerekli değildir.

UNIX, Linux, and Windows sistemlerinde şifreleme donanımı için yapılandırma

Bir kuyruk yöneticisine ya da istemciye ilişkin şifreleme donanımını bir dizi şekilde yapılandırabilirsiniz.

You can configure cryptographic hardware for a queue manager on UNIX, Linux or Pencereler systems using either of the following methods:

- 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 WebSphere MQ Explorer 'ı kullanın. Ek bilgi için çevrimiçi yardıma bakın.

Aşağıdaki yöntemlerden birini kullanarak UNIX, Linux ya da Windows sistemlerinde bir WebSphere MQ istemcisi için şifreleme donanımını yapılandırabilirsiniz:

- MQSSLCRYP ortam değişkenini ayarlayın. MQSSLCRYP için izin verilen değerler, ALTER QMGRiçinde açıklandığı gibi, SSLCRYP parametresiyle aynı olur. SSLCRYP parametresinin GSK_PCS11 sürümünü kullanıyorsanız, PKCS #11 belirteci etiketi tamamen küçük harfle belirtilmelidir.
- 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 135içinde 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 WebSphere 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:

- UNIX, Linux, and Windows sistemlerinde:

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- runmqakm komutunu kullanarak:

```
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 WebSphere MQiçin, `cms`olmalıdır.)

-stash
Anahtar veritabanı parolasını bir dosyaya kaydeder.

-fips.
BSafe şifreleme kitaplığı kullanımını devre dışı bırakır. Yalnızca 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, **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, 0x20 - 0x7Earalığında, standart ASCII yazdırılabilir karakter takımında 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 iKeyman kullanıcı arabirimini başlatın.
4. **Anahtar Veritabanı Dosyası** > **Aç**öğelerini tıklatın.
5. **Anahtar veritabanı tipi** öğesini tıklatın ve **PKCS11Direct**öğesini seçin.
6. **File Name** (Dosya Adı) alanına, şifreleme donanımınızı yönetmek için modülün adını yazın; örneğin, `PKCS11_API.so`.

   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.
7. **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.

8. **Cryptographic Token Password** (Şifreleme Aygıtı Parolası) alanında, şifreleme donanımını yapılandırdığınızda ayarladığınız parolayı yazın.
9. 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 “13” sayfa 137adımından 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.
10. **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.
11. **Konum** alanına yolu yazın, örneğin:

    - Kuyruk yöneticisi için: `/var/mqm/qmgrs/QM1/ssl`
    - Bir IBM WebSphere MQ MQI istemcisi için: `/var/mqm/ssl`

    Tamam'ı tıklatın. Parola İstemi penceresi açılır.
12. Bir parola girin.

    “9” sayfa 137adımında **Var olan ikincil anahtar veritabanı dosyasını aç** seçeneğini belirlediyseniz, **Parola** alanına bir parola yazın.

    “9” sayfa 137adımında **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 alamayacakları için SSL kanallarını başlatma girişimleri başarısız olur.

    c) **Tamam**'ı tıklatın. Parolanın `key.sth` dosyasında olduğunu onaylayan bir pencere açılır (farklı bir kök adı belirtmediyseniz).
13. **Tamam**'ı tıklatın. Key veritabanı içerik çerçevesi görüntülenir.

PKCS #11 donanımınıza ilişkin kişisel bir sertifika istenmesi
Şifreleme donanımınıza ilişkin kişisel bir sertifika istemek için kuyruk yöneticisi ya da bir IBM WebSphere MQ MQI istemcisi için bu yordamı kullanın.

iKeyman kullanıcı arabiriminin kullanılması

Bu görev hakkında

Not: WebSphere 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

iKeyman kullanıcı arabiriminden kişisel bir sertifika istemek için aşağıdaki adımları tamamlayın:

1. Şifreleme donanımınızla çalışmaya ilişkin adımları tamamlayın. Bkz. “PKCS #11 donanımlarındaki sertifikaları yönetme” sayfa 135.
2. **Yarat** menüsünden **Yeni Sertifika İsteği**öğesini tıklatın.

   Yeni Anahtar Yarat ve Sertifika İsteği Oluştur penceresi açılır.
3. **Key Label** (Anahtar Etiketi) alanında aşağıdaki etiketleri girin:

- Kuyruk yöneticisi için, kuyruk yöneticinizin adını izleyen `ibmwebspheremq` yazın küçük harfe çevrilecek. For example, for a queue manager called `QM1`, enter `ibmwebspheremqqm1`.
- IBM WebSphere MQ MQI clientiçin, oturum açma kullanıcı kimliğinizin ardından `ibmwebspheremq` girin; tümü küçük harfli olarak; örneğin, `ibmwebspheremqmyuserid` .

4. **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.
5. **Sertifika isteği saklanacak bir dosyanın adını girin** alanında, varsayılan `certreq.arm`değerini kabul edin ya da tam yolu olan yeni bir değer yazın.
6. **Tamam**'ı tıklatın.

   Bir doğrulama penceresi açılır.
7. **Tamam**'ı tıklatın.

   Kişisel Sertifika İstekleri listesinde, yarattığınız yeni kişisel sertifika isteğinin etiketi gösterilir. Sertifika isteği, “5” sayfa 138adımında seçtiğiniz dosyada saklanır.
8. 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:

- **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 kullanarak:

```
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.

-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.

-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. Bu kip, BSafe şifreleme kitaplığı kullanımını devre dışı bırakır. Yalnızca 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, **runmqakm** komutu başarısız olur.

-sig_alg
runmqckmiçin, girişin anahtar çiftinin oluşturulması için kullanılan asimetrik imza algoritmasını belirtir. Değer, 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, SHAWithDSAya da SHAWithRSA . Varsayılan değer SHA1WithRSAdeğeridir.

-sig_alg
runmqakmiçin, bir sertifika isteğinin oluşturulması sırasında kullanılan HASH algoritmasını belirtir. Bu hash algoritması, yeni yaratılan sertifika isteğiyle ilişkilendirilmiş imzayı yaratmak için kullanılır. Değer, md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA , SHA_WITH_RSA, sha1, SHA1WithDSA olabilir. 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 ya da 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.

Kişisel sertifikanızı PKCS #11 donanımınıza alma
Şifreleme donanımınıza kişisel bir sertifika almak için kuyruk yöneticisi ya da IBM WebSphere MQ MQI istemcisi için bu yordamı kullanın.

iKeyman' ın Kullanılması

Yordam

iKeyman kullanıcı arabiriminden kişisel bir sertifika istemek için aşağıdaki adımları tamamlayın:

1. Şifreleme donanımınızla çalışmaya ilişkin adımları tamamlayın. Bkz. “PKCS #11 donanımlarındaki sertifikaları yönetme” sayfa 135.
2. **Al**düğmesini tıklatın. Bir Dosya penceresindeki Sertifika Al penceresi açılır.
3. Yeni kişisel sertifikana ilişkin **Veri tipi** ' yi seçin; örneğin, .arm uzantılı bir dosya için Base64-encoded ASCII data .
4. Yeni kişisel sertifikana ilişkin sertifika dosyası adını ve yerini yazın ya da adı ve yeri seçmek için **Göz At** düğmesini tıklatın.
5. **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.
6. **Evet** ya da **Hayır**' ı tıklatın. Bir Etiket Girin penceresi açılır.
7. Bir etiket yazın.

Örneğin, kişisel sertifikayı istediğinizde olduğu gibi aynı etiketi kullanabilirsiniz. Etiketin doğru IBM WebSphere MQ biçiminde olması gerektiğini unutmayın:

- Kuyruk yöneticisi için `ibmwebspheremq` , ardından kuyruk yöneticinizin adını küçük harfli olarak takip eder. Örneğin, QM1adlı bir kuyruk yöneticisi için etiket şöyle olurdu: `ibmwebspheremqqm1`.
- Bir IBM WebSphere MQ MQI istemcisi için, `ibmwebspheremq` oturum açma kullanıcı kimliğinizi küçük harfli olarak izlemektedir. Örneğin, `MyUserID`kullanıcı kimliği için etiket şöyle olurdu: `ibmwebspheremqmyuserid`.

8. **Tamam**'ı tıklatın. **Kişisel Sertifikalar** listesi, eklediğiniz yeni kişisel sertifikana ilişkin etiketi gösterir. Bu etiket, belirttiğiniz etiketten önce şifreleme belirteci etiketi eklenerek oluşturulur.

Komut satırını kullanma

Yordam

Bir komut satırından kişisel sertifika istemek için aşağıdaki adımları tamamlayın:

1. Ortamınız için yapılandırılmış bir komut penceresi açın.
2. İşletim sisteminiz ve yapılanışınız için uygun komutu girin:

- Windows, UNIX and Linux sistemlerinde aşağıdaki komutlardan birini kullanın:

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

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

Burada:

-file *kütükadı*
Kişisel sertifikayı içeren dosyanın tam olarak nitelenmiş dosya adını belirtir.

-crypto *yol*
Donanımla birlikte sağlanan PKCS #11 kitaplığının tam olarak nitelenmiş yolunu belirtir.

-tokenlabel *hardware_belirteci*
Kuruluş sırasında şifreleme donanımın depolama bölümüne verilen etiketi belirtir.

-pw *parola_parolası*
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. Bu kip, BSafe şifreleme kitaplığının kullanımını devre dışı bırakır. Yalnızca 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, **runmqakm** komutu başarısız olur.

Kullanıcıların tanımlanması ve kimlik doğrulaması

MQCSP yapısını ya da birkaç tip kullanıcı çıkışı programını kullanarak kullanıcıların kimliklerini belirleyebilir ve kimliklerini doğrulayabilirsiniz.

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.

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 WebSphere MQ istemci uygulamasının kullanıcısı adına hareket eder. Bu durumda, karşılıklı kimlik doğrulaması aslında iki kuyruk yöneticisi arasında ya da bir kuyruk yöneticisi ile bir WebSphere MQ MQI istemcisi 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. “SSPI kanal çıkış programı” sayfa 100.

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.

SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) ve TLS (Transport Layer Security; İletim Arabirimi Katmanı Güvenliği), yalnızca anlatılanlar gibi PKI tekniklerini kullanır. SSL ve TLS ' nin kimlik doğrulamasının nasıl gerçekleştirilmesiyle ilgili daha fazla bilgi için bkz. “Güvenli Yuva Katmanı (SSL) ve İletim Arabirimi Katmanı Güvenliği (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 219içinde açıklanmaktadır. Benzer bir teknik, bir oturum oluşturmak üzere bağlandığında iki LU 'nun karşılıklı kimlik doğrulaması için SNA' da kullanılır. Teknik, “Oturum düzeyi kimlik doğrulaması” sayfa 72içinde 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 145 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.

Ayrıcalıklı kullanıcılar

Ayrıcalıklı bir kullanıcı, WebSphere MQiçin tam yönetim yetkilerine sahip bir kullanıcıdır.

Aşağıdaki tabloda listelenen kullanıcılara ek olarak, kuyruklar için `+crt` yetkisine sahip herhangi bir grubun üyeleri dolaylı olarak yöneticilere sahip olur. Benzer şekilde, kuyruk yöneticisine `+set` yetkisi olan her kullanıcı ve komut kuyruğunda `+put` yetkisi bir yöneticidir.

Bu ayrıcalıkları sıradan kullanıcılara ve uygulamalara vermemelisiniz.

Çizelge 13. Altyapıya göre ayrıcalıklı kullanıcılar.

Ayrıcalıklı kullanıcılara ait bir tablo. Windowsüzerinde, SYSTEM, mqm grubunun tüm üyeleri ve Administrators (Yöneticiler) grubunun tüm üyeleri ayrıcalıklı kullanıcılardır. UNIX and Linux sistemlerinde, mqm grubunun tüm üyeleri ayrıcalıklı kullanıcılardır. IBM iüzerinde, tanıtımlar (kullanıcılar) qmqm ve qmqmadm, qmqmadm grubunun tüm üyeleri ve *ALLOBJ ayarlarıyla tanımlanmış olan tüm kullanıcılar ayrıcalıklı kullanıcılardır.

Altyapı	**Ayrıcalıklı kullanıcılar**
Windows sistemleri	• SYSTEM • mqm grubunun üyeleri • Administrators (Yöneticiler) grubunun üyeleri
UNIX and Linux sistemleri	• mqm grubunun üyeleri

MQCSP yapısını kullanarak kullanıcıların tanımlanması ve kimlikleri doğrulanıyor

MQCONNX çağrısında MQCSP bağlantı güvenliği değiştirgeleri yapısını belirtebilirsiniz.

MQCSP bağlantı güvenliği değiştirgeleri yapısı, yetki hizmetinin kullanıcının kimliğini tanımlamak ve kimliğini doğrulamak için kullanabileceği bir kullanıcı kimliği ve parola içerir.

IBM WebSphere MQ ile sağlanan yetki hizmeti bileşeni, Object Authority Manager (OAM) olarak adlandırılır. OAM, kullanıcılara MQCSP içindeki kimliği temel alan, ancak parolayı doğrulamaması için yetki verir. OAM ile zincirleme çıkışlar kullanılarak ya da bir alternatif yetkilendirme hizmetiyle OAM ' ı değiştirerek, yetkilendirme hizmetinde parola geçerlilik denetimini uygulamak mümkündür.

Bir güvenlik çıkışındaki MQCSP ' yi değiştirebilirsiniz.

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 tipik olarak, WebSphere MQ MQI istemci uygulamasının kullanıcısı adına hareket eder. Bu durumda, karşılıklı kimlik

doğrulaması aslında iki kuyruk yöneticisi arasında ya da bir kuyruk yöneticisi ile bir WebSphere MQ MQI istemcisi 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. “SSPI kanal çıkış programı” sayfa 100.

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.

SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) ve TLS (Transport Layer Security; İletim Arabirimi Katmanı Güvenliği), yalnızca anlatılanlar gibi PKI tekniklerini kullanır. Güvenli Yuva Katmanı 'nın kimlik doğrulama gerçekleştirmesine ilişkin ek bilgi için bkz. “Güvenli Yuva Katmanı (SSL) ve İletim Arabirimi Katmanı Güvenliği (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 219içinde 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 72içinde 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 145 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.

SSL el sıkışması sırasında, iletişim ortakları dijital sertifikalar ile birbirlerini doğrular. 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.

UNIX, Linux ve Windows sistemlerinde, WebSphere 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. IBM WebSphere MQ classes for Java ve IBM WebSphere MQ classes for JMS , istemci kanal tanımlama çizelgesi dosyasında OCSP bilgilerini kullanamaz. Ancak, OCSP ' yi Using Online Certificate Protocol(Çevrimiçi Sertifika İletişim Kuralını Kullanma) bölümünde açıklandığı gibi yapılandırabilirsiniz.

Z/Os üzerinde ve IBM i WebSphere MQ SSL desteği, yalnızca LDAP sunucularında CRL ve ARL ' leri kullanarak geri alınmış sertifikalar olup olmadığını denetler.

Sertifika hakkında daha fazla bilgi için

Yetkililer, bkz. “dijital sertifikalar” sayfa 9.

İptal edilen sertifikalar ve OCSP

IBM WebSphere 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 Windows, UNIX and Linux sistemleri üzerinde WebSphere MQ için geçerlidir.

OCSP kullanılarak sayısal bir sertifikana ilişkin iptal durumunu denetlemek için, WebSphere MQ , hangi OCSP yanıtlayıcıya hangi OCSP yanıtlayıcıya ulaşabileceğini 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 ya da SSL sertifikalarının iptal edilip edilmediği konusunda endişe etmiyorsanız, bir sınama ortamında çalışmakta olduğunuz için, SSL stanza içinde OCSPCheckExtensions öğesini NO (HAYIR) olarak

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 WebSphere MQ , OCSP yanıtlayıcıya erişemiyor.
- OCSP yanıtlayıcısı bir yanıt gönderdi, ancak WebSphere MQ yanıta ilişkin dijital imzayı doğrulayamıyor.
- OCSP yanıtlayıcısı, sertifika için herhangi bir iptal verisi olmadığını belirten bir yanıt gönderdi.

IBM WebSphere MQ , `Bilinmiyor`' un OCSP sonucunu alırsa, davranışı OCSPAuthentication özniteliğinin ayarına bağlıdır. Kuyruk yöneticileri için bu öznitelik, UNIX and Linux sistemlerine ilişkin `qm.ini` dosyasının SSL kısmında ya da Windows kayıt defterinde tutulur. Bu, IBM WebSphere MQ Explorer kullanılarak ayarlanabilir. İstemciler için, istemci konfigürasyon dosyasının SSL kısmında tutulur.

`Bilinmiyor` değeri alındıysa ve OCSPAuthentication REQUIRECTION (varsayılan değer) olarak ayarlanırsa, WebSphere 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, WebSphere MQ , SSL kanalının başlatılmasına ve hiçbir uyarı ya da SSL olay iletisi oluşturulamamasına olanak tanır.

`Bilinmiyor` değeri alınırsa ve OCSPAuthentication WARN olarak ayarlanmışsa, SSL kanalı başlatılır, ancak IBM WebSphere 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, herhangi bir ek sertifika kurmanız gerekmez; SSL bağlanırlığını oluşturmak için önceden almış olduğunuz 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 SSL bağlanırlığı için güvenilen bir sertifika kuruluşu tarafından imzalanır), başka bir 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. You must add a copy of the OCSP responder certificate to the key database of the client or queue manager which performs the OCSP checking; bkz. “UNIX, Linux, and Windows sistemlerinde CA sertifikası (ya da kendinden onaylı bir sertifikenin genel bölümü) bir anahtar havuzuna eklenmesi” sayfa 128. Bir CA sertifikası eklendiğinde, varsayılan olarak, bu bağlamda gerekli ayar olan güvenilen bir kök olarak eklenir. If this certificate is not added, WebSphere MQ cannot verify

the digital signature on the OCSP response and the OCSP check results in an Unknown outcome, which might cause IBM WebSphere MQ to close the channel, depending on the value of OCSPAuthentication.

Java ve JMS istemci uygulamalarında OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü)

Java API ' nın bir sınırlaması nedeniyle, WebSphere MQ , yalnızca OCSP, tüm Java sanal makinesi (JVM) işlemi için etkinleştirildiğinde SSL ve TLS güvenli yuvalarına ilişkin Online Certificate Status Protocol (OCSP) sertifikası iptal denetimini kullanabilir. 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 bağlı olarak API ' ye tabi.

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.

Özellik Adı	Tanım
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 SSL ya da 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 dosyasını geçersiz kılamamak için Java ara düzeltmeleri ve ürün bakımı 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

WebSphere MQ'nun CRL' ler ve ARL ' ler için desteği platforma göre değişir.

Her platform için CRL ve ARL desteği aşağıdaki gibidir:

- z/OSüzerinde, Sistem 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.

WebSphere MQ , önceki 12 saat içinde erişilen CRL ve ARL ' lerin önbelleğini tutar.

Bir kuyruk yöneticisi ya da WebSphere MQ MQI istemcisi bir sertifika aldığında, sertifikenin geçerli olduğunu onaylamak için CRL ' yi denetler. Önbellek varsa, WebSphere MQ önbellekteki ilk denetimleri yapar. CRL önbellekte yoksa, WebSphere MQ , LDAP CRL sunucu konumlarını *SSLCRLNamelist* özniteliği tarafından belirtilen kimlik doğrulama bilgileri nesnelerinin ad listesinde, WebSphere MQ kullanılabilir bir CRL buluncaya kadar sorgular. Ad listesi belirlenmezse ya da boş bir değerle belirtildiyse, CRL ' ler denetlenmez.

LDAP hakkında daha fazla bilgi için bkz. Using lightweight directory access protocol services with WebSphere MQ for Pencereler.

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. WebSphere MQ SSL ile kullanmak için, bu özniteliklere ilişkin ikili verilerin DER (Definite Encoding Rules) biçimine uygun olması gerekir. LDIF dosyalarıyla ilgili ek bilgi için, LDAP sunucunuzla birlikte sağlanan belgelere bakın.

Şekil 12 sayfa 150 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.

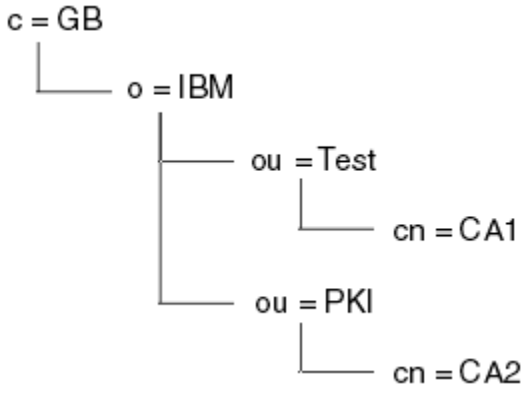
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

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 12. Bir Sertifika Yetkilisi için örnek LDIF dosyası. Bu, somutlamaya uygulanmasına kadar değişebilir.

Şekil 13 sayfa 150 , LDAP sunucunuzun Şekil 12 sayfa 150 içinde gösterilen örnek LDIF dosyasını CA2için benzer bir dosya ile birlikte yüklediğinizde oluşturduğu DBT yapısını, PKI kuruluşu tarafından ayarlanan hayali bir Sertifika Yetkilisi (IBMiçinde de) gösterir.



Şekil 13. 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 151.

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.

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, *SSLCRLNamelist* 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.

   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 nesnesi bulunduğunda, *gerekir* ' in işaret ettiği LDAP sunucuları aynı bilgileri içerir. Bu, bir ya da daha fazla LDAP sunucusunun başarısız olması durumunda hizmet sürekliliğini sağlar.

   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.
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, *SSLCRLNamelist*adlı bir kuyruk yöneticisi özniteliğini ayarlar. Kuyruk yöneticisinin bu özniteliğe ilişkin ilk değeri boş.

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 özdeş bilgiler *içermesi* gerektiğini unutmayın.

IBM WebSphere MQ Explorerkullanarak CRL 'lere ve ARL' lere erişme
Bir kuyruk yöneticisine, CRL ' lere nasıl erişileceğini bir kuyruk yöneticisine anlatmak için IBM WebSphere MQ Explorer olanağını 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** düğmesini tıklatın.
3. **Ad listeleri** 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 (adım “2.a” sayfa 152) listeye ekleyin.
   c. **Tamam** düğmesini 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. **CRL Namelist** (CRL Ad Listesi) alanına, ad listesinin adını yazın (adım “3.a” sayfa 152).

Accessing CRLs and ARLs with an IBM WebSphere MQ MQI client

Bir IBM WebSphere MQ MQI istemcisi tarafından denetlenmek 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
- Using the Active Directory (on Pencereler systems with Active Directory support)

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 özdeş bilgiler *içermesi* gerektiğini unutmayın.

You cannot access LDAP CRLs from a WebSphere MQ MQI client channel running on Linux (zSeries platform).

Bir OCSP yanıtlayıcıya ve CRL ' leri tutan LDAP sunucularının konumu

Bir IBM WebSphere MQ MQI istemcisi 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 listelenen üç şekilde, azalan öncelik sırasına göre sıralayabilirsiniz.

Bir WebSphere MQ MQI istemcisi uygulaması bir MQCONNX çağrısı yayınlandığında

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. Her bir MQAIR yapısı, bir WebSphere MQ MQI istemcisinin bir OCSP yanıtlayıcıya ya da LDAP sunucusuna CRL ' lere erişmesi için gereken tüm bilgileri içerir. 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

So that a WebSphere MQ MQI client can access an OCSP responder or LDAP servers that hold CRLs, include the attributes of one or more authentication information objects in a client channel definition table.

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. Özniteliklerden biri, OCSP yanıtlayıcı URL 'sini, başka bir kullanıcının anasistem adresini ya da LDAP sunucusunun çalıştığı bir sistemin IP adresini belirtir.

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 platformlarda belirtilebilir.

Bir WebSphere MQ MQI istemcisinin CRL ' leri içeren bir OCSP yanıtlayıcıya ya da LDAP sunucularına erişebilmesi için, bir ya da daha fazla kimlik doğrulama bilgisi nesnesinin öznitelikleri bir istemci kanalı tanımlama çizelgesine eklenebilir. Bu tür öznitelikleri aşağıdaki yollardan biriyle ekleyebilirsiniz:

Sunucu platformlarında AIX, HP-UX, Linux, Solaris ve Windows

Bir ya da daha fazla kimlik doğrulama bilgisi nesnesinin adlarını içeren bir ad listesi tanımlayabilirsiniz. Daha sonra, kuyruk yöneticisi özniteliğini **SSLCRLNameList**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 gerekli olduğunda kullanılamıyorsa, bir WebSphere MQ MQI istemcisi 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 (**SSLCRLNameList**), 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, o sistemdeki WebSphere MQ MQI istemcisi, 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 **SSLCRLNameList**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.

Windowsüzerinde Active Directory seçeneğini kullanma

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.

JMS için Java ve IBM WebSphere MQ sınıflarına ilişkin IBM WebSphere MQ sınıflarıyla CRL ve ARL ' lere erişilmesi

IBM WebSphere MQ classes for Java and IBM WebSphere MQ classes for JMS access CRLs differently from other platforms.

Java için IBM WebSphere MQ sınıflarıyla CRL ve ARL ' lerle çalışmaya ilişkin bilgi için Sertifika iptal listelerinin kullanılmasıbaşlıklı konuya bakın.

JMS için IBM WebSphere MQ sınıflarıyla CRL ve ARL ' lerle çalışma hakkında bilgi için bkz. SSLCERTSTORS nesne özelliği.

Kimlik Doğrulama Bilgileri Nesnelerinin Kullanılması

Kimlik doğrulama bilgileri nesnelerini MQSC ya da PCF komutlarını ya da IBM WebSphere MQ Explorerkullanarak 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 Script (MQSC) Commands başlıklı 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 Tanımlamaları başlıklı konuya bakın.

Kullanılabilir olduğu platformlarda, WebSphere MQ Explorer 'ı da kullanabilirsiniz.

Nesnelere erişim yetkisi verme

Bu bölümde, nesnelere erişimi denetlemek için nesne yetkisi yöneticisi ve kanal çıkış programlarının kullanılmasına ilişkin bilgiler yer alır.

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. Ayrıca sisteminize güvenlik uygulamak için hangi görevlerin gerçekleştirileceğini belirlemek üzere kullanabileceğiniz bir denetim listesi ve kullanıcılara IBM WebSphere MQ ürününü yönetme ve IBM WebSphere MQ nesneleriyle çalışma yetkisi verilmesine ilişkin dikkat edilmesi gereken noktalar da vardır. eğer sağlanan güvenlik mekanizmaları ihtiyaçlarınızı karşılamazsa, kendi kanal çıkış programlarınızı geliştirebilirsiniz.

Controlling access to objects by using the OAM on UNIX, Linux and Pencereler systems

Nesne yetkilisi yöneticisi (OAM), WebSphere MQ nesnelerine yetki verilmesi ve yetkiyi iptal etmek için bir komut arabirimi sağlar.

"UNIX, Linux, and Windows sistemlerinde IBM WebSphere MQ yönetimi yetkisi" sayfa 191' ta açıklandığı gibi, bu komutları kullanmak için uygun yetkiye sahip olmanız gerekir. WebSphere MQ ' u yönetme yetkisi olan kullanıcı kimliklerinin kuyruk yöneticisi için *super user* yetkisi vardır; bu yetki, bu kullanıcılara MQI isteklerini ya da komutlarını vermek için ek izin vermemeniz anlamına gelir.

UNIX, Linux, and Windows sistemlerindeki bir IBM WebSphere MQ nesnesine erişim verilmesi

Use the **setmqaut** control command, or the **MQCMD_SET_AUTH_REC** PCF command to give users, and groups of users, access to IBM WebSphere MQ objects.

setmqaut denetim komutunun ve sözdiziminin tam tanımı için, bkz. setmqautve **MQCMD_SET_AUTH_REC** PCF komutunun tam tanımı ve sözdizimi için bkz. Set Authority Record(Yetki Kaydı 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, *tanıtım*olarak belirtiyorsunuz; bu ad 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. "OAM soysal profillerinin UNIX, Linux, and Windows sistemlerinde kullanılması" sayfa 156.
- 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
```

Komutu 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.

OAM soysal profillerinin UNIX, Linux, and Windows sistemlerinde kullanılması

OAM soysal profilleri, bir kullanıcının bir kerede birden çok nesneye sahip olduğu yetkiyi ayarlamanızı sağlar; bu, yaratıldığında her bir nesneye ilişkin ayrı **setmqaut** komutlarını vermek zorunda kalmaktan çok.

setmqaut komutundaki soysal tanıtımların kullanılması, o profile uyan tüm nesneler için soysal bir yetki ayarlamanızı sağlar.

Bu konu derlemi, soysal tanıtımların daha ayrıntılı bir şekilde kullanılmasını açıklar.

OAM profillerinde genel arama karakterlerinin 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.?EFbelirtirseniz, bu tanıtıma verdiğiniz yetki, ABC.DEF , ABC.CEF, ABC.BEFve 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.JKLiçin geçerli olduğunu unutmayın; * bu bağlamda kullanılan her zaman bir niteleyici belirtilir.)
- 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** .

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:

```
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 the example above, the queue AB.CD has **alma** authority (AB.C* is more specific than AB.*).

Soysal karakterleri karşılaştırırken, *belirtimlilik* sırası şöyledir:

1. ?
2. *
3. **

Profil ayarlarının dökümü yapılıyor

dmpmqaut denetim komutunun ve sözdiziminin tam tanımı için bkz. dmpmqautve **MQCMD_INQUIRE_AUTH_RECS** PCF komutunun tam tanımı ve sözdiziminin tam tanımı için bkz. Sorgulama Yetki Kayıtları .

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 şöyle bir şeye benziyor:

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

Not: UNIX and Linux kullanıcıları **dmpmqaut** komutu için -p seçeneğini kullanabilse de, yetkileri tanımlarken bunun yerine -g groupname ' i 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 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.btanıtılmasına ilişkin tüm yetki kayıtlarını dökümünü alır. *, (kuyruk).

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

Sonuçta ortaya çıkan döküm şöyle bir şeye benziyor:

```
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 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. This example dumps all profile names and object types for queue manager qmX.

```
dmpmqaut -m qmX -l
```

Sonuçta ortaya çıkan döküm şöyle bir şeye benziyor:

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

Not: Yalnızca WebSphere MQ for Pencereler 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
```

OAM profillerinde genel arama karakterlerinin kullanılması

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 bir niteleyici belirtilir.)
- 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** .

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 the example above, the queue AB.CD has **alma** authority (AB.C* is more specific than AB.*).

Soysal karakterleri karşılaştırırken, *belirtimlilik* sırası şöyledir:

1. ?
2. *
3. **

Profil ayarlarının dökümü yapılıyor

Belirtilen bir tanıtımla ilişkili yürürlükteki yetkileri dökümünü almak için **dmpmqaut** denetim komutunu ya da **MQCMD_INQUIRE_AUTH_RECS** PCF komutunu kullanın.

dmpmqaut denetim komutunun ve sözdiziminin tam tanımı için bkz. dmpmqautve **MQCMD_INQUIRE_AUTH_RECS** PCF komutunun tam tanımı ve sözdiziminin tam tanımı için bkz. Sorgulama Yetki Kayıtları.

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 WebSphere MQ for Pencereler 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
```

Erişim ayarlarının görüntülenmesi

Belirli bir birincil kullanıcının ya da grubun belirli bir nesne için sahip olduğu yetkileri görüntülemek için **dspmqaut** denetim komutunu ya da **MQCMD_INQUIRE_ENTITY_AUTH** PCF komutunu kullanın.

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. dmpmqautve **MQCMD_INQUIRE_ENTITY_AUTH** PCF komutunun tam tanımı ve sözdizimine ilişkin bilgi için bkz. Sorgulama Varlığı Yetkisi.

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
```

IBM WebSphere MQ nesnesine erişimin değiştirilmesi ve geri alınması

Bir kullanıcının ya da grubun bir nesne üzerinde erişim düzeyini değiştirmek için **setmqaut** komutunu kullanın. Yetkilendirmeye sahip bir grubun üyesi olan belirli bir kullanıcının erişimini iptal etmek için kullanıcıyı gruptan kaldırın.

Kullanıcıyı bir gruptan kaldırma işlemi şu şekilde açıklanmaktadır:

- “Creating and managing groups on Pencereler” sayfa 80
- “Creating and managing groups on HP-UX” sayfa 82
- “Creating and managing groups on AIX” sayfa 83
- “Solaris üzerinde grup yaratılması ve yönetilmesi” sayfa 84
- “Creating and managing groups on Linux” sayfa 85

.

Bir IBM WebSphere MQ nesnesi yaratan kullanıcı kimliği, o nesneye tam denetim yetkilerine sahip olur. Bu kullanıcı kimliğini yerel mqm grubundan (ya da Windows sistemlerindeki denetimciler 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 komutunun ve sözdiziminin tam tanımı için, bkz. setmqautve **MQCMD_INQUIRE_ENTITY_AUTH** PCF komutunun tam tanımı ve sözdizimi için bkz. Sorgulama Varlık Yetkisi.

Pencereler' ta, kullanıcı profilini silmeden önce belirli bir Pencereler kullanıcı hesabıyla ilgili OAM girdilerini silin. Kullanıcı hesabını kaldırdıktan sonra OAM girdilerinin kaldırılması olanaksızdır.

UNIX, Linux, and Windows sistemlerinde güvenlik erişimi denetimlerinin önlenmesi

Tüm güvenlik denetimlerini kapatmak için OAM ' ı devre dışı bırakabilirsiniz. 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 değişkeni MQSNOAUT ' u ayarlayın (bunu yaparsanız, daha sonra bir OAM ekleyemezsiniz):

  MQSNOAUT değişkeninin ayarlanmasına ilişkin etkilere ilişkin ek bilgi için Ortam değişkenleri başlıklı konuya bakın.
- Kuyruk yöneticisi yapılanış dosyasını düzenleyerek hizmeti kaldırın. (Bunu yaparsanız, daha sonra bir OAM ekleyemezsiniz.)

OAM geçersiz kılındığında setmqaut ya da dspmqaut kullanırsanız, aşağıdaki noktaları göz önünde bulundurun:

- 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. This is because the OAM needs to be in place at object creation time. WebSphere MQ OAM kaldırıldıktan sonra yeniden kullanmak için kuyruk yöneticisinin yeniden oluşturulması gerekir.

İlgili kavramlar

Kurulabilir hizmetler

Kaynaklara gerekli erişim verilmesi

Use this topic to determine what tasks to perform to apply security to your WebSphere MQ system.

Bu görev hakkında

Bu görev sırasında, uygun güvenlik düzeyini WebSphere MQ kurulumunuzun öğelerine 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 163.
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 168.
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 173.
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 174.
6. Kuyruk yöneticinize bağlanmak için kullanıcı uygulamalarınız gerekiyor mu?
   a) No: Disable connectivity, as described in “Kuyruk yöneticisine bağlanılırlığı kaldırma” sayfa 175
   b) Evet: Bkz. “Kullanıcı uygulamalarının kuyruk yöneticinize bağlanmasına izin verme” sayfa 175.

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 14. 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 164
Konular	Grant partial administrative access to the required topics, as described in “Bazı konulara sınırlı yönetim erişimi verilmesi” sayfa 165
Kanallar	Grant partial administrative access to the required channels, as described in “Bazı kanallara sınırlı yönetim erişimi verilmesi” sayfa 165
Kuyruk yöneticisi	Kuyruk yöneticisine kısmi denetim erişimi ver (“Kuyruk yöneticisine sınırlı yönetim erişimi verilmesi” sayfa 166içinde açıklandığı gibi)
Süreçler	Grant partial administrative access to the required processes, as described in “Bazı süreçlere sınırlı yönetim erişimi verilmesi” sayfa 166
Ad listeleri	Grant partial administrative access to the required namelists, as described in “Bazı ad listelerine sınırlı yönetim erişimi verilmesi” sayfa 167
Hizmetler	Grant partial administrative access to the required services, as described in “Bazı hizmetler için sınırlı yönetim erişimi verilmesi” sayfa 167

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı. z/OS' ta 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:

  – UNIX, Linux ve Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + dlt, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- 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:

  – UNIX, Linux ve Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. + ctrl. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- Değişken adları aşağıdaki anlamlara sahiptir:

  QMgrName
  Kuyruk yöneticisinin adı. z/OS' ta 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:

– UNIX, Linux ve Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Sonuçlar

Kullanıcının kuyruk yöneticinde hangi MQSC komutlarının gerçekleştirebileceğini belirlemek için, her MQSC komutu için aşağıdaki komutları verin:

```
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:

- UNIX, Linux ve Windows sistemlerinde, 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.

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- 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:

  – UNIX, Linux ve Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- 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:

  – UNIX, Linux ve Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

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.

Not: Hizmet nesneleri z/OSüzerinde yok.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

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

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Sonuçlar

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:

- UNIX, Linux ve Windows sistemlerinde, şu yetkilerin herhangi bir birleşimi: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. authorization + alladm, + chg + clr + dlt + dsp ' ye denk geliyor.

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 15. 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 169

Çizelge 15. Kuyruk yöneticisi kaynaklarına ilişkin bir altkümeye tam denetimci erişimi verilmesi (devamı var)	
Kullanıcıların bu tipteki nesneleri denetlemeleri gerekir	**Bu işlemi gerçekleştir**
Konular	Grant full administrative access to the required topics, as described in "Bazı konulara tam yönetici erişimi verilmesi" sayfa 170
Kanallar	Grant full administrative access to the required channels, as described in "Bazı kanallara tam yönetim erişimi verilmesi" sayfa 170
Kuyruk yöneticisi	Grant full administrative access to the queue manager, as described in "Kuyruk yöneticisine tam denetimci erişimi verilmesi" sayfa 171
Süreçler	Grant full administrative access to the required processes, as described in "Bazı süreçlere tam yönetim erişimi verilmesi" sayfa 171
Ad listeleri	Grant full administrative access to the required namelists, as described in "Bazı ad listelerine tam denetimci erişimi verilmesi" sayfa 172
Hizmetler	"Bazı hizmetlere tam yönetim erişimi verilmesi" sayfa 172' 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM)
MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM)
MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- z/OSiçin şu komutları verin:

```
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/OS' ta 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.

Yordam

- Sihirbazın kullanılması:
  a) WebSphere MQ Explorer Navigator bölmesinde, kuyruk yöneticisini farenin sağ düğmesiyle tıklatın ve **Nesne Yetkilileri** > **Rol Tabanlı Yetkiler Ekle**öğelerini seçin.
  Rol Tabanlı Yetkiler Ekle sihirbazı açılır.
- 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
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 MQ Explorer 'ı kullanmak istiyorsanız gereklidir.
- 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/OSiçin şu komutları verin:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MQTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQTOPIC) ID(GroupName) ACCESS(READ)
RDEFINE MQPROC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQPROC) ID(GroupName) ACCESS(READ)
RDEFINE MQNLIST QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

```
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OS' ta 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 kullanın.

Yordam

- Sihirbazın kullanılması:
  a) WebSphere MQ Explorer Navigator bölmesinde, kuyruk yöneticisini farenin sağ düğmesiyle tıklatın ve **Nesne Yetkilileri** > **Rol Tabanlı Yetkiler Ekle**öğelerini seçin.
  Rol Tabanlı Yetkiler Ekle sihirbazı açılır.
- 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.QUEUE -t queue -g GroupName +dsp +inq +get
setmqaut -m QMgrName -n '**' -t topic -g GroupName +alladm
setmqaut -m QMgrName -n @class -t topic -g GroupName +crt
setmqaut -m QMgrName -n '**' -t channel -g GroupName +alladm
setmqaut -m QMgrName -n @class -t channel -g GroupName +crt
setmqaut -m QMgrName -n '**' -t clntconn -g GroupName +alladm
setmqaut -m QMgrName -n @class -t clntconn -g GroupName +crt
setmqaut -m QMgrName -n '**' -t authinfo -g GroupName +alladm
setmqaut -m QMgrName -n @class -t authinfo -g GroupName +crt
setmqaut -m QMgrName -n '**' -t listener -g GroupName +alladm
setmqaut -m QMgrName -n @class -t listener -g GroupName +crt
setmqaut -m QMgrName -n '**' -t namelist -g GroupName +alladm
setmqaut -m QMgrName -n @class -t namelist -g GroupName +crt
setmqaut -m QMgrName -n '**' -t process -g GroupName +alladm
setmqaut -m QMgrName -n @class -t process -g GroupName +crt
setmqaut -m QMgrName -n '**' -t service -g GroupName +alladm
setmqaut -m QMgrName -n @class -t service -g GroupName +crt
setmqaut -m QMgrName -t qmgr -g GroupName +alladm +conn
```

- Windows sistemleri için, UNIX and Linux sistemleri için aynı komutları verin, ancakprofileyerine @CLASS profil adını kullanın.
- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER('GroupName') AUT(*ALLADM) MQMNAME('QMgrName')
```

- z/OSiçin şu 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' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- IBM iiçin şu komutu verin:

```
RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- z/OSiçin şu 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' ta 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 182.

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 176.

Her iki durumda da, bağlantı güvenliğini “Bağlantı güvenliğinin ayarlanması” sayfa 182içinde 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 183
Konu kullanımını oluşturan uygulamalariniz var	Bkz. “Konulara kullanıcı erişimini denetleme” sayfa 188.
Kuyruk yöneticisi nesnesini sorgulayan uygulamalariniz var	Bkz. “Kuyruk Yöneticisi üzerinde sorgulama için yetki verilmesi” sayfa 189.

Bildirim	Bu işlemi gerçekleştirin
Süreç nesnelerini kullanan uygulamalariniz var	Bkz. “Süreçlere erişim yetkisi verilmesi” sayfa 190
Ad listelerini kullanan uygulamalariniz var	Bkz. “Ad listelerine erişim yetkisi verilmesi” sayfa 190

Kuyruk yöneticisine uzaktan bağlanılırlığın sağlanması

SSL ya da TLS, bir güvenlik çıkışı, kanal doğrulama kayıtları ya da bu yöntemlerin bir bileşimini kullanarak kuyruk yöneticisine uzaktan bağlanılırlığı güvenceye almak için kullanabilirsiniz.

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 SSL ya da TLS ' yi kullanma:
   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 SSL ya da TLS ' nin kullanılması:
   a) MCAUSER, ayrıcalıksız bir kullanıcı tanıtıcıyla sunucu bağlantısı kanalına ayarlanır.
   b) MQCD yapısındaki çıkışa aktarılan SSLPeerNamePtr ve SSLPeerNameLength alanlarında aldığı SSL DN değerine bağlı olarak bir MCAUSER değeri atamak için bir güvenlik çıkışı yazın.
3. SSL ya da TLS ' yi sabit kanal tanımlama değerleriyle kullanarak:
   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. SSL ya da 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 176
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 143. `*MQADMIN`ile 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. Bir sunucu bağlantı kanalının adını aşağıda gösterilen komutlarda 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 adresleri başlıklı konuya bakın.

İlgili başvurular
CHLAUTH KüMESI

İstemcinin değerlendirilen bir kullanıcı kimliğini MCAUSER kullanıcı kimliğiyle eşlenmesi
Bir istemciden alınan özgün 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 tarafından değerlendirilen kullanıcı kimliğidir.

user (kullanıcı), istemci kullanıcı adı yerine kullanılacak kullanıcı kimliğidir.

İlgili başvurular

CHLAUTH KüMESI

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
) 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 WebSphere MQ kurallarını izleyen bir dizgidir. Bkz. WebSphere MQ SSLPEER değerleri için kurallar.

kullanıcı , belirtilen DN ' yi kullanan tüm bağlantılar için kullanılacak kullanıcı kimliğidir.

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. Aşağıda gösterilen komutta bir sunucu bağlantı kanalı adı belirtilirse, hiçbir etkisi olmaz.

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 için erişim engelleyici erişim belirtildi kullanıcı kimliği

Bir istemcinin kullanıcı kimliğini başlatma kanallarından bildirmesini 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 tarafından değerlendirilen kullanıcı kimliğidir.

İlgili başvurular

CHLAUTH KüMESI

SSL Ayırt Edici Adı için erişimin engellenmesi

SSL Ayırt Edici Adının başlangıç kanallarından olmasını önlemek için 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')
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 WebSphere MQ kurallarını izleyen bir dizgidir. Bkz. WebSphere MQ SSLPEER değerleri için kurallar.

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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutu verin:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
```

- IBM iiçin şu komutu verin:

```
GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM)  USER('GroupName') AUT(*CONNECT)
```

- z/OSiçin şu komutları verin:

```
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 yetki verme yetkisine sahip olur. Belirli bir bağlantı tipini kullanmazsanız, ilgili komutları atlayın.

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı. z/OS' ta 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.

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 183
Uygulama kümeleri bağlamı	Bkz. “Bağlamı ayarlamak için yetki verilmesi” sayfa 184
Uygulama bağlamı geçiyor	Bkz. “Bağlam geçişi için yetki verilmesi” sayfa 185
Uygulama, iletileri kümelenmiş bir kuyruğa koyar.	Bkz. “Uzak küme kuyruklarına ileti koyma yetkisi” sayfa 239
Uygulama, iletileri yerel bir kuyruğa koyar	Bkz. “İletileri yerel bir kuyruğa koyma yetkisi verilmesi” sayfa 186
Uygulama, iletileri bir model kuyruğuna koyar.	Bkz. “Bir model kuyruğuna ileti koymak için yetki verilmesi” sayfa 186
Uygulama, iletileri uzak bir kuyruğa koyar.	Bkz. “İletileri uzak bir küme kuyruğuna koyma yetkisi verilmesi” sayfa 187

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.

Yordam

- UNIX, Linux ve 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 şu 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/OS' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutlardan birini yayınlayın:
  - 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
```

- 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 çalıştırın:
  - 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/OS' ta 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.

Yordam

- UNIX, Linux ve Windows sistemleri için aşağıdaki komutlardan birini yayınlayın:
  - 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 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/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/OS' ta 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.

Yordam
- UNIX, Linux ve 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 şu 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/OS' ta 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.

Yordam
- UNIX, Linux ve 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 şu 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/OS' ta 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. Uzak bir kuyruğun yerel tanımlamasını kullanıyorsanız, yerel nesneyi koymak için yetkiniz olması gerekir: bkz. “İletileri yerel bir kuyruğa koyma yetkisi verilmesi” sayfa 186. 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.

UNIX, Linuxve Windows sistemlerinde, SET AUTHREC komutunu da kullanabilirsiniz.

Yordam

- UNIX, Linux ve 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 şu komutları verin:

```
RDEFINE MQQUEUE  QMgrNameObjectProfile UACC(NONE)
PERMIT QMgrNameObjectProfile CLASS(MQADMIN)
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/OS' ta 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 16. Konulara kullanıcı erişimini denetleme

Bildirim	**İşlem**
Uygulama bir konuya ileti yayınlar	Bkz. "Bir konuya ileti yayınlamak için yetki verilmesi" sayfa 188
Uygulama bir konuya abone olur	Bkz. "Konulara abone olmak için yetki verilmesi" sayfa 188

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.

Yordam

- UNIX, Linux ve 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 şu 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/OS' ta 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.

Yordam

- UNIX, Linux ve 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 şu 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/OS' ta 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.

Yordam

- UNIX, Linux ve 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 şu 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/OS' ta 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.

Yordam
- UNIX, Linux ve 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 şu 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/OS' ta 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.

Yordam
- UNIX, Linux ve 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 şu 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/OS' ta 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.

UNIX, Linux, and Windows sistemlerinde IBM WebSphere MQ yönetimi yetkisi

IBM WebSphere MQ yöneticileri tüm IBM WebSphere 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 Pencereler systems.

IBM WebSphere MQ yöneticileri, tüm WebSphere MQ komutlarını kullanma yetkisine sahiptir (diğer kullanıcılar için WebSphere MQ yetkileri vermek için komutlar dahil)

Bir IBM WebSphere MQ yöneticisi olmak için, *mqm* grubu (ya da Pencereler sistemlerinde Administrators (Yöneticiler) grubunun bir üyesi) adlı özel bir grubun üyesi olmanız gerekir. The mqm group is created automatically when WebSphere MQ is installed; add further users to the group to allow them to perform administration. Bu grubun tüm üyelerinin tüm kaynaklara erişimleri vardır. Bu erişim, yalnızca mqm grubundan bir kullanıcı kaldırılarak ve REFRESH SECURITY komutu verilerek iptal edilebilir. Yöneticiler, WebSphere MQ' u yönetmek için denetim komutlarını kullanabilirler. One of these control commands is **setmqaut**, which is used to grant authorities to other users to enable them to access or control WebSphere MQ resources. Yetki kayıtlarının yönetilmesine ilişkin PCF komutları, kuyruk yöneticisine dsp ve chg yetkilerine sahip yönetici olmayan kullanıcılar tarafından kullanılabilir. PCF komutlarını kullanarak yetkilerin yönetilmesine ilişkin ek bilgi için Programlanır Komut Biçimleribaşlıklı konuya bakın.

Yöneticiler, IBM WebSphere 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. WebSphere MQ Explorer, denetim görevlerini gerçekleştirmek için PCF komutları verir. Denetimciler, yerel sistemdeki bir kuyruk yöneticisini denetlemek için WebSphere MQ Explorer olanağını kullanmak için ek yetkilere gerek duymaz. IBM WebSphere MQ Gezgini, 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 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. WebSphere 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.

Ayrıca, Pencereler sistemlerinde, SYSTEM hesabında WebSphere MQ kaynaklarına tam erişim olanağı bulunur.

UNIX and Linux altyapılarında, yalnızca ürün tarafından kullanılmak üzere, mqm ' nin özel bir kullanıcı kimliği de yaratılır. Bu, ayrıcalıklı olmayan kullanıcılar için hiçbir zaman kullanılabilir olmamalıdır. Tüm WebSphere MQ nesneleri kullanıcı kimliği mqm 'e aittir.

Pencereler 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 denetleyicisinden bir etki alanı mqm grubu da yaratabilir ve yerel mqm grubuna ekleyebilirsiniz. Some commands, for example **crtmqm**, manipulate authorities on IBM WebSphere 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 yerel bir kullanıcı ve aynı adı taşıyan bir etki alanı kimliği doğrulanmış bir kullanıcıyla sahipseniz, yetki reddedildiğinde Windows sistemlerinde durumlar olabilir. Bu, “Birincil kullanıcılar ve gruplar” sayfa 195içinde açıklanmaktadır.

Kullanıcı Hesabı Denetimi (UAC) özelliği olanPencereler sürümleri, Administrators (Yöneticiler) grubunun üyeleri olsalar bile, kullanıcıların belirli işletim sistemi tesislerinde gerçekleştirebileceği işlemleri kısıtlar. Kullanıcı kimliğiniz Yöneticiler grubundaysa, ancak mqm grubu değilse, **crtmqm**gibi WebSphere MQ yönetim komutlarını vermek için yükseltilmiş komut istemini kullanmanız gerekir; aksi takdirde, "AMQ7077: İstenen işlemi gerçekleştirme yetkiniz yok" hatası oluşturulur. Yükseltilmiş bir komut istemini açmak için, komut isteminin başlangıç menüsü öğesini sağ tıklatın ya da komut istemi için "Yönetici olarak çalıştır" seçeneğini belirleyin.

Aşağıdaki işlemi 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 69içinde açıklanmaktadır).
- 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.
- WebSphere MQ 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 Sürüm 5.3 bu sınırı yükseltti, ancak WebSphere MQ , tüm UNIX and Linux altyapılarında 12 karakterlik bir kısıtlamayı gözlemlemeye devam eder. 12 karakterden uzun bir kullanıcı kimliği kullanırsanız, WebSphere MQ bu değeri UNKNOWNdeğeriyle değiştirir. Do not define a user ID with a value of UNKNOWN.

mqm grubunu yönetme

Mqm grubundaki kullanıcıların WebSphere MQüzerinde tam denetim ayrıcalıkları verilir. Bu nedenle, uygulamaları ve olağan kullanıcıları mqm grubuna kaydetmemeniz gerekir. Mqm grubu yalnızca WebSphere MQ denetimcilerinin hesaplarını içermelidir.

Bu görevler aşağıda açıklanmıştır:

- Windows üzerinde grup yaratılması ve yönetilmesi
- Creating and managing groups on HP-UX
- Creating and managing groups on AIX
- Solaris üzerinde grup oluşturma ve yönetme
- Creating and managing groups on Linux

Etki alanı denetleyiciniz Pencereler 2000 ya da Pencereler 2003 üzerinde çalışıyorsa, etki alanı yöneticiniz WebSphere MQ için özel bir hesap oluşturmak zorunda kalabilirler. Bu, WebSphereWebSphere MQaccountshesaplarının yapılandırılmasıbaşlıklı konuda açıklanmaktadır.

UNIX, Linux, and Windows sistemlerindeki IBM WebSphere MQ nesneleriyle çalışma yetkisi

Tüm nesneler IBM WebSphere MQtarafından 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 WebSphere MQtarafından 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 (göz atma seçeneği ileMQGET) kullanılabilir. 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 Windows sistemlerinde IBM WebSphere MQ yönetimi yetkisi” sayfa 191
IBM WebSphere MQ yöneticileri tüm IBM WebSphere 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 Pencereler systems.

UNIX, Linux, and Windows sistemlerinde 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. WebSphere MQ , kullanıcı kimliğinin kuyruk yöneticisine bağlanma yetkisine sahip olduğunu doğrular ve ileride yapılacak denetlere ilişkin kullanıcı kimliğini korur.

Kullanıcıların WebSphere MQ' da oturum açması gerekmez; WebSphere MQ , kullanıcıların temeldeki işletim sisteminde oturum açmış olduğunu ve bunun için kimlik doğrulaması gerçekleştirdiğini varsayar.

Nesnenin açılması (MQOPEN ya da MQPUT1 çağrıları)
WebSphere MQ objects are accessed by opening the object and issuing commands against it. 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.

WebSphere 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. Bu, Not “1” sayfa 88içinde açıklanmaktadır.

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 bulunan konu nesnelerine göre 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.

Erişim denetimi, UNIX, Linux, and Windows sistemlerinde IBM WebSphere MQ tarafından nasıl uygulanmaktadır?

IBM WebSphere MQ , nesne yetkili yöneticisi kullanılarak, temeldeki işletim sistemi tarafından sağlanan güvenlik hizmetlerini kullanır. IBM WebSphere MQ , erişim denetimi listelerini oluşturmak ve korumak için komutlar sağlar.

Yetkilendirme Hizmeti Arabirimi adı verilen bir erişim denetimi arabirimi, WebSphere MQ' nun bir parçasıdır. WebSphere MQ , *object authority manager (OAM)*olarak bilinen bir erişim denetimi yöneticisinin (Authorization Service Interface ile uyumlu) bir somutlamasını sağlar. Başka bir şekilde belirtilmedikçe (“UNIX, Linux, and Windows sistemlerinde güvenlik erişimi denetimlerinin önlenmesi” sayfa 162içinde açıklandığı gibi), yarattığınız her kuyruk yöneticisi için 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 durumlarda WebSphere MQ nesnelerine erişebilirler. “Controlling access to objects by using the OAM on UNIX, Linux and Pencereler systems” sayfa 155 , 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, Administrators (Yöneticiler) grubundaki kullanıcılara ve sistem tanıtıcısı ile oturum açan kullanıcılarla sınırlanmıştır. Kuyruğa kullanıcı erişimi değiştirilemez.

WebSphere MQ erişim denetimi listeleri yaratmak ve bunları korumak için komutlar sağlar. Bu komutlarla ilgili daha fazla bilgi için bkz. “Controlling access to objects by using the OAM on UNIX, Linux and Pencereler systems” sayfa 155.

WebSphere MQ , OAM ' yi 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. WebSphere MQ , OM ' nin kararını izler; OAM bir karar veremezse, WebSphere MQ erişime izin vermez.

UNIX, Linux, and Windows sistemlerindeki 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 WebSphere 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 WebSphere 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 ve Windows sistemlerinde bağlam yetkisi” sayfa 197içinde açıklanmıştır. Uygulamalar, bağlam bilgilerini değiştirme yetkisine sahip olmadıkları sürece bu bilgileri değiştiremez.

Birincil kullanıcılar ve gruplar

Birincil kullanıcılar gruplara ait olabilir. Belirli bir kaynağa, bireylere değil, gereken yönetim miktarını azaltmak için erişim izni verebilirsiniz. UNIX and Linux sistemlerinde tüm Erişim Denetim Listeleri (EDL ' ler) grupları temel alır, ancak Windows sistemlerinde, ACLS kullanıcı kimlikleri ve gruplara dayalıdır.

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. Bu işlem aşağıdaki yerde açıklanmaktadır:

- Windows üzerinde grup yaratılması ve yönetilmesi
- Creating and managing groups on HP-UX
- Creating and managing groups on AIX
- Solaris üzerinde grup oluşturma ve yönetme
- 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. Bu yetkiler önbelleğe alınır; dolayısıyla, MQSC komutunu REFRESH SECURITY (ya da PCF eşdeğeri) komutunu vermezseniz, asıl adın grup üyeliği için yaptığınız değişiklikler kuyruk yöneticisi yeniden başlatılıncaya kadar tanınmaz.

UNIX and Linux sistemleri

Tüm EDL ' ler gruplar üzerine kuruludur. Bir kullanıcıya belirli bir kaynağa erişim izni verildiğinde, EDL ' de kullanıcı kimliğinin birincil grubu bulunur. 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. *Hiç kimse* grubundaki yetkilendirmeyi, belirli yetkileri olmayan kullanıcılara WebSphere MQ kaynaklarına erişim izni vermek için değiştirebilirsiniz.

Do not define a user ID with the value "BILINMIYOR". Kullanıcı kimliği çok uzun olduğunda, isteğe bağlı kullanıcı kimlikleri UNKNOWN erişim yetkilerini kullanacakken "BILINMIYOR" değeri kullanılır.

Kullanıcı kimlikleri en çok 12 karakter içerebilir ve 12 karaktere kadar grup adı içerebilir.

Windows sistemleri

ACL ' ler hem kullanıcı kimlikleri, hem de gruplar temel alınarak kullanılabilir. Denetimler, tek tek kullanıcı kimliklerinin EDL ' de de görüntülenebilmesi dışında, UNIX sistemleri için de aynı olup olmamasını sağlar. Aynı kullanıcı kimliğine sahip farklı etki alanlarında farklı kullanıcılarınız olabilir. WebSphere 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\GroupName
```

Genel gruplar OAM tarafından yalnızca iki durumda kontrol edilir:

1. Kuyruk yöneticisi güvenlik kısmı şu ayarı içerir: `GroupModel=GlobalGroups`; bkz. Güvenlik.
2. Kuyruk yöneticisi, diğer 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 yetkilisi yöneticisini (OAM) kullanarak WebSphere 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, yerel bir grup aracılığıyla yerel mqm grubunun üyeliği içeren bir etki alanı denetleyicisi tarafından kimliği doğrulanan bir kullanıcı kimliğinden `crtmqm` komutunu verdiyseniz, sistemde yerel mqm grubunda olmayan aynı adı taşıyan yerel bir kullanıcı varsa komut başarısız olur.

Windows güvenlik tanıtıcıları (SID ' ler)

Pencereler üzerinde WebSphere MQ , kullanılabilir olduğu SID ' yi kullanır. Bir yetki isteğiyle bir Pencereler SID sağlanmıyorsa, WebSphere MQ kullanıcı adına bağlı olarak kullanıcıyı tanımlar; ancak bu, yanlış yetkinin verilmesiyle sonuçlanabilir.

Pencereler sistemlerinde, kullanıcı kimliğini tamamlamak için güvenlik tanıtıcısı (SID) kullanılır. SID, kullanıcının tanımlı olduğu Windows güvenlik hesabı yöneticisi (SAM) veritabanına ilişkin tüm kullanıcı hesabı ayrıntılarını tanımlayan bilgileri içerir. WebSphere MQ 'da Windowsiçin bir ileti yaratıldığında, WebSphere MQ , SID' yi ileti tanımlayıcısında saklar. Pencereler üzerinde WebSphere 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 yetkilendirme isteğiyle bir Windows SID sağlanmıyorsa, WebSphere MQ kullanıcı adına dayalı 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 WebSphere MQ yetkisi verilmiş olabilir. Bu sorunu önlemek için, her yetki isteğine bir SID ekleyin; SID, kullanıcı kimlik bilgilerini oluşturmak için WebSphere MQ tarafından kullanılır.

Tüm yetkilendirme isteklerinin bir SID içermesi gerektiğini belirtmek için `regedit`öğesini kullanın. SecurityPolicy ' yi NTSIDsRequiredolarak ayarlayın.

UNIX, Linux ve Windows sistemlerindeki diğer kullanıcı yetkisi

Bir kullanıcı kimliğinin, bir WebSphere MQ nesnesine erişirken başka bir kullanıcının yetkisini kullanabileceğini belirtebilirsiniz. Buna *diğer-kullanıcı yetkisi*adı verilir ve bunu herhangi bir WebSphere MQ nesnesi üzerinde 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.

UNIX, Linux ve Windows sistemlerinde bağlam yetkisi

Bağlam, belirli bir ileti için geçerli olan ve iletinin bir parçası olan MQMD ileti tanımlayıcısında yer alan bilgilerdir. Uygulamalar, bir MQOPEN ya da MQPUT çağrısı yapıldığında bağlam verilerini belirtebilir.

Bağlam bilgileri iki bölüm halinde gelir:

Kimlik bölümü
Mesajın kimden geldiğini. UserIdentifier, AccountingTokenve ApplIdentityData alanlarından oluşur.

Köken bölümü
Mesajın nereden geldiği ve ne zaman kuyruğa konulduğu. PutApplType, PutApplName, PutDate, PutTimeve ApplOriginData alanlarından oluşur.

Uygulamalar, bir MQOPEN ya da MQPUT çağrısı yapıldığında bağlam verilerini belirtebilir. Bu veriler uygulama tarafından yaratılabilir, başka bir iletiden aktarılabilir ya da varsayılan olarak kuyruk yöneticisi tarafından oluşturulabilir. Örneğin, sunucu programları tarafından istekte bulunanın kimliğini denetlemek, iletinin yetkili bir kullanıcı kimliği altında çalışan bir uygulamadan gelip gelmeyeceğini test etmek için sunucu programları tarafından kullanılabilir.

Bir sunucu programı, alternatif bir kullanıcının kullanıcı kimliğini belirlemek için UserIdentifier olanağını kullanabilir. Kullanıcının herhangi bir MQOPEN ya da MQPUT1 çağrısında bağlam seçeneklerinden herhangi birini belirtip belirtemeyeceğini denetlemek için bağlam yetkilendirmesini kullanabilirsiniz.

Bağlam seçeneklerine ilişkin bilgi için Bağlam bilgilerini denetleme 'e ve bağlamla ilgili ileti tanımlayıcı alanlarına ilişkin açıklamalar için MQMD için genel bakış ' e 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 WebSphere 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. *MCAUserIdentifier* , MCA kullanıcı tanıtıcısının ilk 12 baytını içerir. MCA kullanıcı kimliği boş değilse, ileti kanalı aracısı tarafından MQ kaynaklarına erişim yetkisi için kullanılacak kullanıcı kimliğini belirtir. MCAUSER ' in Windows altyapısında 12 karakterden kısa olmasına dikkat edin.

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.

IBM i, UNIX, Linux ve Pencereler sistemlerinde, *MCAUserIdentifier* değeri boş değilse, kuyruk yöneticisi, bir MCA kuyruk yöneticisine bağlandıktan sonra kuyruk yöneticisinin kaynaklarına erişmeyi denediğinde 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/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
- Denetimler için kullanılan RACF tanıtımı
- 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:

- Provided there is no security exit at the client end of an MQI channel, a user ID associated with the WebSphere MQ client application flows from the client connection MCA to the server connection MCA when the client application issues an MQCONN call.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 bir güvenlik çıkışı, WebSphere MQ MQI istemcisi 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 SSL kullanılıyorsa, MQCD 'nin SSLPeerNamePtr alanında iş ortağının Ayırt Edici Adı (DN), çıkışa iletilir 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: WebSphere MQ v7.1 yayın düzeyinden önce oluşturulan güvenlik çıkışı uygulamaları güncellenmesini gerektirebilir. Ek bilgi için bkz. Kanal güvenlik çıkış programları.

WebSphere MQ nesne yetkisi yöneticisi kullanıcı kimlik doğrulaması

WebSphere MQ MQI istemcisi bağlantılarında, nesne yetkisi 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, kuyruk yöneticisinden istemci adına WebSphere MQ kaynaklarına eriştiğinde yetki denetimleri için bu kullanıcı kimliğini kullanmasını isteyin.

PUTAUT parametresi kanal tanımlamasındaki CTX (ya da z/OSüzerinde ALTMCA) olarak ayarlandıysa, her gelen iletinin *UserIdentifier* (Kullanıcı Kimliği) 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 144.

API çıkışta ve API ' den geçiş çıkışındaki erişim denetimi uygulanıyor

An API or API-crossing exit can provide access controls to supplement those provided by WebSphere MQ. 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.

İletilerin gizliliği

Gizliliği korumak için, mesajlarınızı şifreleyin. Gereksinimlerinize bağlı olarak WebSphere MQ ' ta iletileri şifrelemenin çeşitli yöntemleri vardır.

Your choice of CipherSpec determines what level of confidentiality you have.

Uygulama düzeyinde, noktadan noktaya ileti alışverişi altyapısı için uçtan uca veri koruması gerekiyorsa, iletileri şifrelemek için WebSphere MQ Advanced Message Security olanağını kullanabilir ya da kendi API çıkışınızı ya da API geçiş çıkışınızı yazabilirsiniz.

İletileri yalnızca bir kanaldan aktarırken şifrelemeniz gerekiyorsa, kuyruk yöneticilerinizde yeterli güvenliğiniz olduğundan, SSL ya da TLS ' yi kullanabilir ya da kendi güvenlik çıkışınızı, ileti çıkışınızı ya da gönderme ve alma çıkış programlarını yazabilirsiniz.

WebSphere MQ Advanced Message Securityile ilgili daha fazla bilgi için bkz. “ Gelişmiş İleti Güvenliğiplanlaması” sayfa 62.SSL ve TLS ' nin WebSphere MQ ile kullanımı, “SSL ve TLS içinIBM WebSphere MQ desteği” sayfa 23adresinde açıklanmıştır. İleti şifrelemesinde çıkış programlarının kullanımı, “Kullanıcı çıkış programlarında gizliliği uygulama” sayfa 219adresinde açıklanmıştır.

SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanması

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 edinmeniz ve yönetmeniz gerekir. Bir sınama sisteminde, kendinden imzalı sertifikaları ya da yerel bir sertifika yetkilisi (CA) tarafından verilen sertifikaları

kullanabilirsiniz. Bir üretim sisteminde kendinden onaylı sertifikalar kullanmayın. Daha fazla bilgi için bkz. ..//zs14140_.dita.

Sertifika oluşturma ve yönetme hakkında tam bilgi edinmek için bkz. “UNIX, Linux, and Windows sistemlerinde SSL ya da TLS ile çalışma” sayfa 111.

Bu konular grubu, SSL iletişimini ayarlarken yer alan 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. WebSphere MQ somutlaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

Notlar:

1. Bu bağlamda, bir SSL istemcisi el sıkışmasını başlatan bağlantıyı belirtir.
2. Ek ayrıntılar için Sözlük ' e bakın.

UNIX, Linux ve Windows sistemlerinde, SSL ya da TLS istemcisi yalnızca, doğru WebSphere MQ biçiminde bir etiketi varsa, bu sertifikayı gönderir; bu da kuyruk yöneticinizin adının küçük harfe çevrilerek `ibmwebspheremq` ' in izlediği bir sertifika olur. Örneğin, `QM1`için, `ibmwebspheremqqm1`.

WebSphere MQ , diğer ürünlere ilişkin sertifikalarla 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 işlev gören kanalın sonuna SSLCAUTH parametresiyle ya da bir SSLPEER parametre değeri kümesine ayarlı olarak tanımlandıysa başarısız olur. Bir kuyruk yöneticisini anonim olarak bağlama hakkında daha fazla bilgi için, SSL ya da TLS istemcisi bir sertifika göndermediği zaman bkz. “Tek yönlü kimlik doğrulaması kullanarak iki kuyruk yöneticisinin bağlanması” sayfa 204.

İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için kendinden onaylı sertifikaların kullanılması

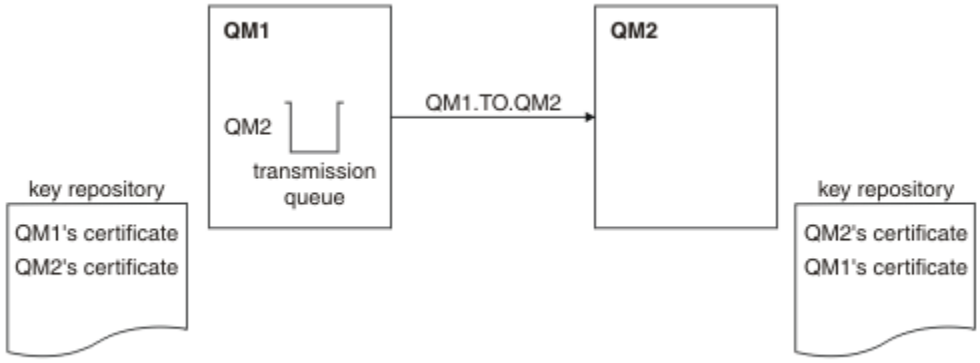
Kendinden onaylı SSL ya da TLS sertifikalarını kullanarak iki kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Güvenli bir şekilde iletişim kurmak zorunda olan iki kuyruk yöneticisi, QM1 ve QM2vardır. QM1 ile QM2arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Kendinden onaylı sertifikalar kullanarak güvenli iletişiminizi test etme kararı aldınız.

Sonuçtaki yapılanış şöyle görünür:



Şekil 14. Bu görevle sonuçlanan yapılandırma

Şekil 14 sayfa 201'ta, QM1 için anahtar havuzu, QM1 sertifikasını ve QM2' den genel sertifikayı içerir. QM2 için anahtar havuzu, QM2 sertifikasını ve QM1' den genel sertifikayı içerir.

Yordam

1. Her kuyruk yöneticisine ilişkin anahtar havuzunu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. Her kuyruk yöneticisi için kendinden onaylı sertifika yarat:
   - UNIX, Linuxve Windows sistemlerinde.
3. Her sertifikana ilişkin bir kopyasını çıkarın:
   - UNIX, Linuxve Windows sistemlerinde.
4. Transfer the public part of the QM1 certificate to the QM2 system and vice versa, using a utility such as FTP.
5. İş ortağı sertifikasını, her kuyruk yöneticisi için anahtar havuzuna ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
6. QM1' ta, aşağıdaki örnek gibi komutlar vererek, bir gönderen kanalı ve ilişkili iletim kuyruğu tanımlayın:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
   SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

   DEFINE QLOCAL(QM2) USAGE(XMITQ)
   ```

   Bu örnek, CipherSpec RC4_MD5' i kullanır. Kanalın her bir ucundaki CipherSpecs (şifreleme Belirtimleri) aynı olmalıdır.
7. QM2üzerinde, aşağıdaki örnek gibi bir komut yayınlayarak bir alıcı kanalı tanımlayın:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
   ```

   Kanal, adım 6 'da tanımladığınız gönderici kanalıyla aynı ada sahip olmalı ve aynı CipherSpec' i kullanmalıdır.
8. Kanalı başlatın).

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 14 sayfa 201içinde gösterildiği gibi oluşturulur

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıktı aşağıdaki örneklerde gösterilen şekilde benzerdir.

Kuyruk yöneticisinden QM1, şu komutu girin:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

QM2kuyruk yöneticisinden şu komutu girin:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Her durumda, SSLPEER değeri, Adım 2 'de oluşturulan ortak sertifikadaki DN ' nin değeriyle eşleşmelidir. Sertifika, kendinden onaylı bir sertifika olduğu için, eşdüzey adıyla ilgili üreticiler adı da eşleşir.

SSLPEER isteğe bağlıdır. Belirtilirse, bu değer, ortak sertifikadaki DN ' nin (adım 2 'de oluşturulmuş) olmasına izin verileceği şekilde ayarlanmalıdır. SSLPEER kullanımına ilişkin ek bilgi için WebSphere MQ for SSLPEER değerleri ile ilgili kurallar konusuna bakın.

İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması

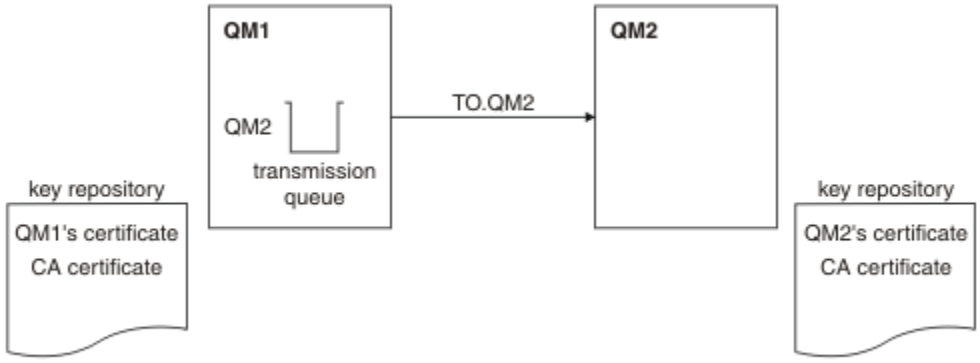
CA imzalı SSL ya da TLS sertifikalarını kullanarak iki kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Güvenli iletişim kurması gereken QMA ve QMB adlı iki kuyruk yöneticiniz var. QMA ile QMB arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Gelecekte bu ağı bir üretim ortamında kullanmayı planlıyorsunuz, bu nedenle CA-imzalı sertifikalarını baştan kullanmaya karar verdiniz.

Sonuçtaki yapılanış şöyle görünür:



Şekil 15. Bu görevle sonuçlanan yapılandırma

Şekil 15 sayfa 203' de, QMA için anahtar havuzu, QMA sertifikası ve CA sertifikası içerir. QMB için anahtar havuzu, QMMB ' nin sertifikasını ve CA sertifikasını içerir. Bu örnekte, hem QMA sertifikasının hem de QMB ' nin sertifikasının aynı CA tarafından yayınlandığı ifade edildi. QMA sertifikasına ve QMB 'nin sertifikasına farklı CA' lar tarafından verildiyse, QMA ve QMB ' ye ilişkin temel havuzlar hem CA sertifikalarını içermelidir.

Yordam

1. Her kuyruk yöneticisine ilişkin anahtar havuzunu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. Her kuyruk yöneticisi için sertifika yetkilisi tarafından imzalanmış bir sertifika isteyin.
   İki kuyruk yöneticisi için farklı CA ' lar kullanabilirsiniz.
   - UNIX, Linuxve Windows sistemlerinde.
3. Her kuyruk yöneticisi için sertifika kuruluşu sertifikasını anahtar havuzuna ekleyin:
   Kuyruk yöneticileri farklı Sertifika Yetkilileri kullanıyorsa, her bir Sertifika Yetkilisi için CA sertifikasının her iki anahtar havuzuna da eklenmesi gerekir.
   - UNIX, Linuxve Windows sistemlerinde.
4. CA imzalı sertifikayı her kuyruk yöneticisi için anahtar havuzuna ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
5. QMA ' da, aşağıdaki örnek gibi komutları girerek bir gönderen kanalı ve ilişkili iletim kuyruğu tanımlayın:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
   SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

   DEFINE QLOCAL(QMB) USAGE(XMITQ)
   ```

   Bu örnek, CipherSpec RC4_MD5' i kullanır. Kanalın her bir ucundaki CipherSpecs (şifreleme Belirtimleri) aynı olmalıdır.
6. QMB ' de, aşağıdaki örnek gibi bir komut kanalı girerek bir alıcı kanalı tanımlayın:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
   ```

   Kanal, adım 6 'da tanımladığınız gönderici kanalıyla aynı ada sahip olmalı ve aynı CipherSpec' i kullanmalıdır.
7. Kanalı başlatın:

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 15 sayfa 203içinde gösterildiği gibi oluşturulur.

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıkış aşağıdaki örneklerde gösterilmeye benzer.

Kuyruk yöneticisi QMA ' dan şu komutu girin:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

Kuyruk yöneticisi QMB ' den şu komutu girin:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Her durumda, SSLPEER değeri, Adım 2 'de oluşturulan ortak sertifikadaki Ayırt Edici Ad (DN) ile eşleşmelidir. Sertifika veren adı, 4. adımda eklenen kişisel sertifikayı imzalayan CA sertifikasının konu DN 'si ile eşleşir.

Tek yönlü kimlik doğrulaması kullanarak iki kuyruk yöneticisinin bağlanması

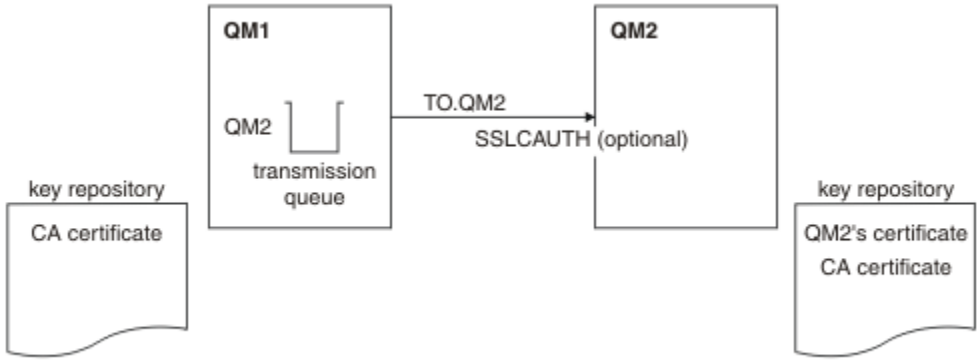
Bir kuyruk yöneticisinin, SSL ya da TLS istemcisi bir sertifika göndermediği durumlarda, bir kuyruk yöneticisinin diğerine tek yönlü kimlik doğrulamasını kullanarak bağlanmasını sağlamak üzere, bir sistemi karşılıklı kimlik doğrulamasıyla değiştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- İki kuyruk yöneticiniz (QM1 ve QM2), “İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması” sayfa 202içinde olduğu gibi ayarlanmıştır.
- You want to change QM1 so that it connects using one-way authentication to QM2.

Sonuçtaki yapılanış şöyle görünür:



Şekil 16. Tek yönlü kimlik doğrulaması sağlayan kuyruk yöneticileri

Yordam

1. QM1' in kişisel sertifikasını, işletim sistemine göre, anahtar havuzundan kaldırın:
   - UNIX, Linuxve Windows sistemlerinde. Sertifika aşağıdaki gibi etiketlenir:
     - `ibmwebspheremq` , ardından kuyruk yöneticinizin adı küçük harfe katlandı. Örneğin, `QM1` için, `ibmwebspheremqqm1`.
2. İsteğe bağlı: QM1' ta, herhangi bir SSL ya da TLS kanalı önceden çalıştırıldıysa, SSL ya da TLS ortamını yenileyin.
3. Alıcıdaki anonim bağlantılara izin ver.

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 16 sayfa 205içinde gösterildiği gibi değiştirilir.

Sonraki adım

Gönderen kanalı çalışıyorsa ve REFRESH SECURITY TYPE (SSL) komutunu verdiyseniz (adım 2 'de) kanal otomatik olarak yeniden başlatılır. Gönderen kanalı çalışmadıysa, başlatın.

Kanalın sunucu ucunda, kanal durumu görüntüsünde eş adı parametre değerinin bulunması, bir istemci sertifikasının akıp geçeceğini gösterir.

Bazı DISPLAY komutları yayınlayarak, görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıktı aşağıdaki örneklerde gösterilen şekilde benzerdir:

QM1 kuyruk yöneticisinden şu komutu girin:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Sonuç çıkışı aşağıdaki örneğe benzer olacaktır:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

QM2 kuyruk yöneticisinden şu komutu girin:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Sonuç çıkışı aşağıdaki örneğe benzer olacaktır:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)                            SSLCERTI( )
   SSLPEER( )                              STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       XMITQ( )
```

QM2'ta SSLPEER alanı boş, QM1 ' un sertifika göndermediğini gösterir. QM1üzerinde, SSLPEER değeri, QM2'in kişisel sertifikasındaki DN' nin değeriyle eşleşir.

İstemcinin kuyruk yöneticisine güvenli bir şekilde bağlanması

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 edinmeniz ve yönetmeniz gerekir. Bir sınama sisteminde, kendinden imzalı sertifikaları ya da yerel bir sertifika yetkilisi (CA) tarafından verilen sertifikaları kullanabilirsiniz. Bir üretim sisteminde kendinden onaylı sertifikalar kullanmayın. Daha fazla bilgi için bkz. ..//zs14140_.dita.

Sertifika oluşturma ve yönetme hakkında tam bilgi edinmek için bkz. “UNIX, Linux, and Windows sistemlerinde SSL ya da TLS ile çalışma” sayfa 111.

Bu konular grubu, SSL iletişimini ayarlarken yer alan 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. WebSphere MQ somutlaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

UNIX, Linux, and Windows sistemlerinde, SSL ya da TLS istemcisi yalnızca doğru WebSphere MQ biçiminde bir etiketi varsa, bu sertifikayı gönderir; `ibmwebspheremq` ise, oturum açma kullanıcı kimliğiniz küçük harfe çevrilir (örneğin, `ibmwebspheremqmyuserid`).

WebSphere MQ , diğer ürünlere ilişkin sertifikalarla 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 işlev gören kanalın sonuna SSLCAUTH parametresiyle ya da bir SSLPEER parametre değeri kümesine ayarlı olarak tanımlandıysa başarısız olur. Kuyruk yöneticisini anonim olarak bağlamaya ilişkin daha fazla bilgi için bkz. “İstemcinin kuyruk yöneticisine anonim olarak bağlanması” sayfa 210.

İstemci ve kuyruk yöneticisinin karşılıklı kimlik doğrulaması için kendinden onaylı sertifikaların kullanılması

Kendinden onaylı SSL ya da TLS sertifikalarını kullanarak, bir istemci ile kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

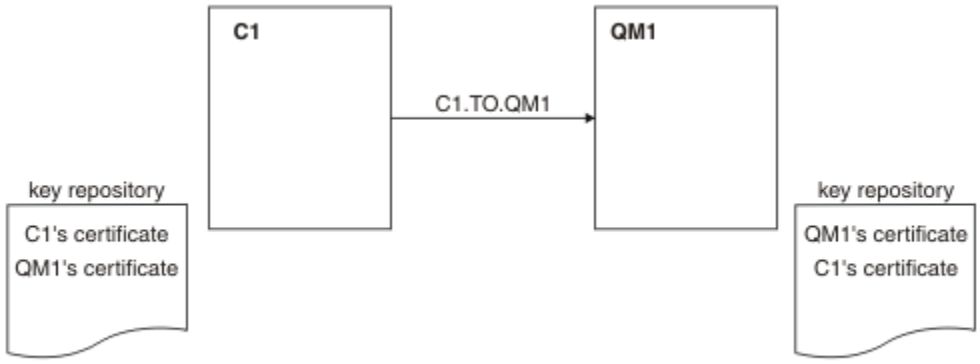
Bu görev hakkında

Senaryo:

- Güvenli bir şekilde iletişim kurulması gereken bir istemci, C1ve kuyruk yöneticisi (QM1) var. C1 ve QM1arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Kendinden onaylı sertifikalar kullanarak güvenli iletişiminizi test etme kararı aldınız.

IBM i üzerindeki DCM, kendinden onaylı sertifikaları desteklemez, bu nedenle bu görev IBM i sistemlerinde geçerli değildir.

Sonuçtaki yapılanış şöyle görünür:



Şekil 17. Bu görevle sonuçlanan yapılandırma

Şekil 17 sayfa 207'ta, QM1 için anahtar havuzu, QM1 sertifikasını ve C1' den genel sertifikayı içerir. C1 için anahtar havuzu, C1 sertifikasını ve QM1' den genel sertifikayı içerir.

Yordam

1. İstemci ve kuyruk yöneticisine ilişkin anahtar havuzu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. İstemci ve kuyruk yöneticisi için kendinden onaylı sertifikalar yarat:
   - UNIX, Linuxve Windows sistemlerinde.
3. Her sertifikana ilişkin bir kopyasını çıkarın:
   - UNIX, Linuxve Windows sistemlerinde.
4. Transfer the public part of the C1 certificate to the QM1 system and vice versa, using a utility such as FTP.
5. İş ortağı sertifikasını istemci ve kuyruk yöneticisi için anahtar havuzuna ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
6. Kuyruk yöneticisininde REFRESH SECURITY TYPE (SSL) komutunu verin.
7. İstemci-bağlantı kanalını aşağıdaki yöntemlerden biriyle tanımlayın:
   - Using the MQCONNX call with the MQSCO structure on C1, as described in WebSphere MQ MQI istemcisinde istemci-bağlantı kanalı yaratılması.
   - Using a client channel definition table, as described in Sunucuda sunucu bağlantısı ve istemci-bağlantı tanımları yaratılması .
8. QM1' ta, bir sunucu bağlantısı kanalı tanımlayın; örneğin, aşağıdaki örneğin gibi bir komut yayınlayın:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanal, adım 6 'da tanımladığınız istemci-bağlantı kanalıyla aynı adı ve aynı CipherSpec' u kullanmalıdır.

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 17 sayfa 207içinde gösterildiği gibi oluşturulur

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıktı aşağıdaki örnekte gösterilen çıkışa benzerdir.

Kuyruk yöneticisinden QM1, şu komutu girin:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Kanal tanımlamalarının SSLPEER süzgeç özniteliğini ayarlamaya isteğe bağlıdır. Kanal tanımlaması SSLPEER ayarlıysa, değerinin Adım 2 'de oluşturulan ortak sertifikadaki konu DN ' iyle eşleşmesi gerekir. Başarılı bir bağlantıdan sonra, DISPLAY CHSTATUS çıkışındaki SSLPEER alanı, uzak istemci sertifikasının konu ayırt edici adını (DN) gösterir.

İstemci ve kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması

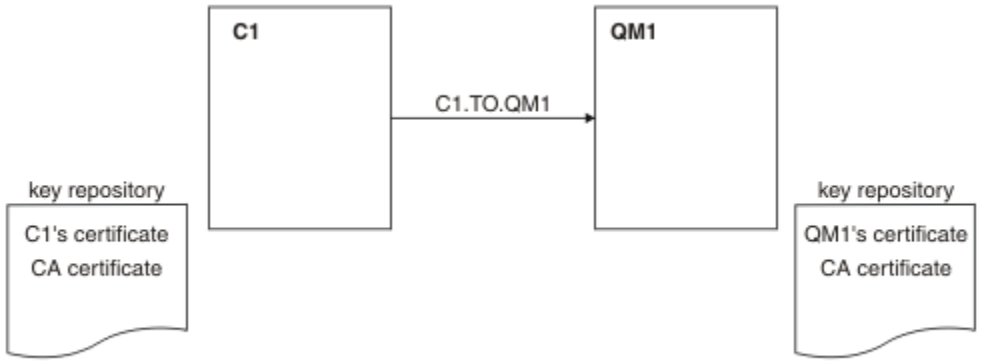
CA imzalı SSL ya da TLS sertifikalarını kullanarak, bir istemci ile kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Güvenli bir şekilde iletişim kurulması gereken bir istemci, C1ve kuyruk yöneticisi (QM1) var. C1 ve QM1arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Gelecekte bu ağı bir üretim ortamında kullanmayı planlıyorsunuz, bu nedenle CA-imzalı sertifikalarını baştan kullanmaya karar verdiniz.

Sonuçtaki yapılanış şöyle görünür:



Şekil 18. Bu görevle sonuçlanan yapılandırma

Şekil 18 sayfa 208' ta, C1 için anahtar havuzu C1 ve CA sertifikasına ilişkin sertifika içerir. QM1 için anahtar havuzu, QM1 sertifikasının ve CA sertifikasının bulunduğunu içerir. Bu örnekte hem C1'in

sertifikası, hem de QM1' in sertifikası aynı CA tarafından yayınlandı. C1'in sertifikası ve QM1' in sertifikası farklı CA ' lar tarafından verildiyse, C1 ve QM1 için anahtar havuzları hem CA sertifikalarını içermeli.

Yordam

1. İstemci ve kuyruk yöneticisine ilişkin anahtar havuzu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. İstemci ve kuyruk yöneticisi için sertifika yetkilisi tarafından imzalanmış bir sertifika isteyin.
   İstemci ve kuyruk yöneticisi için farklı CA ' lar kullanabilirsiniz.
   - UNIX, Linuxve Windows sistemlerinde.
3. Sertifika yetkilisi sertifikasını istemci ve kuyruk yöneticisi için anahtar havuzuna ekleyin.
   İstemci ve kuyruk yöneticisi farklı Sertifika Yetkilileri kullanıyorsa, her bir Sertifika Yetkilisi için CA sertifikasının her iki anahtar havuzuna da eklenmesi gerekir.
   - UNIX, Linuxve Windows sistemlerinde.
4. İstemcinin ve kuyruk yöneticisinin anahtar havuzuna CA imzalı sertifikayı ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
5. İstemci-bağlantı kanalını aşağıdaki yöntemlerden biriyle tanımlayın:
   - Using the MQCONNX call with the MQSCO structure on C1, as described in WebSphere MQ MQI istemcisinde istemci-bağlantı kanalı yaratılması.
   - Using a client channel definition table, as described in Sunucuda sunucu bağlantısı ve istemci-bağlantı tanımları yaratılması .
6. QM1üzerinde, aşağıdaki örnek gibi bir komut vererek bir sunucu bağlantı kanalı tanımlayın:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanal, adım 6 'da tanımladığınız istemci-bağlantı kanalıyla aynı adı ve aynı CipherSpec' u kullanmalıdır.

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 18 sayfa 208içinde gösterildiği gibi oluşturulur.

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, sonuç çıkışı aşağıdaki örnekte gösterildiği gibi olur.

Kuyruk yöneticisinden (QM1) aşağıdaki komutu girin:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

DISPLAY CHSTATUS çıkışındaki SSLPEER alanı, Adım 2 'de yaratılan uzak istemci sertifikasının konu DN değerini gösterir. Sertifika veren adı, 4. adımda eklenen kişisel sertifikayı imzalayan CA sertifikasının konu DN 'si ile eşleşir.

İstemcinin kuyruk yöneticisine anonim olarak bağlanması

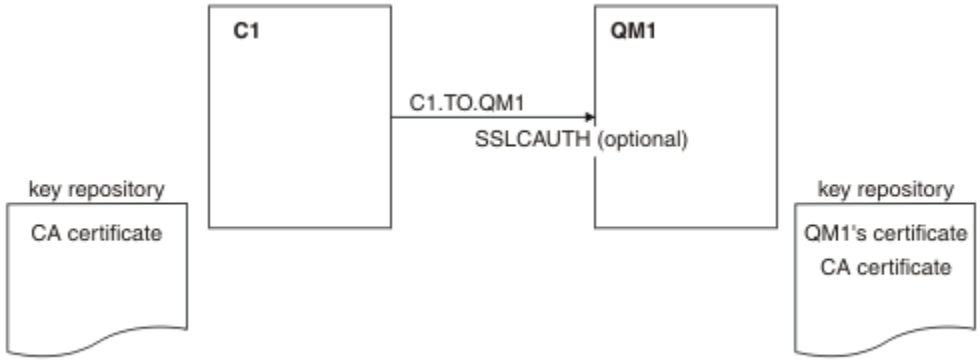
Bir kuyruk yöneticisinin anonim olarak başka bir kuyruk yöneticisine bağlanmasına izin vermek üzere karşılıklı kimlik doğrulama içeren bir sistemi değiştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Kuyruk yöneticinizin ve istemcinizin (QM1 ve C1), “İstemci ve kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması” sayfa 208içinde olduğu gibi ayarlanmıştır.
- C1 'yi anonim olarak QM1' e bağlanmasını istiyorsanız,change' i değiştirmek istiyorsunuz.

Sonuçtaki yapılanış şöyle görünür:



Şekil 19. Anonim bağlantıya izin veren istemci ve kuyruk yöneticisi

Yordam

1. Kişisel sertifikayı, işletim sistemine göre C1için anahtar havuzundan kaldırın:
   - UNIX, Linuxve Windows sistemlerinde. Sertifika aşağıdaki gibi etiketlenir:
     - `ibmwebspheremq` , ardından oturum açma kullanıcı kimliğiniz küçük harfe (örneğin, `ibmwebspheremqmyuserid`) katlandı.
2. İstemci uygulamasını yeniden başlatın ya da istemci uygulamasının tüm SSL ya da TLS bağlantılarını kapatmasına ve yeniden açmasına neden olur.
3. Aşağıdaki komutu girerek, kuyruk yöneticiside anonim bağlantılara izin ver:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 19 sayfa 210içinde gösterildiği gibi değiştirilir.

Sonraki adım

Kanalın sunucu ucunda, kanal durumu görüntüsünde eş adı parametre değerinin bulunması, bir istemci sertifikasının akıp geçeceğini gösterir.

Bazı DISPLAY komutları yayınlayarak, görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıkış aşağıdaki örnekteki gibi gösterilmeye benzer:

Kuyruk yöneticisinden QM1, şu komutu girin:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Sonuç çıkışı aşağıdaki örneğe benzer olacaktır:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

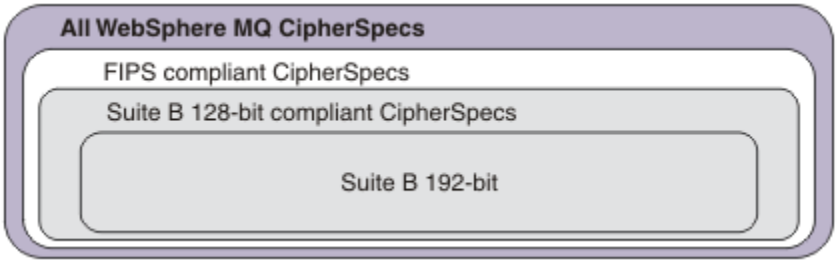
SSLCERTI ve SSLPEER alanları boş, C1 ' in sertifika göndermediğini gösterir.

CipherSpecs ' nin Belirtilmesi

DEFINE CHANNEL MQSC komutunda ya da **ALTER CHANNEL** MQSC komutunda **SSLCIPH** değiştirgesini kullanarak CipherSpec belirtin.

IBM WebSphere MQ ile kullanabileceğiniz CipherSpecs ' in bazıları FIPS uyumludur. NULL_MD5gibi diğerleri değildir. Benzer şekilde, bazı FIPS uyumlu CipherSpecs de Suite B uyumludur, ancak diğerleri uyumludur. Tüm Suite B uyumlu CipherSpecs de 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 çizge, bu altkümeler arasındaki ilişkiyi gösterir:



IBM WebSphere MQ SSL ve TLS desteği ile kullanabileceğiniz şifre belirtimleri aşağıdaki tabloda listelenmiştir. Kişisel sertifika isteğinde bulunduğunuzda, genel ve özel anahtar çifti için bir anahtar boyutu belirtirsiniz. SSL el sıkışması sırasında kullanılan anahtar boyutu, çizelgede belirtildiği şekilde CipherSpectarafından belirlenmedikçe sertifikada saklanan boyuttur.

CipherSpec adı	Kullanılan protokol	MAC algoritması	Şifreleme Algoritması	Şifreleme bitleri	FIPS[1]	Suite B 128 bit	Takım B 192 bit
NULL_MD5 [a]	SSL 3.0	MD5	Yok	0	Hayır	Hayır	Hayır
NULL_SHA [a]	SSL 3.0	SHA-1	Yok	0	Hayır	Hayır	Hayır
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Hayır	Hayır	Hayır
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Hayır	Hayır	Hayır
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Hayır	Hayır	Hayır
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Hayır	Hayır	Hayır

CipherSpec adı	Kullanılan protokol	MAC algoritması	Şifreleme Algoritması	Şifreleme bitleri	FIPS[1]	Suite B 128 bit	Takım B 192 bit
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Hayır	Hayır	Hayır
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Hayır	Hayır	Hayır
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Hayır	Hayır	Hayır
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES.	128	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES.	256	Evet	Hayır	Hayır
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	[5] yok	Hayır	Hayır
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Hayır[6]	Hayır	Hayır
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES.	128	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES.	256	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	128	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	256	Evet	Hayır	Hayır
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	Hayır
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Hayır	Hayır	Hayır
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	128	Evet	Hayır	Hayır
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES.	256	Evet	Hayır	Hayır
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	128	Evet	Hayır	Hayır
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES.	256	Evet	Hayır	Hayır
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES.	128	Evet	Evet	Hayır
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES.	256	Evet	Hayır	Evet

CipherSpec adı	Kullanılan protokol	MAC algoritması	Şifreleme Algoritması	Şifreleme bitleri	FIPS[1]	Suite B 128 bit	Takım B 192 bit
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES.	128	Evet	Hayır	Hayır
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES.	256	Evet	Hayır	Hayır
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Yok	0	Hayır	Hayır	Hayır
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Yok	0	Hayır	Hayır	Hayır
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Yok	0	Hayır	Hayır	Hayır
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Yok	Yok	0	Hayır	Hayır	Hayır
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	Hayır

Notlar:

1. CipherSpec ' in FIPS onaylı bir platformda FIPS onaylı olup olmadığını belirtir. FIPS ' ye ilişkin açıklamalar için bkz. Federal Information Processing Standards (FIPS) .
2. 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.
3. Tokalaşma anahtarı boyutu 1024 bittir.
4. Bu CipherSpec , Explorer tarafından kullanılan JRE ' ye uygun kısıtlamasız ilke dosyaları uygulanmadıkça, WebSphere MQ Explorer 'dan bir kuyruk yöneticisine bağlantı güvenli kılmak için kullanılamaz.
5. Bu CipherSpec , 19 Mayıs 2007 'den önce FIPS 140-2 sertifikalıydı.
6. 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.
7. Bu CipherSpec , bağlantı AMQ9288hatasıyla sonlandırılmadan önce 32 GB ' ye kadar veri aktarmak için kullanılabilir. Bu hatayı önlemek için üçlü DES kullanmaktan kaçının ya da bu CipherSpec' i kullanırken gizli anahtar sıfırlamasını etkinleştirin.

Platform desteği:

- a Desteklenen tüm platformlarda kullanılabilir.
- b Yalnızca UNIX, Linux, and Windows platformlarında kullanılabilir.

İlgili kavramlar

“Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33
Bu konuda, IBM WebSphere MQiçindeki CipherSpecs ve dijital sertifikalar arasındaki ilişkiyi sıralayarak uygun CipherSpecs ve güvenlik ilkeniz için dijital sertifikalar nasıl seçileceği hakkında bilgi sağlanmaktadır.

İlgili başvurular

KANAL TANıMLAYıN
KANAL DEğIşTIR

Kullanımdan kaldırılan CipherSpecs

A list of deprecated CipherSpecs that you are able to use with WebSphere MQ if necessary.

Kullanımdan kaldırılan CipherSpecs' ı nasıl etkinleştirebileceğiyle ilgili daha fazla bilgi için bkz. “IBM WebSphere MQiçinde desteklenenCipherSpec değerleri” sayfa 38 .

WebSphere MQ TLS desteği ile kullanabileceğiniz kullanımdan kaldırılan CipherSpecs , aşağıdaki tabloda listelenir:

Platform desteği “1” sayfa 216	CipherSpec adı	Kullanılan iletişim kuralı	Veri bütünlüğü	Şifreleme Algoritması	Şifreleme bitleri	FIPS “2” sayfa 216	Takım B	Kullanımdan kaldırıldığında güncelle
Tümü	DES_SHA_EXPORT“3” sayfa 216	SSL 3.0	SHA-1	DES	56	Hayır	Hayır	7.5.0.6
UNIX Linux Windows	DES_SHA_EXPORT1024“4” sayfa 216	SSL 3.0	SHA-1	DES	56	Hayır	Hayır	7.5.0.6
UNIX Linux Windows	FIPS_WITH_DES_CBC_SHA	SSL 3.0	SHA-1	DES	56	Hayır “6” sayfa 216	Hayır	7.5.0.6
UNIX Linux Windows	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	SHA-1	3DES	168	Hayır “7” sayfa 216	Hayır	7.5.0.8
Tümü	NULL_MD5	SSL 3.0	MD5	Yok	0	Hayır	Hayır	7.5.0.6
Tümü	NULL_SHA	SSL 3.0	SHA-1	Yok	0	Hayır	Hayır	7.5.0.6
Tümü	RC2_MD5_EXPORT“3” sayfa 216	SSL 3.0	MD5	RC2	40	Hayır	Hayır	7.5.0.7
Tümü	RC4_MD5_EXPORT“3” sayfa 216	SSL 3.0	MD5	RC4	40	Hayır	Hayır	7.5.0.7
Tümü	RC4_MD5_US	SSL 3.0	MD5	RC4	128	Hayır	Hayır	7.5.0.7
Tümü	RC4_SHA_US	SSL 3.0	SHA-1	RC4	128	Hayır	Hayır	7.5.0.7
UNIX Linux Windows	RC4_56_SHA_EXPORT1024“4” sayfa 216	SSL 3.0	SHA-1	RC4	56	Hayır	Hayır	7.5.0.7
Tümü	TRIPLE_DES_SHA_US	SSL 3.0	SHA-1	3DES	168	Hayır	Hayır	7.5.0.8
Tümü	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	SHA-1	DES	56	Hayır “5” sayfa 216	Hayır	7.5.0.6
UNIX Linux Windows	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	SHA-1	Yok	0	Hayır	Hayır	7.5.0.6

Platform desteği “1” sayfa 216	CipherSpec adı	Kullanılan iletişim kuralı	Veri bütünlüğü	Şifreleme Algoritması	Şifreleme bitleri	FIPS “2” sayfa 216	Takım B	Kullanımdan kaldırıldığında güncelle
UNIX Linux Windows	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	7.5.0.7
UNIX Linux Windows	ECDHE_RSA_NULL_SHA256	TLS 1.2	SHA-1	Yok	0	Hayır	Hayır	7.5.0.6
UNIX Linux Windows	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	7.5.0.7
UNIX Linux Windows	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Yok	Yok	0	Hayır	Hayır	7.5.0.6
Tümü	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	SHA-256	Yok	0	Hayır	Hayır	7.5.0.6
UNIX Linux Windows	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	7.5.0.7
Tümü	TLS_RSA_WITH_3DES_EDE_CBC_SHA“8” sayfa 216	TLS 1.0	SHA-1	3DES	168	Evet	Hayır	7.5.0.8
UNIX Linux Windows	ECDHE_ECDSA_3DES_EDE_CBC_SHA256“8” sayfa 216	TLS 1.2	SHA-1	3DES	168	Evet	Hayır	7.5.0.8
UNIX Linux Windows	ECDHE_RSA_3DES_EDE_CBC_SHA256“8” sayfa 216	TLS 1.2	SHA-1	3DES	168	Evet	Hayır	7.5.0.8

Platform desteği “1” sayfa 216	CipherSpec adı	Kullanılan iletişim kuralı	Veri bütünlüğü	Şifreleme Algoritması	Şifreleme bitleri	FIPS “2” sayfa 216	Takım B	Kullanımdan kaldırıldığında güncelle

Notlar:

1. Belirli bir altyapı belirtilmiyorsa, CipherSpec tüm platformlarda kullanılabilir.
2. CipherSpec ' in FIPS onaylı bir altyapıda FIPS onaylı olup olmadığını belirtir. FIPS ' ye ilişkin açıklamalar için Federal Information Processing Standards (FIPS) belgesine bakın.
3. El sıkışma anahtarı büyüklüğü üst sınırı 512 bittir. SSL anlaşması sırasında değiş tokuş edilen sertifikalardan biri 512 bitden büyük bir anahtar boyutuna sahipse, el sıkışma sırasında kullanılmak üzere geçici bir 512 bit anahtar oluşturulur.
4. Tokalaşma anahtarı boyutu 1024 bit 'dir.
5. Bu CipherSpec , 19 Mayıs 2007 tarihinden önce FIPS 140-2 sertifikasına sahiptir.
6. Bu CipherSpec , 19 Mayıs 2007 tarihinden önce FIPS 140-2 sertifikasına sahiptir. The name `FIPS_WITH_DES_CBC_SHA` is historical and reflects the fact that this CipherSpec was previously (but is no longer) FIPS-compliant. Bu CipherSpec kullanımdan kaldırıldı ve kullanımı önerilmiyor.
7. The name `FIPS_WITH_3DES_EDE_CBC_SHA` is historical and reflects the fact that this CipherSpec was previously (but is no longer) FIPS-compliant. Bu CipherSpec kullanımı kullanımdan kaldırılmıştır.
8. This CipherSpec can be used to transfer up to 32 GB of data before the connection is terminated with error AMQ9288. Bu hatayı önlemek için, üçlü DES kullanmaktan kaçının ya da bu CipherSpeckomutunu kullanırken gizli anahtar sıfırlamayı etkinleştirin.

IBM WebSphere MQ Explorerkullanılarak CipherSpecs hakkında bilgi edinme

CipherSpecs' in açıklamalarını görüntülemek için IBM WebSphere MQ Explorer olanağını kullanabilirsiniz.

“CipherSpecs ' nin Belirtilmesi” sayfa 211içindeki CipherSpecs ile ilgili bilgi edinmek için aşağıdaki yordamı kullanın:

1. **IBM WebSphere MQ Explorer** ' ı 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.

CipherSpecs belirtilerek ilgili alternatifler

İşletim sisteminin SSL desteğini sağladığı bu platformlar için, sisteminiz yeni CipherSpecsözelliğini destekleyebilir. SSLCIPH parametresiyle yeni bir CipherSpec belirtebilirsiniz, ancak sağladığınız değer altyapınıza bağlıdır.

Not: CipherSpecs , WebSphere MQ ürünüyle birlikte sağlandığından bu bölüm UNIX, Linux ya da Windows sistemleri için geçerli değildir; bu nedenle yeni CipherSpecs , sevkiyattan sonra kullanılamaz.

İşletim sisteminin SSL desteğini sağladığı platformlarda, sisteminiz “CipherSpecs ' nin Belirtilmesi” sayfa 211içinde bulunmayan yeni CipherSpecs ' i destekleyebilir. SSLCIPH parametresiyle yeni bir CipherSpec belirtebilirsiniz, ancak sağladığınız değer altyapınıza bağlıdır. Her durumda belirtim, sisteminizin çalıştırdığı SSL sürümü tarafından hem geçerli hem de desteklenen bir SSL CipherSpec belirtimine karşılık *gelmelidir* .

IBM i
Onaltılı bir değeri gösteren iki karakterli bir dizgi.

İzin verilen değerlerle ilgili ek bilgi için uygun ürün belgelerine bakın (IBM i ürün belgelerinde *cipher_spec* öğesini arayın).

Değeri belirlemek için CHGMQMCHL ya da CRTMQMCHL komutunu kullanabilirsiniz; örneğin:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

SSLCIPH değiştirgesini ayarlamak için ALTER QMGR MQSC komutunu da kullanabilirsiniz.

z/OS
Onaltılı bir değeri gösteren iki karakterli bir dizgi. Onaltılı kodlar, SSL protokolünde tanımlanan değerlere karşılık gelir.

Daha fazla bilgi için, *z/OS Cryptographic Services System SSL Programming*, SC24-5901' in API başvuru bölümündeki gsk_environment_open () açıklamasına bakın; burada desteklenen tüm SSL V3.0 ve TLS V1.0 şifre belirtimlerinin bir listesi 2 basamaklı onaltılı kodlar biçiminde bulunur.

WebSphere MQ kümeleri için dikkat edilecek noktalar

WebSphere MQ kümeleriyle “CipherSpecs ' nin Belirtilmesi” sayfa 211içindeki CipherSpec adlarını kullanmak en güvenlidir. Alternatif bir belirtim kullanıyorsanız, belirtimin diğer platformlarda geçerli olmayabileceğini unutmayın. Daha fazla bilgi için bkz. “SSL ve kümeler” sayfa 242.

IBM WebSphere MQ MQI istemcisi için bir CipherSpec belirtme

Bir IBM WebSphere MQ MQI istemcisi için bir CipherSpec belirtme 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.
- Using the Active Directory (on Pencereler systems with Active Directory support)

Java için IBM WebSphere MQ sınıfları ve JMS için IBM WebSphere MQ sınıfları içeren bir CipherSuite belirtilmesini

JMS içinIBM WebSphere MQ sınıfları ve JMS için IBM WebSphere MQ sınıfları, diğer altyapılardan farklı CipherSuites değerlerini belirtir.

Java için IBM WebSphere MQ sınıflarıyla bir CipherSuite belirtilmesine ilişkin bilgi edinmek için bkz. Secure Sockets Layer (SSL) support.

JMS için IBM WebSphere MQ sınıflarıyla CipherSuite belirtilmesine ilişkin bilgi için bkz. JMS için WebSphere MQ sınıflarıyla SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) kullanılıyor.

SSL ve TLS gizli anahtarlarının ilk durumuna getirilmesi

IBM WebSphere MQ , kuyruk yöneticilerinde ve istemcilerde gizli anahtarların sıfırlanmasını destekler.

Kanal boyunca ya da kanal bir süre boşta durduktan sonra, gizli anahtarlar, belirtilen sayıda şifrelenmiş veri baytı akışı olduğunda ilk durumuna getirilir.

Anahtar ilk duruma getirme değeri her zaman MQ kanalınının başlangıç tarafına ayarlanır.

Kuyruk yöneticisi

For a queue manager, use the command **ALTER QMGR** with the parameter **SSLRKEYC** to set the values used during key renegotiation.

MQI istemcisi

Varsayılan olarak, MQI istemcileri gizli anahtarı yeniden müzakere etmiyamaz. Bir MQI istemcisi, anahtarı üç yöntemden herhangi biriyle yeniden görüşebilir. Aşağıdaki listede, yöntemler öncelik sırasına göre gösterilir. Birden çok değer belirtirseniz, en yüksek öncelikli değer kullanılır.

1. MQCONNX çağrısındaki MQSCO yapısındaki KeyResetSayı alanını kullanarak
2. MQSSLRESET ortam değişkenini kullanarak
3. MQI istemcisi yapılanış kütüğündeki SSLKeyResetSayı özniteliği ayarlanarak

Bu değişkenler, SSL ya da TLS gizli anahtarı yeniden anlaşılmadan önce bir SSL ya da TLS etkileşimi içinde gönderilen ve alınan şifrelenmemiş bayt sayısını temsil eden 0-999 999 999 aralığında bir tamsayıya ayarlanabilir. 0 değeri belirtildiğinde, SSL ya da TLS gizli anahtarlarının hiçbir zaman yeniden anlaşma sunulmadığını belirtir. SSL ya da TLS gizli anahtarı sıfırlama sayısı, 1 bayt-32 KB arasında bir değer belirlerseniz, SSL ya da TLS kanalları 32 KB ' lik bir gizli anahtar sıfırlama sayısını kullanır. Bu, küçük SSL ya da TLS gizli anahtar ilk duruma getirme değerleri için oluşacağı aşırı anahtar sıfırlamalarından kaçınmak içindir.

Kanal için sıfırdan büyük bir değer belirtilirse ve kanal kalp atışları kanal için etkinleştirilirse, ileti verileri gönderilmeden ya da kanal sağlıklı işletim bildirimi sonrasında alınmadan önce gizli anahtar da yeniden görüşilir.

Her başarılı yeniden görüşmeden sonra bir sonraki gizli anahtar yeniden müzakere edilinceye kadar bayt sayısı sıfırlanır.

MQSCO yapısının tam ayrıntıları için bkz. KeyResetCount (MQlong). MQSSLRESET ile ilgili tüm ayrıntılar için MQSSLRESETbaşlıklı konuya bakın. İstemci yapılandırma dosyasında SSL ya da TLS kullanımıyla ilgili daha fazla bilgi için İstemci yapılandırma dosyasının SSL stanzasıbaşlıklı konuya bakın.

Java

IBM WebSphere MQ classes for Javaiçin bir uygulama, aşağıdaki yöntemlerden biriyle gizli anahtarı sıfırlayabilir:

- MQEnvironment sınıfındaki sslResetSayı alanını ayarlayarak.
- Bir Hashtable nesnesinde MQC.SSL_RESET_COUNT_PROPERTY ortam özelliği ayarlanarak. Uygulama daha sonra, hashtable 'ı MQEnvironment sınıfındaki `properties` alanına atar ya da hashtable 'ı oluşturucudaki bir MQQueueManager nesnesine geçirir.

Uygulama bu yollardan birden fazla kullanırsa, olağan öncelik kuralları geçerlidir. Öncelik kuralları için bakınız: Class com.ibm.mq.MQEnvironment .

The value of the sslResetCount field or environment property MQC.SSL_RESET_COUNT_PROPERTY represents the total number of bytes sent and received by the WebSphere MQ classes for Java client code before the secret key is renegotiated. Gönderilen bayt sayısı, şifrelemeden önceki sayıdır ve alınan bayt sayısı, şifre çözme işleminden sonra gelen sayıdır. Bayt sayısı, Java istemcisi için WebSphere MQ sınıfları tarafından gönderilen ve alınan denetim bilgilerinin de içerilmesine neden olur.

İlk duruma getirme sayısı sıfırsa, varsayılan değer olan gizli anahtar hiçbir zaman yeniden anlaşılamamaktadır. CipherSuite belirtilmediyse, ilk duruma getirme sayısı dikkate alınmaz.

JMS

IBM WebSphere MQ classes for JMSiçin, SSLRESETCOUNT özelliği, şifreleme için kullanılan gizli anahtardan önce bir bağlantı tarafından gönderilen ve alınan toplam bayt sayısını temsil eder. Gönderilen bayt sayısı, şifrelemeden önceki sayıdır ve alınan bayt sayısı, şifre çözme işleminden sonra gelen sayıdır. Bayt sayısı, IBM WebSphere MQ classes for JMStarafından gönderilen ve alınan denetim bilgilerini de içerir. Örneğin, bir SSL ya da TLS etkin MQI kanalı üzerinden bağlantı yaratmak için kullanılabilecek bir

ConnectionFactory nesnesini yapılandırmak için, 4 MB ' lik veri akıldıktan sonra JMSAdmin komutunu kullanarak aşağıdaki komutu verin:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Varsayılan değer olan SSLRESETCOUNT değeri sıfırsa, gizli anahtar hiçbir zaman yeniden anlaşılamamaktadır. SSLCIPHERSUITE ayarlanmadıysa, SSLRESETCOUNT özelliği yoksayılır.

.NET

.NET yönetilmeyen istemciler için, SSLKeyResetSayı özelliği özelliği, gizli anahtar yeniden anlaşılmadan önce bir SSL ya da TLS etkileşimi içinde gönderilen ve alınan şifrelenmemiş baytların sayısını gösterir.

.NET için IBM WebSphere MQ sınıflarında nesne özelliklerinin kullanımıyla ilgili bilgi edinmek için Öznitelik değerlerini alma ve ayarlamabaşlıklı konuya bakın.

XMS .NET

XMS .NET yönetilmeyen istemciler için IBM WebSphere MQ kuyruk yöneticisine güvenli bağlantılarbaşlıklı konuya bakın.

İlgili başvurular
ALTER QMGR
QMGR GöRüNTüLE

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 219.

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.

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

SSL ya da TLS ' yi kullandığınızda, kuruluştaki veri bütünlüğü düzeyini CipherSpec seçiminiz belirler. WebSphere 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.

SSL ya da TLS kullanarak iki kuyruk yöneticisinin bağlanması

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 edinmeniz ve yönetmeniz gerekir. Bir sınama sisteminde, kendinden imzalı sertifikaları ya da yerel bir sertifika yetkilisi (CA) tarafından verilen sertifikaları kullanabilirsiniz. Bir üretim sisteminde kendinden onaylı sertifikalar kullanmayın. Daha fazla bilgi için bkz. ../zs14140_.dita.

Sertifika oluşturma ve yönetme hakkında tam bilgi edinmek için bkz. “UNIX, Linux, and Windows sistemlerinde SSL ya da TLS ile çalışma” sayfa 111.

Bu konular grubu, SSL iletişimini ayarlarken yer alan 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. WebSphere MQ somutlaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

Notlar:

1. Bu bağlamda, bir SSL istemcisi el sıkışmasını başlatan bağlantıyı belirtir.
2. Ek ayrıntılar için Sözlük ' e bakın.

UNIX, Linux ve Windows sistemlerinde, SSL ya da TLS istemcisi yalnızca, doğru WebSphere MQ biçiminde bir etiketi varsa, bu sertifikayı gönderir; bu da kuyruk yöneticinizin adının küçük harfe çevrilerek `ibmwebspheremq` ' in izlediği bir sertifika olur. Örneğin, `QM1`için, `ibmwebspheremqqm1`.

WebSphere MQ , diğer ürünlere ilişkin sertifikalarla 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 işlev gören kanalın sonuna SSLCAUTH parametresiyle ya da bir SSLPEER parametre değeri kümesine ayarlı olarak tanımlandıysa başarısız olur. Bir kuyruk yöneticisini anonim olarak bağlama hakkında daha fazla bilgi için, SSL ya da TLS istemcisi bir sertifika göndermediği zaman bkz. “Tek yönlü kimlik doğrulaması kullanarak iki kuyruk yöneticisinin bağlanması” sayfa 204.

Dijital sertifika etiketleri, gereksinimleri anlama

Dijital sertifikaları kullanmak için SSL ve TLS ' yi ayarlarken, kullanılan platforma ve bağlanmak için kullandığınız yönteme bağlı olarak, izlemeniz gereken belirli etiket gereksinimleri olabilir.

Bu görev hakkında

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, sertifikana *Konu Ayırt Edici Ad* ya da *Ortak Ortak Ad* alanlarından ayrıdır. *Genel Ayırt Edici Ad* ve *Konu Ortak Adı* ' nın, sertifika içindeki alanlar olduğunu unutmayın. Bu bilgiler, sertifika yaratıldığında tanımlanır ve değiştirilemez. Ancak, gerekirse sayısal bir sertifikan ile ilişkili etiketi değiştirebilirsiniz.

Sertifika etiketi nasıl kullanılır?

IBM WebSphere MQ , SSL 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 etiketleri bir adlandırma kuralını izler; kullanmakta olduğunuz platforma karşılık gelen doğru etiket adlandırma kuralını kullandığınızdan emin olmanız gerekir.

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

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

SSL ya da TLS sunucusu, gönderildiyse istemci sertifikasının her zaman geçerliliğini denetler. İstemci bir sertifika göndermezse, SSL ya da TLS sunucusu olarak hareket eden kanalın sonu, SSLCAUTH parametresiyle ya da REQUIRD ya da SSLPEER parametre değeri ayarına ayarlı olarak tanımlandıysa kimlik doğrulaması başarısız olur.

Tek yönlü kimlik doğrulamasını kullanarak bir kuyruk yöneticisini bağlama hakkında daha fazla bilgi için, SSL ya da TLS istemcisi bir sertifika göndermediği zaman bkz. “Tek yönlü kimlik doğrulaması kullanarak iki kuyruk yöneticisinin bağlanması” sayfa 204.

, UNIX, Linux, and Windows sistemleri

Bu görev hakkında

, UNIX, Linux, and Windows sistemlerinde, SSL ya da TLS sunucusu istemciye bir sertifika gönderir, ancak sunucu doğru IBM WebSphere MQ biçiminde bir etiket bulursa, bu sertifika gönderir. Bu sistemlerde, doğru biçim `ibmwebspheremq`biçimidir ve kuyruk yöneticinizin adı küçük harfe çevrilir.

Örneğin, `QM1`adlı bir kuyruk yöneticisi için, sertifika etiketi gereksinmesi şöyledir:

```
ibmwebspheremqqm1
```

Kuyruk yöneticisinin anahtar havuzunda herhangi bir sertifika bulunamazsa, gerekli etiketle doğru büyük ve küçük bir biçimde eşleştirilirse, bir hata oluşur ve SSL ya da TLS anlaşması başarısız olur.

IBM WebSphere MQ istemci

Bu görev hakkında

Bir IBM WebSphere MQ istemci uygulamasından bağlantı kurulurken, SSL ya da TLS istemcisi yalnızca, `ibmwebspheremq`biçiminde bir etiketi olan bir sertifikasına sahip olduğunda ve ardından istemci uygulaması sürecini çalıştıran kullanıcının kullanıcı adı tarafından bir sertifika gönderir.

Örneğin, `wasadmin`kullanıcı adı için, sertifika etiketi gereksinimi küçük harfe katlanır:

```
   ibmwebspheremqwasadmin
```

Yukarıdaki etiket gereksinimi, C ya da C + + ve .NET için İleti Hizmeti İstemcileri için geçerlidir.

IBM WebSphere MQ Java ya da IBM WebSphere MQ JMS istemcisi

Bu görev hakkında

IBM WebSphere MQ Java ya da IBM WebSphere MQ JMS istemcileri, SSL ya da TLS el sıkışması sırasında kişisel bir sertifika seçmek için Java Secure Socket Extension (JSSE) sağlayıcısının olanaklarını kullanır ve dolayısıyla sertifika etiketi gereksinimlerine tabi değildir.

Varsayılan davranış, JSSE istemcisinin anahtar havuzundaki sertifikalar üzerinden yinelenmesi, bulunan ilk kabul edilebilir kişisel sertifika seçmesi olabilir. 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.

Sorun giderme için ya da IBM WebSphere MQ Java istemcisi uygulamasının özel JSSE sağlayıcısıyla birlikte gerçekleştirdiği el sıkışmayı daha iyi anlamak için, hata ayıklamayı ayarlayarak etkinleştirebilirsiniz.

```
javax.net.debug=ssl
```

(JVM).

Komut satırında `-Djavax.net.debug=ssl` komutunu kullanabilir ya da değişkeni uygulama içinde ya da yapılandırma aracılığıyla ayarlayabilirsiniz.

İlgili kavramlar

“Kişisel bir sertifikin UNIX, Linux, and Windows sistemlerindeki bir anahtar havuzuna aktarılması” sayfa 130

Kişisel bir sertifikayı içe aktarmak için bu yordamı izleyin

İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için kendinden onaylı sertifikaların kullanılması

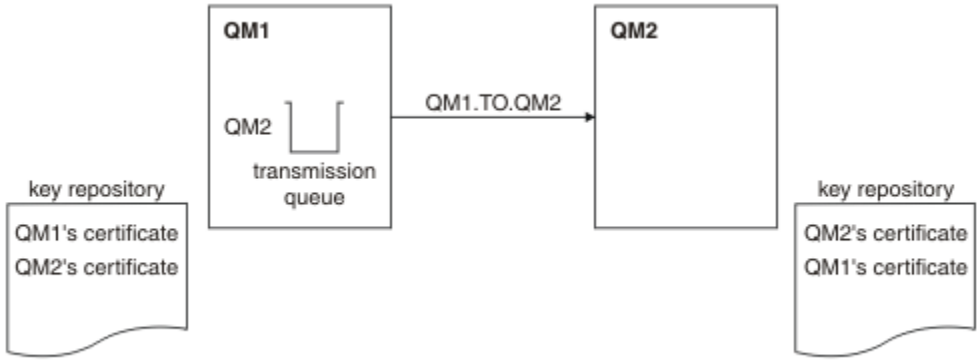
Kendinden onaylı SSL ya da TLS sertifikalarını kullanarak iki kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Güvenli bir şekilde iletişim kurmak zorunda olan iki kuyruk yöneticisi, QM1 ve QM2vardır. QM1 ile QM2arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Kendinden onaylı sertifikalar kullanarak güvenli iletişiminizi test etme kararı aldınız.

Sonuçtaki yapılanış şöyle görünür:



Şekil 20. Bu görevle sonuçlanan yapılandırma

Şekil 14 sayfa 201'ta, QM1 için anahtar havuzu, QM1 sertifikasını ve QM2' den genel sertifikayı içerir. QM2 için anahtar havuzu, QM2 sertifikasını ve QM1' den genel sertifikayı içerir.

Yordam

1. Her kuyruk yöneticisine ilişkin anahtar havuzunu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. Her kuyruk yöneticisi için kendinden onaylı sertifika yarat:
   - UNIX, Linuxve Windows sistemlerinde.
3. Her sertifikana ilişkin bir kopyasını çıkarın:
   - UNIX, Linuxve Windows sistemlerinde.
4. Transfer the public part of the QM1 certificate to the QM2 system and vice versa, using a utility such as FTP.
5. İş ortağı sertifikasını, her kuyruk yöneticisi için anahtar havuzuna ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
6. QM1' ta, aşağıdaki örnek gibi komutlar vererek, bir gönderen kanalı ve ilişkili iletim kuyruğu tanımlayın:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
   SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

   DEFINE QLOCAL(QM2) USAGE(XMITQ)
   ```

   Bu örnek, CipherSpec RC4_MD5' i kullanır. Kanalın her bir ucundaki CipherSpecs (şifreleme Belirtimleri) aynı olmalıdır.
7. QM2üzerinde, aşağıdaki örnek gibi bir komut yayınlayarak bir alıcı kanalı tanımlayın:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
   ```

   Kanal, adım 6 'da tanımladığınız gönderici kanalıyla aynı ada sahip olmalı ve aynı CipherSpec' i kullanmalıdır.
8. Kanalı başlatın).

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 14 sayfa 201içinde gösterildiği gibi oluşturulur

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıktı aşağıdaki örneklerde gösterilen şekilde benzerdir.

Kuyruk yöneticisinden QM1, şu komutu girin:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

QM2kuyruk yöneticisinden şu komutu girin:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Her durumda, SSLPEER değeri, Adım 2 'de oluşturulan ortak sertifikadaki DN ' nin değeriyle eşleşmelidir. Sertifika, kendinden onaylı bir sertifika olduğu için, eşdüzey adıyla ilgili üreticiler adı da eşleşir.

SSLPEER isteğe bağlıdır. Belirtilirse, bu değer, ortak sertifikadaki DN ' nin (adım 2 'de oluşturulmuş) olmasına izin verileceği şekilde ayarlanmalıdır. SSLPEER kullanımına ilişkin ek bilgi için WebSphere MQ for SSLPEER değerleri ile ilgili kurallar konusuna bakın.

İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması

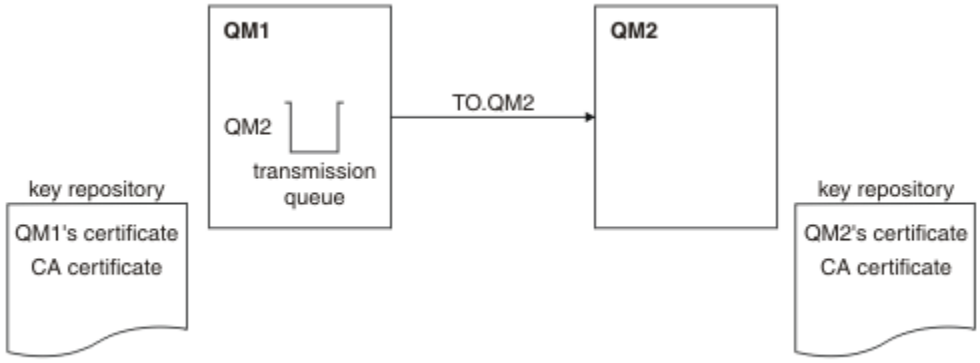
CA imzalı SSL ya da TLS sertifikalarını kullanarak iki kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Güvenli iletişim kurması gereken QMA ve QMB adlı iki kuyruk yöneticiniz var. QMA ile QMB arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Gelecekte bu ağı bir üretim ortamında kullanmayı planlıyorsunuz, bu nedenle CA-imzalı sertifikalarını baştan kullanmaya karar verdiniz.

Sonuçtaki yapılanış şöyle görünür:



Şekil 21. Bu görevle sonuçlanan yapılandırma

Şekil 15 sayfa 203' de, QMA için anahtar havuzu, QMA sertifikası ve CA sertifikası içerir. QMB için anahtar havuzu, QMMB ' nin sertifikasını ve CA sertifikasını içerir. Bu örnekte, hem QMA sertifikasının hem de QMB ' nin sertifikasının aynı CA tarafından yayınlandığı ifade edildi. QMA sertifikasına ve QMB 'nin sertifikasına farklı CA' lar tarafından verildiyse, QMA ve QMB ' ye ilişkin temel havuzlar hem CA sertifikalarını içermelidir.

Yordam

1. Her kuyruk yöneticisine ilişkin anahtar havuzunu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. Her kuyruk yöneticisi için sertifika yetkilisi tarafından imzalanmış bir sertifika isteyin.
   İki kuyruk yöneticisi için farklı CA ' lar kullanabilirsiniz.
   - UNIX, Linuxve Windows sistemlerinde.
3. Her kuyruk yöneticisi için sertifika kuruluşu sertifikasını anahtar havuzuna ekleyin:
   Kuyruk yöneticileri farklı Sertifika Yetkilileri kullanıyorsa, her bir Sertifika Yetkilisi için CA sertifikasının her iki anahtar havuzuna da eklenmesi gerekir.
   - UNIX, Linuxve Windows sistemlerinde.
4. CA imzalı sertifikayı her kuyruk yöneticisi için anahtar havuzuna ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
5. QMA ' da, aşağıdaki örnek gibi komutları girerek bir gönderen kanalı ve ilişkili iletim kuyruğu tanımlayın:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
   SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

   DEFINE QLOCAL(QMB) USAGE(XMITQ)
   ```

   Bu örnek, CipherSpec RC4_MD5' i kullanır. Kanalın her bir ucundaki CipherSpecs (şifreleme Belirtimleri) aynı olmalıdır.
6. QMB ' de, aşağıdaki örnek gibi bir komut kanalı girerek bir alıcı kanalı tanımlayın:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
   ```

   Kanal, adım 6 'da tanımladığınız gönderici kanalıyla aynı ada sahip olmalı ve aynı CipherSpec' i kullanmalıdır.
7. Kanalı başlatın:

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 15 sayfa 203içinde gösterildiği gibi oluşturulur.

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıkış aşağıdaki örneklerde gösterilmeye benzer.

Kuyruk yöneticisi QMA ' dan şu komutu girin:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

Kuyruk yöneticisi QMB ' den şu komutu girin:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Her durumda, SSLPEER değeri, Adım 2 'de oluşturulan ortak sertifikadaki Ayırt Edici Ad (DN) ile eşleşmelidir. Sertifika veren adı, 4. adımda eklenen kişisel sertifikayı imzalayan CA sertifikasının konu DN 'si ile eşleşir.

Tek yönlü kimlik doğrulaması kullanarak iki kuyruk yöneticisinin bağlanması

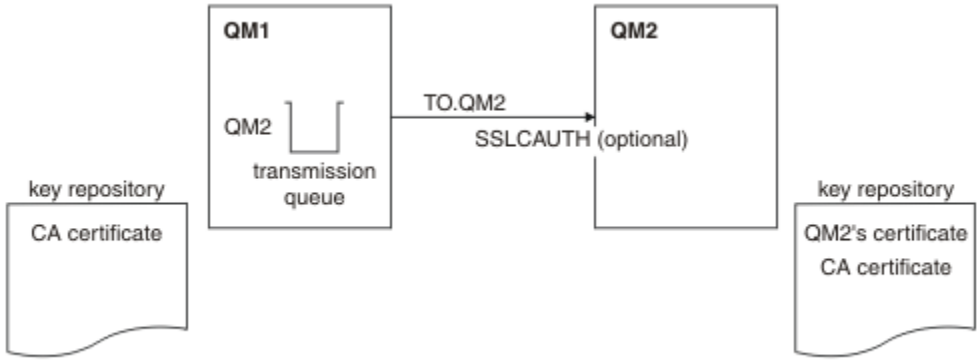
Bir kuyruk yöneticisinin, SSL ya da TLS istemcisi bir sertifika göndermediği durumlarda, bir kuyruk yöneticisinin diğerine tek yönlü kimlik doğrulamasını kullanarak bağlanmasını sağlamak üzere, bir sistemi karşılıklı kimlik doğrulamasıyla değiştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- İki kuyruk yöneticiniz (QM1 ve QM2), “İki kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması” sayfa 202içinde olduğu gibi ayarlanmıştır.
- You want to change QM1 so that it connects using one-way authentication to QM2.

Sonuçtaki yapılanış şöyle görünür:



Şekil 22. Tek yönlü kimlik doğrulaması sağlayan kuyruk yöneticileri

Yordam

1. QM1' in kişisel sertifikasını, işletim sistemine göre, anahtar havuzundan kaldırın:
   - UNIX, Linuxve Windows sistemlerinde. Sertifika aşağıdaki gibi etiketlenir:
     - `ibmwebspheremq` , ardından kuyruk yöneticinizin adı küçük harfe katlandı. Örneğin, `QM1` için, `ibmwebspheremqqm1`.
2. İsteğe bağlı: QM1' ta, herhangi bir SSL ya da TLS kanalı önceden çalıştırıldıysa, SSL ya da TLS ortamını yenileyin.
3. Alıcıdaki anonim bağlantılara izin ver.

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 16 sayfa 205içinde gösterildiği gibi değiştirilir.

Sonraki adım

Gönderen kanalı çalışıyorsa ve REFRESH SECURITY TYPE (SSL) komutunu verdiyseniz (adım 2 'de) kanal otomatik olarak yeniden başlatılır. Gönderen kanalı çalışmadıysa, başlatın.

Kanalın sunucu ucunda, kanal durumu görüntüsünde eş adı parametre değerinin bulunması, bir istemci sertifikasının akıp geçeceğini gösterir.

Bazı DISPLAY komutları yayınlayarak, görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıktı aşağıdaki örneklerde gösterilen şekilde benzerdir:

QM1 kuyruk yöneticisinden şu komutu girin:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Sonuç çıkışı aşağıdaki örneğe benzer olacaktır:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

QM2 kuyruk yöneticisinden şu komutu girin:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Sonuç çıkışı aşağıdaki örneğe benzer olacaktır:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)                            SSLCERTI( )
   SSLPEER( )                              STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       XMITQ( )
```

QM2'ta SSLPEER alanı boş, QM1 ' un sertifika göndermediğini gösterir. QM1üzerinde, SSLPEER değeri, QM2'in kişisel sertifikasındaki DN' nin değeriyle eşleşir.

İstemcinin kuyruk yöneticisine güvenli bir şekilde bağlanması

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 edinmeniz ve yönetmeniz gerekir. Bir sınama sisteminde, kendinden imzalı sertifikaları ya da yerel bir sertifika yetkilisi (CA) tarafından verilen sertifikaları kullanabilirsiniz. Bir üretim sisteminde kendinden onaylı sertifikalar kullanmayın. Daha fazla bilgi için bkz. ../zs14140_.dita.

Sertifika oluşturma ve yönetme hakkında tam bilgi edinmek için bkz. “UNIX, Linux, and Windows sistemlerinde SSL ya da TLS ile çalışma” sayfa 111.

Bu konular grubu, SSL iletişimini ayarlarken yer alan 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. WebSphere MQ somutlaması ile, SSL ya da TLS sunucusu her zaman istemciden bir sertifika ister.

UNIX, Linux, and Windows sistemlerinde, SSL ya da TLS istemcisi yalnızca doğru WebSphere MQ biçiminde bir etiketi varsa, bu sertifikayı gönderir; `ibmwebspheremq` ise, oturum açma kullanıcı kimliğiniz küçük harfe çevrilir (örneğin, `ibmwebspheremqmyuserid`).

WebSphere MQ , diğer ürünlere ilişkin sertifikalarla 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 işlev gören kanalın sonuna SSLCAUTH parametresiyle ya da bir SSLPEER parametre değeri kümesine ayarlı olarak tanımlandıysa başarısız olur. Kuyruk yöneticisini anonim olarak bağlamaya ilişkin daha fazla bilgi için bkz. “İstemcinin kuyruk yöneticisine anonim olarak bağlanması” sayfa 210.

İstemci ve kuyruk yöneticisinin karşılıklı kimlik doğrulaması için kendinden onaylı sertifikaların kullanılması

Kendinden onaylı SSL ya da TLS sertifikalarını kullanarak, bir istemci ile kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

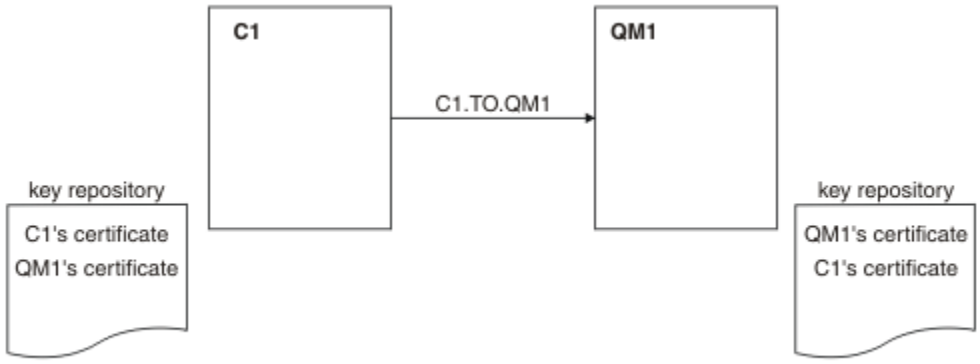
Bu görev hakkında

Senaryo:

- Güvenli bir şekilde iletişim kurulması gereken bir istemci, C1ve kuyruk yöneticisi (QM1) var. C1 ve QM1arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Kendinden onaylı sertifikalar kullanarak güvenli iletişiminizi test etme kararı aldınız.

IBM i üzerindeki DCM, kendinden onaylı sertifikaları desteklemez, bu nedenle bu görev IBM i sistemlerinde geçerli değildir.

Sonuçtaki yapılanış şöyle görünür:



Şekil 23. Bu görevle sonuçlanan yapılandırma

Şekil 17 sayfa 207'ta, QM1 için anahtar havuzu, QM1 sertifikasını ve C1' den genel sertifikayı içerir. C1 için anahtar havuzu, C1 sertifikasını ve QM1' den genel sertifikayı içerir.

Yordam

1. İstemci ve kuyruk yöneticisine ilişkin anahtar havuzu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. İstemci ve kuyruk yöneticisi için kendinden onaylı sertifikalar yarat:
   - UNIX, Linuxve Windows sistemlerinde.
3. Her sertifikana ilişkin bir kopyasını çıkarın:
   - UNIX, Linuxve Windows sistemlerinde.
4. Transfer the public part of the C1 certificate to the QM1 system and vice versa, using a utility such as FTP.
5. İş ortağı sertifikasını istemci ve kuyruk yöneticisi için anahtar havuzuna ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
6. Kuyruk yöneticisininde REFRESH SECURITY TYPE (SSL) komutunu verin.
7. İstemci-bağlantı kanalını aşağıdaki yöntemlerden biriyle tanımlayın:
   - Using the MQCONNX call with the MQSCO structure on C1, as described in WebSphere MQ MQI istemcisinde istemci-bağlantı kanalı yaratılması.
   - Using a client channel definition table, as described in Sunucuda sunucu bağlantısı ve istemci-bağlantı tanımları yaratılması .
8. QM1' ta, bir sunucu bağlantısı kanalı tanımlayın; örneğin, aşağıdaki örneğin gibi bir komut yayınlayın:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanal, adım 6 'da tanımladığınız istemci-bağlantı kanalıyla aynı adı ve aynı CipherSpec' u kullanmalıdır.

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 17 sayfa 207içinde gösterildiği gibi oluşturulur

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıktı aşağıdaki örnekte gösterilen çıkışa benzerdir.

Kuyruk yöneticisinden QM1, şu komutu girin:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Kanal tanımlamalarının SSLPEER süzgeç özniteliğini ayarlamaya isteğe bağlıdır. Kanal tanımlaması SSLPEER ayarlıysa, değerinin Adım 2 'de oluşturulan ortak sertifikadaki konu DN ' iyle eşleşmesi gerekir. Başarılı bir bağlantıdan sonra, DISPLAY CHSTATUS çıkışındaki SSLPEER alanı, uzak istemci sertifikasının konu ayırt edici adını (DN) gösterir.

İstemci ve kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması

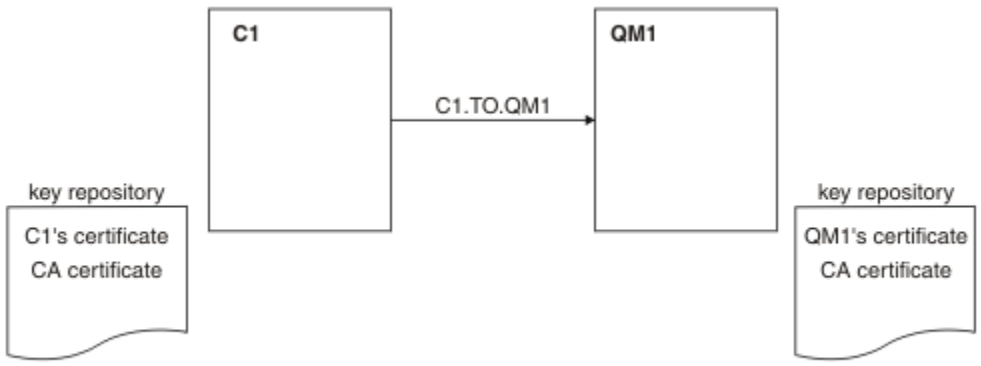
CA imzalı SSL ya da TLS sertifikalarını kullanarak, bir istemci ile kuyruk yöneticisi arasında karşılıklı kimlik doğrulaması gerçekleştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Güvenli bir şekilde iletişim kurulması gereken bir istemci, C1ve kuyruk yöneticisi (QM1) var. C1 ve QM1arasında karşılıklı kimlik doğrulaması gerçekleştirilmesini zorunlu kısınız.
- Gelecekte bu ağı bir üretim ortamında kullanmayı planlıyorsunuz, bu nedenle CA-imzalı sertifikalarını baştan kullanmaya karar verdiniz.

Sonuçtaki yapılanış şöyle görünür:



Şekil 24. Bu görevle sonuçlanan yapılandırma

Şekil 18 sayfa 208' ta, C1 için anahtar havuzu C1 ve CA sertifikasına ilişkin sertifika içerir. QM1 için anahtar havuzu, QM1 sertifikasının ve CA sertifikasının bulunduğunu içerir. Bu örnekte hem C1'in

sertifikası, hem de QM1' in sertifikası aynı CA tarafından yayınlandı. C1'in sertifikası ve QM1' in sertifikası farklı CA ' lar tarafından verildiyse, C1 ve QM1 için anahtar havuzları hem CA sertifikalarını içermeli.

Yordam

1. İstemci ve kuyruk yöneticisine ilişkin anahtar havuzu işletim sistemine göre hazırlayın:
   - UNIX, Linuxve Windows sistemlerinde.
2. İstemci ve kuyruk yöneticisi için sertifika yetkilisi tarafından imzalanmış bir sertifika isteyin.
   İstemci ve kuyruk yöneticisi için farklı CA ' lar kullanabilirsiniz.
   - UNIX, Linuxve Windows sistemlerinde.
3. Sertifika yetkilisi sertifikasını istemci ve kuyruk yöneticisi için anahtar havuzuna ekleyin.
   İstemci ve kuyruk yöneticisi farklı Sertifika Yetkilileri kullanıyorsa, her bir Sertifika Yetkilisi için CA sertifikasının her iki anahtar havuzuna da eklenmesi gerekir.
   - UNIX, Linuxve Windows sistemlerinde.
4. İstemcinin ve kuyruk yöneticisinin anahtar havuzuna CA imzalı sertifikayı ekleyin:
   - UNIX, Linuxve Windows sistemlerinde.
5. İstemci-bağlantı kanalını aşağıdaki yöntemlerden biriyle tanımlayın:
   - Using the MQCONNX call with the MQSCO structure on C1, as described in WebSphere MQ MQI istemcisinde istemci-bağlantı kanalı yaratılması.
   - Using a client channel definition table, as described in Sunucuda sunucu bağlantısı ve istemci-bağlantı tanımları yaratılması .
6. QM1üzerinde, aşağıdaki örnek gibi bir komut vererek bir sunucu bağlantı kanalı tanımlayın:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanal, adım 6 'da tanımladığınız istemci-bağlantı kanalıyla aynı adı ve aynı CipherSpec' u kullanmalıdır.

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 18 sayfa 208içinde gösterildiği gibi oluşturulur.

Sonraki adım

DISABLE komutları kullanılarak görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, sonuç çıkışı aşağıdaki örnekte gösterildiği gibi olur.

Kuyruk yöneticisinden (QM1) aşağıdaki komutu girin:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

Sonuçtaki çıkış aşağıdaki örnekteki gibidir:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

DISPLAY CHSTATUS çıkışındaki SSLPEER alanı, Adım 2 'de yaratılan uzak istemci sertifikasının konu DN değerini gösterir. Sertifika veren adı, 4. adımda eklenen kişisel sertifikayı imzalayan CA sertifikasının konu DN 'si ile eşleşir.

İstemcinin kuyruk yöneticisine anonim olarak bağlanması

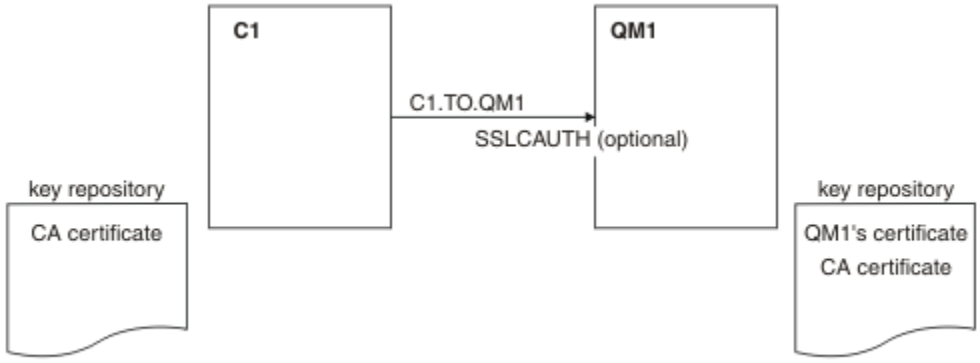
Bir kuyruk yöneticisinin anonim olarak başka bir kuyruk yöneticisine bağlanmasına izin vermek üzere karşılıklı kimlik doğrulama içeren bir sistemi değiştirmek için bu örnek yönergeleri izleyin.

Bu görev hakkında

Senaryo:

- Kuyruk yöneticinizin ve istemcinizin (QM1 ve C1), “İstemci ve kuyruk yöneticisinin karşılıklı kimlik doğrulaması için CA imzalı sertifikaların kullanılması” sayfa 208içinde olduğu gibi ayarlanmıştır.
- C1 'yi anonim olarak QM1' e bağlanmasını istiyorsanız,change' i değiştirmek istiyorsunuz.

Sonuçtaki yapılanış şöyle görünür:



Şekil 25. Anonim bağlantıya izin veren istemci ve kuyruk yöneticisi

Yordam

1. Kişisel sertifikayı, işletim sistemine göre C1için anahtar havuzundan kaldırın:
   - UNIX, Linuxve Windows sistemlerinde. Sertifika aşağıdaki gibi etiketlenir:
     - `ibmwebspheremq` , ardından oturum açma kullanıcı kimliğiniz küçük harfe (örneğin, `ibmwebspheremqmyuserid`) katlandı.
2. İstemci uygulamasını yeniden başlatın ya da istemci uygulamasının tüm SSL ya da TLS bağlantılarını kapatmasına ve yeniden açmasına neden olur.
3. Aşağıdaki komutu girerek, kuyruk yöneticiside anonim bağlantılara izin ver:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Sonuçlar

Anahtar havuzları ve kanallar, Şekil 19 sayfa 210içinde gösterildiği gibi değiştirilir.

Sonraki adım

Kanalın sunucu ucunda, kanal durumu görüntüsünde eş adı parametre değerinin bulunması, bir istemci sertifikasının akıp geçeceğini gösterir.

Bazı DISPLAY komutları yayınlayarak, görevin başarıyla tamamlandığını doğrulayın. Görev başarılı olursa, elde edilen çıkış aşağıdaki örnekteki gibi gösterilmeye benzer:

Kuyruk yöneticisinden QM1, şu komutu girin:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Sonuç çıkışı aşağıdaki örneğe benzer olacaktır:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

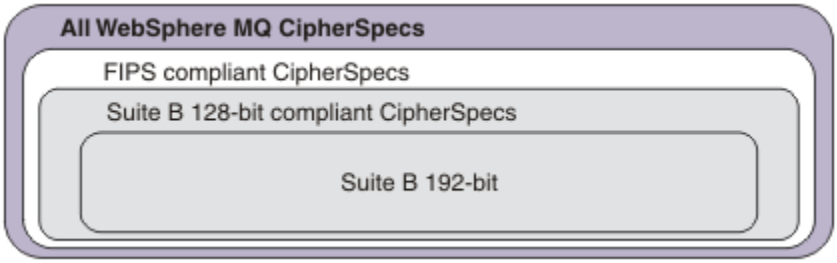
SSLCERTI ve SSLPEER alanları boş, C1 ' in sertifika göndermediğini gösterir.

CipherSpecs ' nin Belirtilmesi

DEFINE CHANNEL MQSC komutunda ya da **ALTER CHANNEL** MQSC komutunda **SSLCIPH** değiştirgesini kullanarak CipherSpec belirtin.

IBM WebSphere MQ ile kullanabileceğiniz CipherSpecs ' in bazıları FIPS uyumludur. NULL_MD5gibi diğerleri değildir. Benzer şekilde, bazı FIPS uyumlu CipherSpecs de Suite B uyumludur, ancak diğerleri uyumludur. Tüm Suite B uyumlu CipherSpecs de 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 çizge, bu altkümeler arasındaki ilişkiyi gösterir:



IBM WebSphere MQ SSL ve TLS desteği ile kullanabileceğiniz şifre belirtimleri aşağıdaki tabloda listelenmiştir. Kişisel sertifika isteğinde bulunduğunuzda, genel ve özel anahtar çifti için bir anahtar boyutu belirtirsiniz. SSL el sıkışması sırasında kullanılan anahtar boyutu, çizelgede belirtildiği şekilde CipherSpectarafından belirlenmedikçe sertifikada saklanan boyuttur.

CipherSpec adı	Kullanılan protokol	MAC algoritması	Şifreleme Algoritması	Şifreleme bitleri	FIPS[1]	Suite B 128 bit	Takım B 192 bit
NULL_MD5 [a]	SSL 3.0	MD5	Yok	0	Hayır	Hayır	Hayır
NULL_SHA [a]	SSL 3.0	SHA-1	Yok	0	Hayır	Hayır	Hayır
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Hayır	Hayır	Hayır
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Hayır	Hayır	Hayır
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Hayır	Hayır	Hayır
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Hayır	Hayır	Hayır

CipherSpec adı	Kullanılan protokol	MAC algoritması	Şifreleme Algoritması	Şifreleme bitleri	FIPS[1]	Suite B 128 bit	Takım B 192 bit
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Hayır	Hayır	Hayır
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Hayır	Hayır	Hayır
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Hayır	Hayır	Hayır
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES.	128	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES.	256	Evet	Hayır	Hayır
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	[5] yok	Hayır	Hayır
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Hayır[6]	Hayır	Hayır
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES.	128	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES.	256	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	128	Evet	Hayır	Hayır
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	256	Evet	Hayır	Hayır
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	Hayır
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Hayır	Hayır	Hayır
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	128	Evet	Hayır	Hayır
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES.	256	Evet	Hayır	Hayır
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES.	128	Evet	Hayır	Hayır
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES.	256	Evet	Hayır	Hayır
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES.	128	Evet	Evet	Hayır
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES.	256	Evet	Hayır	Evet

CipherSpec adı	Kullanılan protokol	MAC algoritması	Şifreleme Algoritması	Şifreleme bitleri	FIPS[1]	Suite B 128 bit	Takım B 192 bit
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES.	128	Evet	Hayır	Hayır
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES.	256	Evet	Hayır	Hayır
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Yok	0	Hayır	Hayır	Hayır
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Yok	0	Hayır	Hayır	Hayır
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Yok	0	Hayır	Hayır	Hayır
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Yok	Yok	0	Hayır	Hayır	Hayır
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Hayır	Hayır	Hayır

Notlar:

1. CipherSpec ' in FIPS onaylı bir platformda FIPS onaylı olup olmadığını belirtir. FIPS ' ye ilişkin açıklamalar için bkz. Federal Information Processing Standards (FIPS) .
2. 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.
3. Tokalaşma anahtarı boyutu 1024 bittir.
4. Bu CipherSpec , Explorer tarafından kullanılan JRE ' ye uygun kısıtlamasız ilke dosyaları uygulanmadıkça, WebSphere MQ Explorer 'dan bir kuyruk yöneticisine bağlantı güvenli kılmak için kullanılamaz.
5. Bu CipherSpec , 19 Mayıs 2007 'den önce FIPS 140-2 sertifikalıydı.
6. 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.
7. Bu CipherSpec , bağlantı AMQ9288hatasıyla sonlandırılmadan önce 32 GB ' ye kadar veri aktarmak için kullanılabilir. Bu hatayı önlemek için üçlü DES kullanmaktan kaçının ya da bu CipherSpec' i kullanırken gizli anahtar sıfırlamasını etkinleştirin.

Platform desteği:

- a Desteklenen tüm platformlarda kullanılabilir.
- b Yalnızca UNIX, Linux, and Windows platformlarında kullanılabilir.

İlgili kavramlar

“Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33
Bu konuda, IBM WebSphere MQiçindeki CipherSpecs ve dijital sertifikalar arasındaki ilişkiyi sıralayarak uygun CipherSpecs ve güvenlik ilkeniz için dijital sertifikalar nasıl seçileceği hakkında bilgi sağlanmaktadır.

İlgili başvurular

KANAL TANıMLAYıN
KANAL DEğIşTIR

IBM WebSphere MQ Explorerkullanılarak CipherSpecs hakkında bilgi edinme

CipherSpecs' in açıklamalarını görüntülemek için IBM WebSphere MQ Explorer olanağını kullanabilirsiniz.

“CipherSpecs ' nin Belirtilmesi” sayfa 211içindeki CipherSpecs ile ilgili bilgi edinmek için aşağıdaki yordamı kullanın:

1. **IBM WebSphere MQ Explorer** ' ı 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.

CipherSpecs belirtilerek ilgili alternatifler

İşletim sisteminin SSL desteğini sağladığı bu platformlar için, sisteminiz yeni CipherSpecsözelliğini destekleyebilir. SSLCIPH parametresiyle yeni bir CipherSpec belirtebilirsiniz, ancak sağladığınız değer altyapınıza bağlıdır.

Not: CipherSpecs , WebSphere MQ ürünüyle birlikte sağlandığından bu bölüm UNIX, Linux ya da Windows sistemleri için geçerli değildir; bu nedenle yeni CipherSpecs , sevkiyattan sonra kullanılamaz.

İşletim sisteminin SSL desteğini sağladığı platformlarda, sisteminiz “CipherSpecs ' nin Belirtilmesi” sayfa 211içinde bulunmayan yeni CipherSpecs ' i destekleyebilir. SSLCIPH parametresiyle yeni bir CipherSpec belirtebilirsiniz, ancak sağladığınız değer altyapınıza bağlıdır. Her durumda belirtim, sisteminizin çalıştırdığı SSL sürümü tarafından hem geçerli hem de desteklenen bir SSL CipherSpec belirtimine karşılık *gelmelidir* .

IBM i
Onaltılı bir değeri gösteren iki karakterli bir dizgi.

İzin verilen değerlerle ilgili ek bilgi için uygun ürün belgelerine bakın (IBM i ürün belgelerinde *cipher_spec* öğesini arayın).

Değeri belirlemek için CHGMQMCHL ya da CRTMQMCHL komutunu kullanabilirsiniz; örneğin:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

SSLCIPH değiştirgesini ayarlamak için ALTER QMGR MQSC komutunu da kullanabilirsiniz.

z/OS
Onaltılı bir değeri gösteren iki karakterli bir dizgi. Onaltılı kodlar, SSL protokolünde tanımlanan değerlere karşılık gelir.

Daha fazla bilgi için, *z/OS Cryptographic Services System SSL Programming*, SC24-5901' in API başvuru bölümündeki gsk_environment_open () açıklamasına bakın; burada desteklenen tüm SSL V3.0 ve TLS V1.0 şifre belirtimlerinin bir listesi 2 basamaklı onaltılı kodlar biçiminde bulunur.

WebSphere MQ kümeleri için dikkat edilecek noktalar

WebSphere MQ kümeleriyle “CipherSpecs ' nin Belirtilmesi” sayfa 211içindeki CipherSpec adlarını kullanmak en güvenlidir. Alternatif bir belirtim kullanıyorsanız, belirtimin diğer platformlarda geçerli olmayabileceğini unutmayın. Daha fazla bilgi için bkz. “SSL ve kümeler” sayfa 242.

IBM WebSphere MQ MQI istemcisi için bir CipherSpec belirtme

Bir IBM WebSphere MQ MQI istemcisi için bir CipherSpec belirtme 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.
- Using the Active Directory (on Pencereler systems with Active Directory support)

Java için IBM WebSphere MQ sınıfları ve JMS için IBM WebSphere MQ sınıfları içeren bir CipherSuite belirtilmesini

JMS içinIBM WebSphere MQ sınıfları ve JMS için IBM WebSphere MQ sınıfları, diğer altyapılardan farklı CipherSuites değerlerini belirtir.

Java için IBM WebSphere MQ sınıflarıyla bir CipherSuite belirtilmesine ilişkin bilgi edinmek için bkz. Secure Sockets Layer (SSL) support.

JMS için IBM WebSphere MQ sınıflarıyla CipherSuite belirtilmesine ilişkin bilgi için bkz. JMS için WebSphere MQ sınıflarıyla SSL (Secure Sockets Layer; Güvenli Yuva Katmanı) kullanılıyor.

Denetleme

Olay iletilerini kullanarak, güvenlik izinsiz girişlerinin ya da izinsiz girişlerin denenmesini denetleyebilirsiniz. Ayrıca, IBM WebSphere 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 izleme konusuna 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 SSL yapılandırılırken bazı ek noktaları 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 WebSphere MQ ' daki erişim denetimi mekanizmasını kullanın.

Yordam

1. Belirli kuyruk yöneticilerinin bir kuyruğa ileti yerleştirmesini önlemek için, platformunuzda bulunan güvenlik olanaklarını kullanın.

   Örneğin:

   - z/OSiçin WebSphere MQ ' dakiRACF 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 (yalnızcaz/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 (yalnızcaz/OS)
   CTXiçin olduğu gibi, ağdan alınan herhangi bir kullanıcı kimliği kullanılmaz.

Uzak küme kuyruklarına ileti koyma yetkisi

Altyapınızda, kuyruk yöneticisine bağlanmak ve kuyruk yöneticisine kuyruk koymak 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

- UNIX, Linux ve 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
```

Kullanıcı iletileri yalnızca belirtilen küme kuyruğuna ve diğer küme kuyruklarına koyabilir.

Değişken adları aşağıdaki anlamlara sahiptir:

QMgrName
Kuyruk yöneticisinin adı.

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 187içindeki yönergeleri izleyerek ayarlayın.

İlgili bilgiler
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 SSL/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.

   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 yöneticilerinin bir küme bırakması zorlanması

İstenmeyen bir kuyruk yöneticisini, tam havuz kuyruk yöneticisinde RESET CLUSTER komutunu vererek bir küme bırakmasını zorunlu kılacak şekilde zorlayın.

Bu görev hakkında

İstenmeyen kuyruk yöneticisini bir küme bırakması için zorlayabilirsiniz. Örneğin, bir kuyruk yöneticisi silinir, ancak küme alıcı kanalları küme için hala tanımlıdır. Ortalığı toparlamak isteyebilirsin.

Bir küme yöneticisini bir kümeden çıkarma yetkisi yalnızca tam havuz kuyruğu yöneticilerine verilir.

Follow this procedure to eject the queue manager OSLO from the cluster NORWAY:

Yordam

1. Tam havuz kuyruk yöneticisininde, şu komutu verin:

   ```
   RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
   ```
2. Diğer bir seçenek de, komutta QMNAME yerine QMID ' yi kullanır.

   ```
   RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
   ```

Sonuçlar

Zorlamalı olarak kaldırılan kuyruk yöneticisi değişmez: yerel küme tanımlamaları bunu kümede olacak şekilde gösterir. Diğer tüm kuyruk yöneticilerindeki tanımlar bunu kümede göstermiyor.

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 ve kümeler

Kümeler için SSL yapılandırılırken, bir CLUSRCVR kanal tanımının, otomatik olarak tanımlanmış bir CLUSSDR kanalı olarak diğer kuyruk yöneticilerine yayılırdığı dikkate alın. Bir CLUSRCVR kanalı SSL kullanıyorsa, kanalı kullanarak iletişim kuran tüm kuyruk yöneticilerindeki SSL ' yi yapılandırmanız gerekir.

SSL ile ilgili ek bilgi için WebSphere MQ support for SSL and TLSbaşlıklı konuya bakın. Bu öneri, genellikle küme kanallarına uygulanabilir, ancak aşağıdakine özel bir önem vermek isteyebilirsiniz:

Bir IBM WebSphere 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 SSL bağlanırlığı için yapılandırıldıysa, aşağıdaki noktalar geçerlidir:

- Bu CLUSRCVR ile iletişim kurmak isteyen tüm kuyruk yöneticilerinin SSL desteğine erişimi olması gerekir. Bu SSL hükmü, kanal için CipherSpec ' i 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 WebSphere 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=WebSphere 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. An example of this is that the CipherSpec string RC4_SHA_US has a value of 05 on IBM i but is not a valid specification on UNIX, Linux or Windows systems. Bir CLUSRCVRüzerinde özel SSLCIPH değiştirgeleri kullanılırsa, sonuçta elde edilen tüm otomatik tanımlı küme gönderen kanalları, temeldeki SSL 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, RC4_MD5_US).

Bir SSLCRLNL parametresi, tek bir kuyruk yöneticisine uygulanır ve bir küme içindeki diğer kuyruk yöneticilerine yayılmaz.

Kümelenmiş kuyruk yöneticileri ve kanalları SSL ' ye yükseltiliyor

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 WebSphere MQ yayın düzeyinde yeni olabilir ve 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.

Bu düzeylerde önceden yoksa, kümedeki tüm kuyruk yöneticilerini WebSphere MQ V6 ' e ya da daha yüksek bir sürüme yükseltin. Sertifikalar ve anahtarları dağıtın, böylece her birinden SSL ' ler çalışır.

Bu görev hakkında

Bir kerede bir CLUSRCVR ' yi değiştirin ve bir sonraki değiştirmeden önce kümedeki değişikliklerin küme üzerinden akmasına izin verin. Yürürlükteki kanal için yapılan değişiklikler küme boyunca dağıtılıncaya kadar, ters yolu değiştirmediğinizden emin olun.

Yordam

1. CLUSRCVR kanallarını, istediğiniz sırayla SSL ' ye geçin.

   Değişiklikler, SSL ' de değiştirilmeyen kanallar üzerinden ters yönde akışı sağlar.
2. Tüm el ile CLUSSDR kanallarını SSL ' ye geçin.

   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.

İlgili kavramlar

“CipherSpecs ' nin Belirtilmesi” sayfa 211
DEFINE CHANNEL MQSC komutunda ya da **ALTER CHANNEL** MQSC komutunda **SSLCIPH** değiştirgesini kullanarak CipherSpec belirtin.

“Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33
Bu konuda, IBM WebSphere MQiçindeki CipherSpecs ve dijital sertifikalar arasındaki ilişkiyi sıralayarak uygun CipherSpecs ve güvenlik ilkeniz için dijital sertifikalar nasıl seçileceği hakkında bilgi sağlanmaktadır.

İlgili bilgiler

Kümeleme: REFRESH CLUSTER en iyi uygulamaları kullanma

Kümelenmiş kuyruk yöneticileri ve kanallar üzerinde SSL ya da TLS devre dışı bırakılması

SSL ya da 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 .

   SSL ya da TLS ' yi küme alıcı kanallarında istediğiniz herhangi bir sırayla kapatabilirsiniz.

   SSL ya da 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 SSL ya da TLS ' yi kapatın.

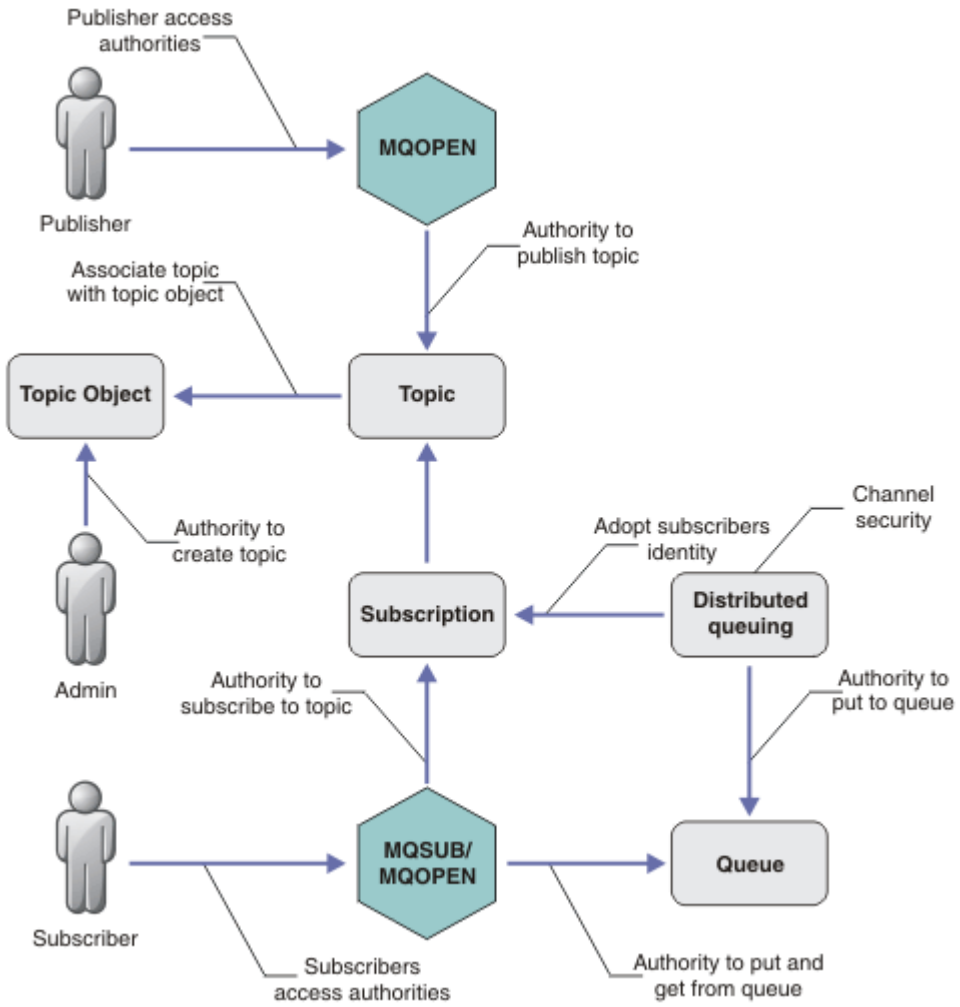
   REFRESH CLUSTER komutunu REPOS （YES） seçeneğiyle birlikte kullanmadığınız sürece, bu işlem kümenin işleyişi üzerinde herhangi bir etkiye sahip değildir.

   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 tanımlanir.

Bir konuya yayınlanırken ve bir konuya abone olmak için bir dizi bileşen vardır. Aralarındaki bazı güvenlik ilişkileri Şekil 26 sayfa 245 ' de gösterilir ve aşağıdaki örnekte anlatılır.



Şekil 26. Güvenlik ilişkilerini yayınla/abone ol

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 247 konu nesnelerini kullanarak konuları 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 251 ve “Bir konuyla ilgili olarak yayınlamak için kullanıcıya erişim izni ver” sayfa 256örneklerine bakın.

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 248

Konu kullanarak abone olma

“Konu düğümünün var olmadığı bir konu dizesini kullanarak abone olma” sayfa 249

Genel arama karakterleri içeren bir konu kullanarak abone olma

“Genel arama karakterleri içeren bir konu dizesini kullanarak abone olma” sayfa 249

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 261.

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 249.

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

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 WebSphere MQ kümesi yapılandırmalarında, kanal işleminin yetkisini kullanarak iletileri hedef kuyruklara yerleştirmek için kanallar PUTUUT=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 güvenlik yayınla/abone ol , abonelikleri kümedeki diğer sunuculara dağıtmaya izin verilen 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. WebSphere 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.

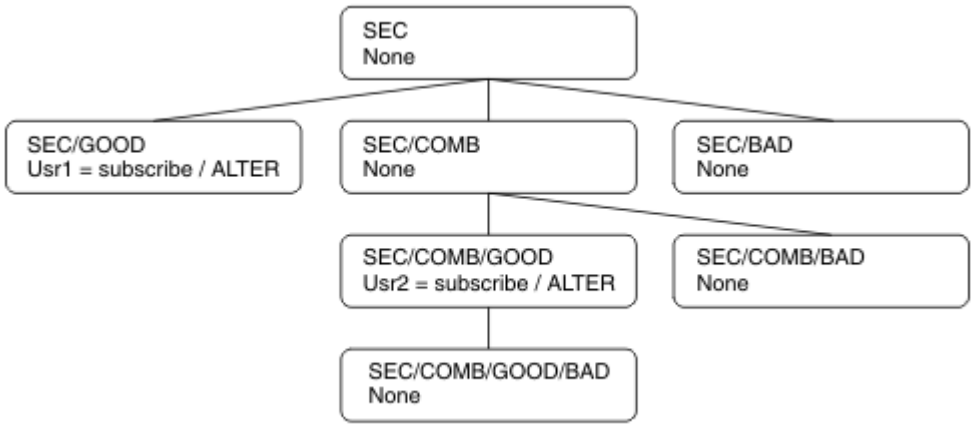
Aşağıdaki örnekte, konu nesnelerinin güvenlik öznitelikleriyle tanımlanmış olduğu ya da gösterilen yetkilerin olduğu bir örnek olarak göz önünde bulundurun:

Çizelge 17. 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

Çizelge 17. Örnek konu nesnesi yetkileri (devamı var)			
Konu adı	**Konu dizesi**	**Yetkiler- z/ OSdeğil**	**z/OS yetkileri**
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.

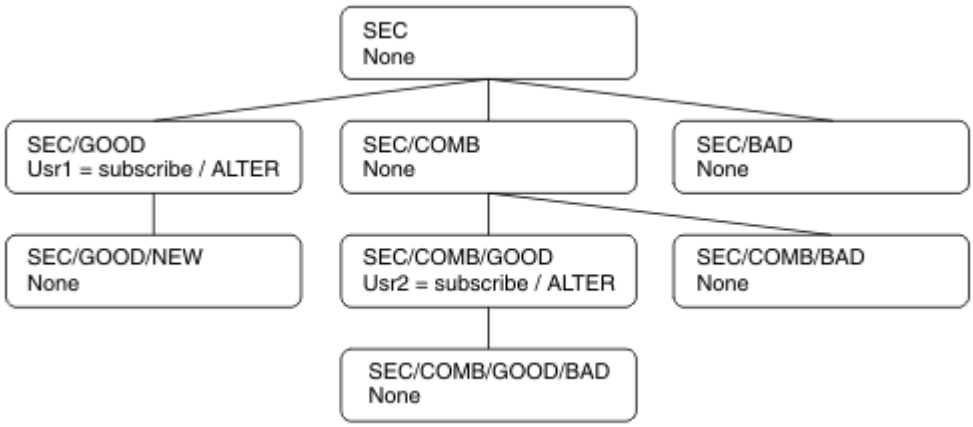
Konu düğümünün var olduğu bir konu dizesini kullanarak abone olma

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, temeldeki kuyruğun *yapılamamasını* denetler. 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 18 sayfa 251:

Çizelge 18. Komutlar için güvenlik denetimleri için kullanılan kullanıcı kimlikleri

Komut	SUBUSER belirlendi ve boş	SUBUSR belirlendi ve tamamlandı	SUBUSR belirtilmedi
	Yönetici kimliğini kullan		Yönetici kimliğini kullan
	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 konulara ilişkin erişim denetimi kurulumu olan bir senaryo açıklanmaktadır.

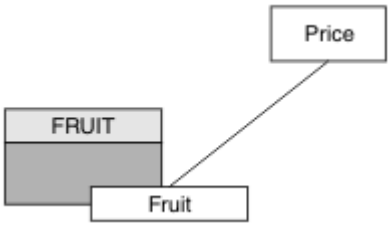
Bir konuya abone olmak için kullanıcıya erişim izni ver

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 27. Konu nesne erişimi örneği

Çizelge 19. 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:
   - 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:

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

     ```
     setmqaut -t topic -n FRUIT -p USER1 +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:

- UNIX Linux Windows Diğer platformlarda, 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

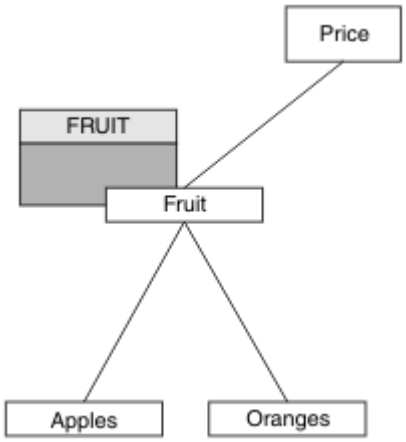
Bu konu, birden çok kullanıcı tarafından konulara nasıl erişim verileceğini size bildiren görevler listesinde ikinci sıradır.

Başlamadan önce

Bu konu, “Bir konuya abone olmak için kullanıcıya erişim izni ver” sayfa 251içinde 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 28. Bir konu ağacındaki bir konuya erişim verme örneği

Çizelge 20. 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	
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/OSüzerinde, 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 profiller olarak önceki görevdeki alınanlarla 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

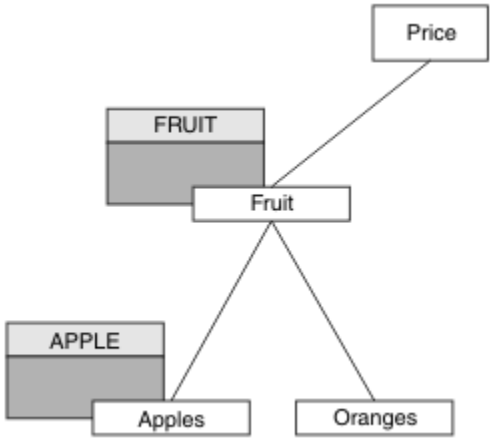
Bu konu, birden çok kullanıcı tarafından konulara abone olmak için nasıl erişim verileceğini size bildiren görevler listesinde üçüncü konudur.

Başlamadan önce

Bu konu, “Bir kullanıcıya ağaç içinde daha derin bir konuya abone olmak için erişim izni ver” sayfa 252içinde 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 29. Bir konu ağacındaki belirli konulara erişim verilmesi

Çizelge 21. 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:
   - 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:

     Windows, UNIX and Linux sistemleri

     ```
     setmqaut -t topic -n APPLE -p USER2 +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:

- 

Windows, UNIX ve Linux altyapılarında, 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

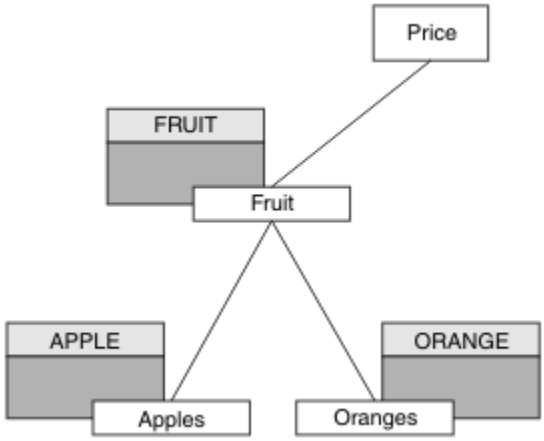
Bu konu, birden çok kullanıcıya göre konulara abone olma ve z/OSüzerinde ek RACF ICH408I iletilerinden kaçınmak için erişim verilmesine nasıl izin verileceğini bildiren görevler listesinde dördüncüye yer verir.

Başlamadan önce

Bu konu, ek hata iletilerini önlemek için “Başka bir kullanıcıya, ağaç içindeki daha derinlere abone olmak için başka bir kullanıcı erişimi verin” sayfa 254 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 30. 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:
   - Diğer platformlar:

     Altyapıya ilişkin yetki komutlarını kullanarak eşdeğer erişimi ayarlayın:

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

     ```
     setmqaut -t topic -n ORANGE -p USER1 +sub
     setmqaut -t topic -n APPLE -p USER1 +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:

- UNIX Linux Windows 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"
```

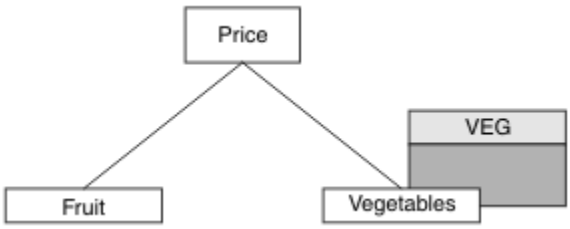
Bir konuyla ilgili olarak yayınlamak için kullanıcıya erişim izni ver

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 31. Bir konuya yayınlama erişimi verilmesi

Çizelge 22. 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:
   - 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:

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

     ```
     setmqaut -t topic -n VEG -p USER1 +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:

- UNIX Linux Windows Diğer platformlarda, 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

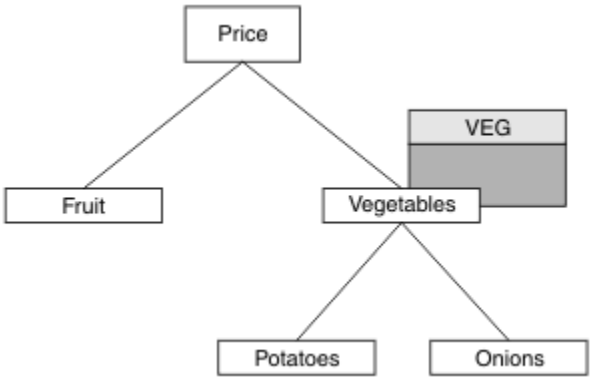
Bu konu, birden çok kullanıcıya göre konu başlıklarına nasıl erişilmesine ilişkin erişim verileceğini size bildiren görevler listesinde ikinci sıradır.

Başlamadan önce

Bu konu, “Bir konuyla ilgili olarak yayınlamak için kullanıcıya erişim izni ver” sayfa 256içinde 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 32. Bir konu ağacındaki bir konuya yayınlama erişimi verilmesi

Çizelge 23. 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/OSüzerinde, 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 profiller olarak önceki görevdeki alınanlarla aynıdır.
- Diğer platformlarda aldığınız olay iletisi, önceki görevdeki alınana benzer, ancak gerçek konu dizgisi farklıdır.

Yayınlama ve abone olma için erişim izni ver

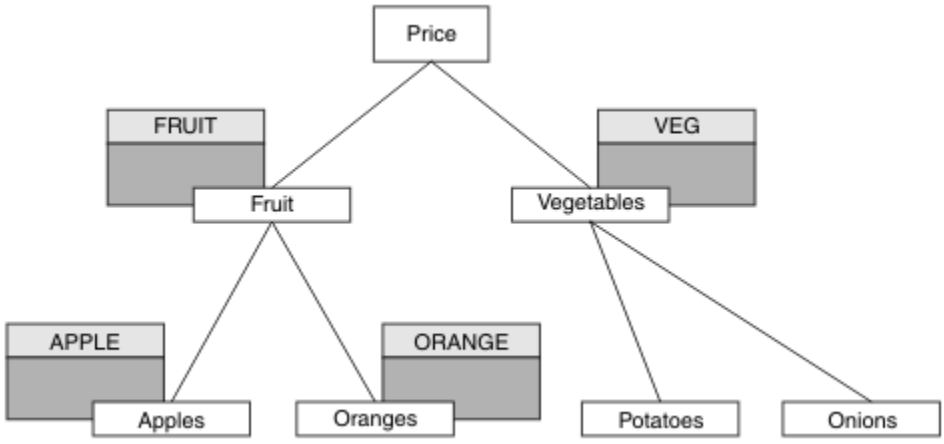
Bu konu, bir kullanıcıya birden çok kullanıcı tarafından yayınlama ve konuya abone olma erişim izni verileceğini bildiren görevler listesinin en sonuncunda yer alıyor.

Başlamadan önce

Bu konu, “Bir kullanıcıya ağaç içinde daha derin bir konu yayınlamak için erişim izni ver” sayfa 258içinde 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 33. Yayınlama ve abone olma için erişim verilmesi

Çizelge 24. 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

Çizelge 24. Erişim gereksinmelerini yayınlama ve abone olma örneği (devamı var)			
Konu	**Abone olma erişimi gerekiyor**	**Yayınlama erişimi gerekli**	**Konu nesnesi**
Fiyat/Meyve/Portakal	USER1		Turuncu

Yordam

Erişim izni aşağıdaki gibi olur:

- 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:

  Windows, UNIX and Linux sistemleri

```
setmqaut -t topic -n FRUIT -p USER1 +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:

- 

  Windows, UNIX ve Linux altyapılarında, 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 25. 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 25. 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 26. 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.

IBM WebSphere MQ Advanced Message Security

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

IBM WebSphere MQ Advanced Message Security'e genel bakış

IBM WebSphere MQ uygulamaları, genel anahtar şifrelemesi modeli kullanılarak farklı koruma düzeylerine sahip yüksek değerli finansal işlemler ve kişisel bilgiler gibi hassas verileri göndermek için IBM WebSphere MQ Advanced Message Security ' i kullanabilir.

İlgili başvurular

GSKit return codes used in IBM WebSphere MQ AMS messages

Sürüm 7.0.1 ve sürüm 7.5arasında değişen davranış

IBM Gelişmiş İleti Güvenliği , WebSphere MQ 7.5' te bir bileşen haline geldikçe, IBM WebSphere MQ AMS işlevlerinin bazı yönleri değişerek, var olan uygulamaları, yönetim komut dosyalarını ya da yönetim yordamlarını nelerin etkileyebileceğini belirler.

Kuyruk yöneticilerini 7.5sürümüne büyütmeden önce aşağıdaki değişiklikler listesini dikkatli bir şekilde gözden geçirin. Sistemleri IBM WebSphere MQ sürüm 7.5:

- IBM WebSphere MQ AMS kuruluşu, WebSphere MQ kuruluş sürecinin bir parçasıdır.
- IBM WebSphere MQ AMS güvenlik yetenekleri, kuruluş ve güvenlik ilkeleriyle denetlenerek etkinleştirilir. You do not need to enable interceptors to allow IBM WebSphere MQ AMS start intercepting data.
- IBM WebSphere MQ AMS in WebSphere MQ version 7.5 does not require the use of the **cfgmqs** command as in the stand-alone version of IBM WebSphere MQ AMS.

IBM WebSphere MQ Advanced Message Security' in özellikleri ve işlevleri

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

Aşağıda, IBM WebSphere MQ AMS işlevlerinin eksiksiz bir listesi yer alıyor:

- WebSphere MQtarafından işlenen hassas ya da yüksek değerli işlemleri sabitler.
- 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.
- WebSphere MQiçin var olan özel ve müşteri tarafından yazılan uygulamaların güvenliğini sağlar.

Hata işleme

Gelişmiş İleti Güvenliği , korumasız olamayan iletileri ya da iletileri 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- WebSphere MQ 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.

WebSphere MQ AMS, SYSTEM.PROTECTION.ERROR.QUEUE , hata işleme kuyruğunda. IBM WebSphere MQ AMS tarafından SYSTEM.PROTECTION.ERROR.QUEUE ' e konulan tüm iletilerin başında MQDLH üstbilgisi vardır.

WebSphere MQ yöneticiniz SYSTEM.PROTECTION.ERROR.QUEUE başka bir kuyruğu işaret eden bir diğer ad olarak kuyruğa aldı.

Temel kavramlar

Aracın nasıl çalıştığını ve nasıl etkili bir şekilde yönetileceğini anlamak için Gelişmiş İleti Güvenliği içindeki temel kavramlara ilişkin bilgi edinin.

Genel anahtar altyapısı

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. Gelişmiş İleti Güvenliği , 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 286

WebSphere MQ uygulamalarına şeffaf şifreleme koruması sağlamak için, Gelişmiş İleti Güvenliği , ortak anahtar sertifikalarının ve bir özel anahtarın saklandığı anahtar deposu dosyasını kullanır.

dijital sertifikalar

Gelişmiş İleti Güvenliği , 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: Gelişmiş İleti Güvenliği , hem Java 'da 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.

Nesne yetkisi yöneticisi

Object Authority Manager (OAM), WebSphere MQ ürünleri ile birlikte sağlanan yetkilendirme hizmeti bileşenidir.

Gelişmiş İleti Güvenliği ' a erişim, WebSphere 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.

- MQI aracılığıyla Gelişmiş İleti Güvenliği 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

Desteklenen teknoloji

Gelişmiş İleti Güvenliği , güvenlik altyapısı sağlamak için birkaç teknoloji bileşenine bağlıdır.

Gelişmiş İleti Güvenliği , aşağıdaki WebSphere MQ uygulama programlama arabirimlerini (API ' ler) destekler:

- İleti kuyruğu arabirimi (MQI)
- WebSphere MQ Java Message Service (JMS) 1.0.2 ve 1.1.
- Java içinWebSphere MQ Temel Sınıfları
- Yönetilmeyen kipte ağ içinWebSphere MQ sınıfları

Not: Gelişmiş İleti Güvenliği , X.509 uyumlu sertifika yetkililerine destek sağlar.

Bilinen sınırlamalar

IBM WebSphere MQ Advanced Message Securityile ilgili sınırlamalar hakkında bilgi edinin.

- Aşağıdaki IBM WebSphere MQ seçenekleri desteklenmez:
  - Yayınla/abone ol.
  - Kanal veri dönüştürme.
  - Dağıtım listeleri.
  - Uygulama iletisi bölümlemesi
  - The use of non-threaded applications using API exit on HP-UX platforms.
  - Yönetilen kipteki .NET içinIBM WebSphere MQ sınıfları (istemci ya da bağ tanımları bağlantıları).
  - Message Service Client for .NET (XMS) uygulamaları.
  - C/C++ için Message Service istemcisi (XMS supportPac IA94) uygulamaları.
- Tüm Java uygulamaları IBM Java Runtime 'a bağımlıdır.

  IBM WebSphere MQ Advanced Message Security , diğer satıcı firmalar tarafından sağlanan JRE ' yi desteklemez.
- İstemci kipinde IBM WebSphere MQ Advanced Message Security kullanan JMS ve Java istemci uygulamaları.

Herhangi bir JMS ya da Java, istemci uygulaması (IBM WebSphere MQ Explorer ve IBM WebSphere MQ Managed File Transfer aracıları da içinde olmak üzere), Version 7.5' den önceki bir WebSphere MQ kuyruk yöneticisiyle istemci kipinde IBM WebSphere MQ Advanced Message Security kullanamaz.

İleti koruma ilkelerini kullanmak için, bu uygulamaların bir IBM WebSphere MQ Version 7.5 kuyruk yöneticisiyle etkileşimde bulunması ya da yerel bağ tanımları kipinde, uygulamayla aynı makineden bir kuyruk yöneticisine bağlanması gerekir.

- IBM WebSphere MQ Advanced Message Security aracısının bu tür sertifikalarla çalıştığı için, aynı Ayırt Edici Adlara sahip iki ya da daha fazla sertifikayı tek bir anahtar deposu dosyasında koymaktan kaçınmalısınız.
- IBM WebSphere MQ Version 7.5 kaynak bağdaştırıcısı IBM WebSphere MQ Advanced Message Security' i desteklemiyor. Bir uygulama sunucusu ortamında çalışan IBM WebSphere MQ classes for JMS ya da IBM WebSphere MQ classes for Java uygulamalarıyla birlikte kullanılması gereken ileti koruması gerekiyorsa:
  - Uygulama sunucusu, Version 8.0 ya da daha sonraki bir kaynak bağdaştırıcısını kullanacak şekilde yapılandırılmalıdır.
  - Ya da Message Channel Agent (MCA) ara başlangıcı kullanılmalıdır.

Kullanıcı senaryoları

Gelişmiş İleti Güvenliğiile elde edebildiğiniz iş hedeflerini anlamak için olası senaryolar hakkında bilgi edinmenizi sağlar.

Quick Start Guide for Windows altyapıları

Use this guide to quickly configure IBM Gelişmiş İleti Güvenliği to provide message security on Pencereler 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 WebSphere MQ özellikleri başlıklı konuya bakın.

Uygun WebSphere MQ komutlarının işletim sistemi tarafından konumlandırılması ve yürütülebilmesi için, **setmqenv** komutunun kullanılmasıyla ilgili bilgi edinmek için setmqenvbaşlıklı konuya bakın.

1. Kuyruk yöneticisi ve kuyruk yaratılması

Bu görev hakkında

Aşağıdaki örneklerin tümü, uygulamalar arasında ileti geçirmesi için TEST.Q adlı bir kuyruk kullanır. Gelişmiş İleti Güvenliği İletilerin, standart WebSphere MQ arabirimi aracılığıyla WebSphere MQ altyapısına girdikleri noktada iletileri imzalamak ve şifrelemek için kullanımları kullanılır. Temel kurulum WebSphere MQ içinde yapılır ve aşağıdaki adımlarda yapılandırılır.

You can use WebSphere 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 \WebSphere 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 koymasına da 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
```

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 270.

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

“Java istemcileri için Hızlı Başlama Kılavuzu” sayfa 277 ' a bakın). Diğer tüm diller ve yerel bağ tanımları kullanan Java uygulamaları için bu kılavuzdaki adımlar doğru olur.

Yordam

1. Kullanıcı `alice`için yeni bir anahtar veritabanı yaratmak üzere IBM Key Management GUI 'sini (`strmqikm.exe`) kullanın.

   ```
   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. **New Self Signed**(Yeni Otomatik İmza) seçeneğini belirleyin; bu senaryoda kendinden imzalı sertifikalar 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

Gelişmiş İleti Güvenliği izlemelerini anahtar veritabanlarının ve sertifikaların located.This olduğu dizine, bu bilgilerin düz metin biçiminde tutan `keystore.conf` dosyası aracılığıyla gerçekleştirilmesini işaretlemelisiniz. Her kullanıcının 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, 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. “Anahtar deposu yapılandırma dosyasının yapısı (keystore.conf)” sayfa 287.
- *%HOMEDRIVE%\%HOMEPATH%*\.mqs\keystore.conf (örn. C:\Documents and Settings\alice\.mqs\keystore.conf), Gelişmiş İleti Güvenliği 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 286.
- `.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/alice/AMS/bobkey.kdb" -pw passw0rd
   -label Bob_Cert -target bob_public.arm

   runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/alicekey.kdb" -pw passw0rd -label
   Bob_Cert -file bob_public.arm
   ```

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` işareti. 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.

Quick Start Guide for UNIX platforms

Use this guide to quickly configure IBM Gelişmiş İleti Güvenliği to provide message security on UNIX 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 bileşenlerin kurulu olması gerekir:

- Yürütme Ortamı
- Sunucu
- Örnek programlar
- IBM Global Security Kit
- MQ Advanced Message Security

Her bir altyapıda bileşen adları için aşağıdaki konulara bakın:

- Linux sistemleri içinIBM WebSphere MQ bileşenleri
- HP-UX sistemleri içinIBM WebSphere MQ bileşenleri

- AIX sistemleri içinIBM WebSphere MQ bileşenleri
- Solaris sistemleri içinIBM WebSphere 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. Gelişmiş İleti Güvenliği İletilerin, standart WebSphere MQ arabirimi aracılığıyla WebSphere MQ altyapısına girdikleri noktada iletileri imzalamak ve şifrelemek için kullanımları kullanılır. Temel kurulum WebSphere MQ içinde yapılır ve aşağıdaki adımlarda yapılandırılır.

You can use WebSphere 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_INSTALL_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.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 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 koymasına da 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
```

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 276.

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 “Java istemcileri için Hızlı Başlama Kılavuzu” sayfa 277 ' a bakın). Diğer tüm diller ve yerel bağ tanımları kullanan Java uygulamaları için bu kılavuzdaki adımlar doğru olur.

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

Gelişmiş İleti Güvenliği algılayıcılarını, anahtar veritabanlarının ve sertifikaların bulunduğu dizine işaretlemelisiniz. 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 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 = /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. “Anahtar deposu yapılandırma dosyasının yapısı (keystore.conf)” sayfa 287.
- `HOME/.mqs/keystore.conf` varsayılan konumdur; burada Gelişmiş İleti Güvenliği , `keystore.conf` dosyasını arar. `keystore.conf`için varsayılan olmayan bir konumu nasıl kullanabilmeye ilişkin bilgi için bkz. “Anahtar depolarının ve sertifikaların kullanılması” sayfa 286.

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` işareti. 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.

Java istemcileri için Hızlı Başlama Kılavuzu

İstemci bağ tanımlarını kullanarak bağlanan Java uygulamaları için ileti güvenliği sağlamak üzere IBM Gelişmiş İleti Güvenliği 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 kurulu 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. Gelişmiş İleti Güvenliği İletilerin, standart WebSphere MQ arabirimi aracılığıyla WebSphere MQ altyapısına girdikleri noktada iletileri imzalamak ve şifrelemek için kullanımları kullanılır. Temel kurulum WebSphere 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

Senaryomuzda 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. Altyapınıza ilişkin **Hızlı Başlama Kılavuzu** ' nda (Windows ya da UNIX) açıklandığı gibi iki kullanıcıyı yaratın.
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
```

3. Ayrıca, iki kullanıcının sistem ilke kuyruğuna göz atmasına ve iletileri hata kuyruğuna koymasına da 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
```

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 281.

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 'da yazılmış örnek uygulamaları kullanırız. Yerel bağ tanımlarını ya da C uygulamalarını kullanarak Java uygulamalarını kullanmayı planlıyorsanız, **runmqakm** komutunu kullanarak bir CMS anahtar deposu ve sertifikalar yaratmanız gerekir. Bu, **Hızlı Başlangıç Kılavuzu** ' nda (Windows ya da UNIX) gösterilir.

Yordam

1. Anahtar deponunuzu yaratmak için bir dizin yaratın (örneğin, `/home/alice/.mqs`). Altyapınıza ilişkin **Hızlı Başlama Kılavuzu** (Windows ya da UNIX) tarafından kullanılan dizinde bu değeri yaratmak isteyebilirsiniz.

   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 onaylı sertifika kullanmamanız önerilir, ancak bunun yerine bir Sertifika Yetkilisi tarafından imzalanan sertifikalara güvenmeniz önerilir.
- `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 'te, 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

Gelişmiş İleti Güvenliği algılayıcılarını, anahtar veritabanlarının ve sertifikaların bulunduğu dizine işaretlemelisiniz. 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` will be 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 will be 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.
- If you already have a `keystore.conf` because you have followed **Hızlı Başlama Kılavuzu** (Pencereler or UNIX), you can edit the existing one to add in the above lines.
- Daha fazla bilgi için, bkz. “Anahtar deposu yapılandırma dosyasının yapısı (keystore.conf)” sayfa 287.

5. Sertifikaları Paylaşma

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 Keyman (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, WebSphere 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: WebSphere MQ kurulumunda sağlanan Java sürümünün bu ilke dosyaları zaten var. *MQ_INSTALLATION_PATH*/java/biniçinde bulunabilir.

Bu görev hakkında

Farklı kullanıcıların altında farklı programlar çalıştırarak, uygulamanın doğru yapılandırılıp yapılandırıldığını doğrulayabilirsiniz. Farklı kullanıcılar altındaki programların çalıştırılmasına ilişkin ayrıntılar için, altyapınıza ilişkin **Quick Start Guide** (Hızlı Başlangıç Kılavuzu) (Windows ya da UNIX) adlı belgeye bakın.

Yordam

1. To run these JMS sample applications, use the CLASSPATH setting for your platform as shown in JMS için IBM WebSphere MQ sınıfları tarafından 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 kuyruk bağlantılarını tam olarak korumak için, aynı ilkenin uzak kuyruğunda ve iletilerin iletileceği yerel kuyruğda ayarlanması gerekir.

Bir ileti uzak bir kuyruğa konduğunda, Gelişmiş İleti Güvenliği , işlemi algılar ve iletiyi uzak kuyruk için belirlenen bir ilke kümesine göre işler. Örneğin, bir şifreleme ilkesi için, ileti, bunu işlemek için WebSphere MQ ' a iletilmeden önce şifrelenir. Gelişmiş İleti Güvenliği , uzak bir kuyruğa konulan iletiyi işledikten sonra, WebSphere MQ bu iletiyi ilişkili iletim kuyruğuna koyar ve hedef kuyruk yöneticisine ve hedef kuyruğa iletir.

Yerel kuyruğunda bir GET işlemi gerçekleştirildiğinde, Gelişmiş İleti Güvenliği , yerel kuyruklardaki ilke kümesine göre iletinin kodunu 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 Gelişmiş İleti Güvenliği roll-out has been completed.

İlgili başvurular

setmqspl (güvenlik ilkesini ayarla)

WebSphere Message Broker olanağını kullanarak korunan iletiler yöneltilmesi

IBM Gelişmiş İleti Güvenliği can protect messages in an infrastructure where WebSphere Message Broker version 8.0.0.1 (or later) is installed. WebSphere Message Broker ortamında güvenliği uygulamadan önce her iki ürünün doğasını da anlamanız gerekir.

Bu görev hakkında

Gelişmiş İleti Güvenliği , 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. Bu, WebSphere Message Broker aracılığıyla akan iletileri güvenli kılmak için, WebSphere Message Broker 'ın iletileri bilmeden iletileri işlemesine izin verebilir (1. senaryo) ya da ileti alma ve gönderme yetkisi olan bir yetkili kullanıcı haline getirilebilir (2. senaryo).

Senaryo 1-Message Broker ileti içeriğini göremiyor

Başlamadan önce

WebSphere Message Broker 'ın 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 `QIN`yerleştirir. 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 Gelişmiş İleti Güvenliği protects only the message payload and not its headers and properties which remain unprotected and can be read by WebSphere Message Broker. Gelişmiş İleti Güvenliği yalnızca *alice*, *bob* ve *cecil*tarafından kullanılır. WebSphere Message Broker olanağını kurmak ya da yapılandırmak gerekli değildir.

WebSphere Message Broker, 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, WebSphere Message Broker tarafından yönlendirilir ve hedef kuyruğa değiştirilmeden gelir. Bu nedenle, özgün yazar (*bob* ve *cecil* tarafından yalnızca *alice*tarafından gönderilen iletileri kabul eder) ve daha önce olduğu gibi korunan (yalnızca *bob* ve *cecil* tarafından okunabilen iletileri kabul eder)) tarafından imzalanır. WebSphere Message Broker, yönlendirilmiş iletiyi korunmayan bir diğer ada yerleştirir. Alıcılar, korunan bir çıkış kuyruğundan iletiyi alır; burada IBM WebSphere MQ AMS , iletiyi saydam bir şekilde şifresini çözer.

Yordam

1. Configure *alice*, *bob* and *Cecil* to use Gelişmiş İleti Güvenliği 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 `QDEF`adlı yerel kuyrukları tanımlayın.

[1] Cecil's

```
DEFINE QLOCAL(QIN)
```

5. QIN kuyruğuna ilişkin 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.

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. WebSphere Message Broker 'da, 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 WebSphere Message Broker 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. Bu, AIN diğer ad kuyruğundan WebSphere Message Broker tarafından korunan biçimde alınır. WebSphere Message Broker decides where to route

the message reading the `routeTo` property which is, as all properties, not encrypted. WebSphere Message Broker, iletiyi daha fazla korumadan uzak bir korunmayan diğer ada yerleştirir. Kuyruktan *bob* ya da *cecil* tarafından alındığında, iletinin şifresi çözülüyor ve dijital imza doğrulanır.

2. senaryo-Message Broker ileti içeriğini görebilirler

Bu görev hakkında

Bu senaryoda, bir grup kişinin WebSphere Message Broker 'a ileti göndermesine izin verilir. Başka bir grup, WebSphere Message Broker tarafından yaratılan iletileri alma yetkisine sahip olur. Taraflar ve WebSphere Message Broker arasındaki iletim yeniden gönderilemeyecek.

WebSphere Message Broker 'ın koruma ilkelerini ve sertifikalarını yalnızca bir kuyruk açıldığı zaman 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 WebSphere Message Broker is considered an authorized party allowed to read or sign the message payload, you must configure Gelişmiş İleti Güvenliği for the user starting the WebSphere Message Broker service. Be aware it is not necessarily the same user who puts/gets the messages onto queues nor the user creating and deploying the WebSphere Message Broker applications.

Yordam

1. Configure *alice*, *bob*, *Cecil* and *dave* and the WebSphere Message Broker service user, to use Gelişmiş İleti Güvenliği 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. WebSphere Message Broker hizmeti kullanıcısına *alice*, *bob*, *Cecil* ve *Dave's* sertifikalarını sağlayın.

   Bu işlemi, *alice*, *bob*, *Cecil* ve *dave*olarak tanımlayan sertifikaların her birinin dış dosyalarına çekerek, çıkarılan sertifikaları WebSphere Message Broker anahtar deposuna ekleyerek yapın. **Görev 5 'te açıklanan yöntemi kullanmanız önemlidir. Hızlı Başlama Kılavuzu (Windows ya da UNIX) içindeSertifikaları Paylaşma** .
3. WebSphere Message Broker hizmeti kullanıcısının sertifikasını *alice*, *bob*, *Cecil* ve *dave*olarak sağlayın.

   Bunu, önceki adımda belirtilen yöntemi kullanarak yapın.

   Not: *Alice.* and *bob* need the WebSphere Message Broker service user's certificate to encrypt the messages correctly. WebSphere Message Broker hizmeti kullanıcısının, iletilerin yazarlarını doğrulamak için *alice's* ve *bob's* sertifikalarına gerek vardır. WebSphere Message Broker hizmeti kullanıcısı, iletileri şifrelemek için *Cecil's* ve *Dave's* sertifikalarına gerek duyar. *Cecil* and *dave* need the WebSphere Message Broker service user's certificate to verify if the message comes from WebSphere Message Broker.
4. Define a local queue named `IN` and define the security policy with *alice* and *bob* specified as authors and WebSphere Message Broker's service user specified as recipient:

   ```
   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. Define a local queue named `OUT` and define the security policy with WebSphere Message Broker's service user specified as author and *Cecil* and *dave* specified as recipients:

   ```
   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. WebSphere Message Broker olanağında, `MQInput` ve `MQOutput` düğümü içeren bir ileti akışı yaratın. Configure the `MQInput` node to use the `IN` queue and the `MQOutput` node to use the `OUT` queue.
7. İleti akışını WebSphere Message Broker 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 WebSphere Message Broker to read it. WebSphere Message Broker yalnızca *alice* ve *bob* ' dan gelen iletileri kabul eder ve diğerlerini reddedecektir. The accepted messages will be 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, WebSphere Message Broker tarafından imzalanmamış iletiler reddedilir.

IBM WebSphere MQ Advanced Message Security ile IBM WebSphere MQ Managed File Transferkomutunu kullanma

Bu senaryo, bir IBM WebSphere MQ Managed File Transferaracılığıyla gönderilen veriler için ileti gizliliği sağlamak üzere Gelişmiş İleti Güvenliği ürününü nasıl yapılandıracağını açıklar.

Başlamadan önce

Korumak istediğiniz IBM WebSphere MQ Managed File Transfer tarafından kullanılan kuyrukları barındıran WebSphere MQ kurulumunda Gelişmiş İleti Güvenliği bileşeniniz olduğundan emin olun.

IBM WebSphere MQ Managed File Transfer aracılarınız bağ tanımları moduna bağlanıyorsa, GSKit bileşeninin yerel kuruluşlarında kurulu olduğundan da emin olun.

Bu görev hakkında

İki IBM WebSphere MQ Managed File Transfer aracısı arasında veri aktarımı kesintiye uğradığında, aktarımın yönetilmesi için kullanılan temeldeki WebSphere MQ kuyruklarında gizli veriler korunmasız olarak kalabilir. Bu senaryoda, IBM WebSphere MQ Managed File Transfer kuyruklarında bu tür verileri korumak için Gelişmiş İleti Güvenliği olanağının nasıl yapılandırılacağı ve kullanılacağı açıklanır.

In this scenario we consider a simple topology comprising one machine with two IBM WebSphere MQ Managed File Transfer queues and two agents, `AGENT1` and `AGENT2`, sharing a single queue manager, `hubQM`, as described in the scenario Komut dosyalarını kullanarak temel dosya aktarımı. 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 IBM WebSphere MQ Managed File Transfer agent processes. Kendi kullanıcı ve grup adlarınızı kullanıyorsanız, komutları uygun şekilde değiştirin.

Bu görev hakkında

Gelişmiş İleti Güvenliği , korunan kuyruklardaki iletileri imzalamak ve/ya da şifrelemek için genel anahtar şifrelemesi kullanır.

Not:

- IBM WebSphere MQ Managed File Transfer aracılarınız bağ tanımları kipinde çalışıyorsa, bir CMS (Şifreleme İletisi Sözdizimi) anahtar deposu oluşturmak için kullandığınız komutlar, altyapınıza ilişkin **Hızlı Başlangıç Kılavuzu** ' nda (Windows ya da UNIX) ayrıntılı bir şekilde açıklanmıştır.
- IBM WebSphere MQ Managed File Transfer aracılarınız istemci kipinde çalışıyorsa, bir JKS (Java Anahtar Deposu) yaratmak için gereksinim duyacak komutlar “Java istemcileri için Hızlı Başlama Kılavuzu” sayfa 277' 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=IBM, L=Hursley, ST=Hampshire, C=GB
   ```

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 IBM WebSphere MQ 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=IBM,
   L=Hursley, ST=Hampshire, C=GB"
   -e AES128 -r "CN=ftagent, OU=MFT, O=IBM, L=Hursley, ST=Hampshire, C=GB"
   ```

3. IBM WebSphere MQ Managed File Transfer aracı işlemini çalıştıran kullanıcının, sistem ilke kuyruğuna göz atmak ve iletileri hata kuyruğuna koymak için erişimi 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 IBM WebSphere MQ 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.

kurmaIBM WebSphere MQ Advanced Message Security

Install the IBM WebSphere MQ Advanced Message Security component on various platforms.

Bu görev hakkında

Tam kuruluş yordamları için bkz. Installing IBM WebSphere MQ Advanced Message Security.

İlgili görevler

kaldırmaIBM WebSphere MQ Advanced Message Security

Anahtar depolarının ve sertifikaların kullanılması

WebSphere MQ uygulamalarına şeffaf şifreleme koruması sağlamak için, Gelişmiş İleti Güvenliği , ortak anahtar sertifikalarının ve bir özel anahtarın saklandığı anahtar deposu dosyasını kullanır.

Gelişmiş İleti Güvenliği' 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.

Anahtar deposunun yeri, varsayılan olarak `keystore.conf` olan anahtar deposu yapılanış kütüğünde bulunur. Her bir Gelişmiş İleti Güvenliği kullanıcısı, bir anahtar deposu dosyasını işaret eden anahtar deposu yapılandırma dosyasına sahip olmalıdır. Gelişmiş İleti Güvenliği Anahtar deposu dosyalarının şu biçimini kabul eder: `.kdb`, `.jceks`, `.jks`.

`keystore.conf` dosyasının varsayılan konumu şöyledir:

- UNIX altyapılarında: `$HOME/.mqs/keystore.conf`
- Windows altyapılarında: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

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`*

    Not: Birden çok sürücü harfi kullanılabiliyorsa, Windows ' taki yol, sürücü harfini belirtmeli ve bu harfle ilgili bir değer belirtmelidir.

İlgili kavramlar

“Gönderen ayırt edici adları” sayfa 300
Gönderen ayırt edici adları (DN), bir kuyruğa ileti yerleştirmek için yetki verilen kullanıcıları tanımlar.

“Alıcı ayırt edici adları” sayfa 301
Alıcı ayırt edici adları (DN), kuyruktan ileti alma yetkisi olan kullanıcıları tanımlar.

Anahtar deposu yapılandırma dosyasının yapısı (keystore.conf)

The keystore configuration file (`keystore.conf`) points Gelişmiş İleti Güvenliği to the location of the appropriate keystore.

İki tip yapılandırma CMS ve Java (JKS ve JCEKS) vardır. CMS configuration entries are prefixed with `cms.` and Java are prefixed with `jks.` or `jceks.` depending on the type of a keystore.

Yapılandırma dosyası, yapılandırma dosyasının tipine bağlı olarak aşağıdaki yapılardan birine sahip olabilir:

```
cms.keystore = /<dir>/<keystore_file>
cms.certificate = certificate_label

jceks.keystore = <dir>/Keystore
jceks.certificate = <certificate_label>
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE

jks.keystore = <dir>/Keystore
jks.certificate = <certificate_label>
jks.encrypted = no
jks.keystore_pass = <password>
jks.key_pass = <password>
jks.provider = IBMJCE
```

Yapılanış dosyası değiştirgeleri aşağıdaki gibi tanımlanır:

keystore
Anahtar deposu dosyasının yolu.

Önemli:

- Anahtar deposu dosyasının yolu dosya uzantısını içermemelidir.

- Java anahtar deposu dosyaları için IBM WebSphere MQ AMS , şu dosya biçimlerini destekler: `.jks`, `.jceks`, `.jck`.

`certificate`
Sertifika etiketi.

`encrypted`
Parolanın durumu.

`keystore_pass`
Anahtar deposu dosyasına ilişkin parola.

Not:

- CMS anahtar deposu için IBM WebSphere MQ AMS , (`.sth`)zula dosyalarına dayanır; JKS ve JCEKS, hem sertifika hem de kullanıcının özel anahtarı için bir parola gerektirebilir.
- Parolaları düz metin olarak depolamak bir güvenlik riskidir.

`key_pass`
Kullanıcının özel anahtarı için parola.

Önemli: Parolaları düz metin biçiminde depolamak bir güvenlik riski oluşturabilir.

`provider`
Anahtar deposu sertifikasının gerektirdiği şifreleme algoritmalarını uygulayan Java güvenlik sağlayıcısı.

Not: Şu anda IBMJCE, Gelişmiş İleti Güvenliğitarafından desteklenen tek sağlayıcısıdır.

Önemli: Anahtar deposunda saklanan bilgiler, WebSphere MQkullanılarak gönderilen verilerin güvenli akışı için çok önemlidir. Bu nedenle, güvenlik yöneticilerinin bu dosyalara dosya izinleri atarken özellikle dikkat etmesi gerekir.

Aşağıda, `keystore.conf` dosyasına ilişkin bir örnek yer alıyor:

```
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE
```

İlgili görevler

“Parolaları Java 'da koruma” sayfa 298
Anahtar deposu ve özel anahtar parolalarının düz metin olarak saklanması, bu nedenle Gelişmiş İleti Güvenliği olanağının, anahtar deposu dosyasında bulunan bir kullanıcının anahtarını kullanarak bu parolaları karıştırabilecek bir araç sağladığına ilişkin bir risk oluşturur.

Message Channel Agent (MCA) etkileşimi

MCA etkileşimi, IBM WebSphere MQ altında çalışan bir kuyruk yöneticisinin, sunucu bağlantı kanalları için ilkelerin uygulanmasını geçerli bir şekilde etkinleştirmesini sağlar.

MCA etkileşimi, IBM WebSphere MQ 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 IBM WebSphere MQ AMS capability when IBM WebSphere MQ AMS cannot be enabled at the client. MCA ' yı algılamayı ve bir IBM WebSphere MQ AMSetkin istemciyi kullanarak, uygulama almak için sorunlu olabilecek iletilerin iki kez korunmasını sağlayan bir müşteri adayını göz önünde bulundurun.

Ürünün önceki bir sürümünden bir kuyruk yöneticisine bağlanmak için Version 7.5 ya da daha sonraki bir istemci kullanıyorsanız, `2085 (MQRC_UNKNOWN_OBJECT_NAME)` hatası bildirilirse, istemcide IBM

WebSphere MQ Advanced Message Security ' i devre dışı bırakmanız gerekir. Daha fazla bilgi için, bkz. “İstemcide IBM WebSphere MQ Advanced Message Security devre dışı bırakılması” sayfa 291.

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. IBM WebSphere MQ AMS anahtar deposunun yapılandırılmasıyla ilgili daha fazla bilgi için bkz. “Anahtar depolarının ve sertifikaların kullanılması” sayfa 286.

MCA ' yı yeniden başlatma özelliğini etkinleştirmek için, anahtar deposu yapılandırma dosyasında kullanmak istediğiniz bir kanal adını sağlamanız gerekir. MCA başlangıcında, yalnızca bir cms anahtar deposu tipi kullanılabilir.

MCA ' nın algılanmasını ayarlama gibi bir örnek için bkz. “IBM WebSphere MQ AMS MCA başlangıcı örneği” sayfa 289.

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 WebSphere MQ AMS MCA başlangıcı örneği

IBM WebSphere MQ AMS MCA ' yı nasıl ayarladığınızı 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.

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 Version 7.5öncesinde, IBM WebSphere MQ AMS , uygulamaları korumak için ayrı olarak kurulmuş ve kesiciler için gerekli olan bir eklenti üründü. From Version 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 Version 7.5 ya da daha sonraki bir istemci kullansaydı, iletinin iki kez korunmasına neden olur; MQ istemcisi yürütme ortamı algılayıcısı ve MCA dinleyici, iletiyi MQ' ya geldiği 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/mq75
KEYSTORELOC=/home/testusr/ssl/ams1
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64
```

```
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd
-label bob_cert  -dn "cn=bob,O=IBM,c=IN"  -default_cert yes
```

2. 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 Version 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 WebSphere MQ Version 7.5 installation:

```
/opt/mq75/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 WebSphere MQ Version 7.5 kurulumundan çalıştırın:

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

İlgili görevler

"Java istemcileri için Hızlı Başlama Kılavuzu" sayfa 277
İstemci bağ tanımlarını kullanarak bağlanan Java uygulamaları için ileti güvenliği sağlamak üzere IBM Gelişmiş İleti Güvenliği 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 sınırlamalar" sayfa 265
IBM WebSphere MQ Advanced Message Securityile ilgili sınırlamalar hakkında bilgi edinin.

İstemcide IBM WebSphere MQ Advanced Message Security devre dışı bırakılması

Ürünün önceki bir sürümünden bir kuyruk yöneticisine bağlanmak için Version 7.5 ya da daha sonraki bir istemci kullanıyorsanız ve 2085 (MQRC_UNKNOWN_OBJECT_NAME) hatası bildirilirse, istemcide IBM WebSphere MQ Advanced Message Security (AMS) özelliğini devre dışı bırakmanız gerekir.

Bu görev hakkında

Version 7.5' tan IBM WebSphere MQ Advanced Message Security (AMS), bir IBM WebSphere MQ istemcisinde otomatik olarak etkinleştirilir; bu nedenle, istemci varsayılan olarak kuyruk yöneticisinde nesnelere ilişkin güvenlik ilkelerini denetmeye çalışır. Ancak, ürünün önceki sürümlerindeki sunucular (örneğin, Version 7.1gibi), 2085 (MQRC_UNKNOWN_OBJECT_NAME) hatasının bildirilmesine neden olan AMS etkinleştirilmemiş.

Bu hata bildirilirse, ürünün önceki bir sürümünden bir kuyruk yöneticisine bağlanmayı denerken, aşağıdaki gibi istemcide AMS ' i devre dışı bırakabilirsiniz:

- Java istemcileri için aşağıdaki yöntemlerden birini kullanın:
  - V7.5.0.4 Bir ortam değişkeni AMQ_DISABLE_CLIENT_AMS ayarlanarak.
  - V7.5.0.4 By setting the Java system property com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - V7.5.0.5 DisableClientAMS özelliğini kullanarak, `mqclient.ini` dosyasındaki **`Security`** stanza altında.
- C istemcileri için aşağıdaki yöntemlerden birini kullanın:
  - V7.5.0.4 Bir ortam değişkeni AMQ_DISABLE_CLIENT_AMS ayarlanarak.
  - V7.5.0.5 DisableClientAMS özelliğini kullanarak, `mqclient.ini` dosyasındaki **`Security`** stanza altında.

Yordam

- İstemcide AMS olanağını devre dışı bırakmak için aşağıdaki seçeneklerden birini kullanın:

  V7.5.0.4 **AMQ_DISABLE_CLIENT_AMS ortam değişkeni**

  Bu değişkeni aşağıdaki durumlarda ayarlamanız gerekir:

  - IBM Java Runtime Environment (JRE) dışında Java Runtime Environment (JRE) kullanıyorsanız
  - Version 7.5ya da daha sonraki bir sürümü kullanıyorsanız, IBM WebSphere MQ classes for Java ya da IBM WebSphere MQ classes for JMS istemcisini kullanın.

  C istemcilerine ilişkin AMS işlevlerini geçersiz kılmak için AMQ_DISABLE_CLIENT_AMS seçeneğini de kullanabilirsiniz.

AMQ_DISABLE_CLIENT_AMS ortam değişkenini yaratın ve uygulamanın çalıştırıldığı ortamda TRUE olarak ayarlayın. Örneğin:

```
export AMQ_DISABLE_CLIENT_AMS=TRUE
```

V 7.5.0.4 com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS sistem özelliği

For IBM WebSphere MQ classes for JMS and IBM WebSphere MQ classes for Java clients, set the Java system property com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS to the value TRUE for the Java application.

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.

V 7.5.0.5 `mqclient.ini` dosyasındaki`DisableClientAMS` özelliği

For IBM WebSphere MQ classes for JMS and IBM WebSphere MQ classes for Java clients, and for C clients, 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 korunan kuyrukları açılmasına ilişkin sorunlar hakkında daha fazla bilgi için bkz. “JMSkullanılırken korunan kuyruklar açılırken birden çok sorun oluştu” sayfa 314.

İlgili kavramlar

“Message Channel Agent (MCA) etkileşimi” sayfa 288
MCA etkileşimi, IBM WebSphere MQ altında çalışan bir kuyruk yöneticisinin, sunucu bağlantı kanalları için ilkelerin uygulanmasını geçerli bir şekilde etkinleştirmesini sağlar.

İlgili görevler

Yapılandırma dosyası kullanarak istemci yapılandırılması

İlgili başvurular

IBM WebSphere MQ classes for JMS yapılandırma dosyası

AMS için sertifika gereksinimleri

Sertifikaların Gelişmiş İleti Güvenliğiile kullanılabilmesi için RSA genel anahtarı olmalıdır.

Farklı genel anahtar tipleri ve bunların nasıl yaratılacağı hakkında daha fazla bilgi için bkz. “Digital certificates and CipherSpec compatibility in IBM WebSphere MQ” sayfa 33.

Anahtar kullanım uzantıları

Anahtar kullanım uzantıları, bir sertifikenin kullanılabileceği şekilde ek sınırlamalar sağlar.

Gelişmiş İleti Güvenliğiiçinde, anahtar kullanımı şu şekilde ayarlanmalıdır: Koruma bütünlüğü kalitesi için kullanılan X.509 V3 ya da sonraki bir standarda ilişkin sertifikalar için, anahtar kullanım uzantıları ayarlanmışsa, bu iki kişinin en az birini içermelidir:

- **`nonRepudiation`**

- **digitalSignature**

Koruma gizliliğinin kalitesi için, temel kullanım uzantıları ayarlandıysa, bu uzantıların **keyEncipherment** uzantısını da içermesi gerekir.

İlgili kavramlar

“Koruma kalitesi” sayfa 302
Gelişmiş İleti Güvenliği veri koruma ilkeleri, bir koruma kalitesi (QOP) anlamına gelir.

IBM WebSphere MQ Advanced Message Securityiçinde sertifika geçerlilik denetimi yöntemleri

Kuyruklarınıza ilişkin iletilerin güvenlik standartlarını yerine getirmeyen sertifikalar kullanılarak korunmamasını, iptal etmek ve reddetmek için IBM WebSphere MQ Advanced Message Security ' u kullanabilirsiniz.

IBM WebSphere MQ AMS , bir sertifikanın geçerliliğini Online Certificate Status Protocol (OCSP) ya da sertifika iptal listesi (CRL) kullanarak doğrulamanıza olanak tanır.

IBM WebSphere MQ AMS , OCSP ya da CRL denetimi için yapılandırılabilir ya da her ikisi için de yapılandırılabilir. Her iki yöntem de etkinleştirilmişse, performans nedenlerinden dolayı IBM WebSphere MQ AMS önce iptal durumu için OCSP ' yi kullanır. Bir sertifikana ilişkin iptal durumu OCSP denetlemesinden sonra belirlenmezse, IBM WebSphere MQ AMS CRL denetimini kullanır.

İlgili kavramlar

“OCSP (Çevrimiçi Sertifika Durumu Protokolü)” sayfa 293
OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü), bir sertifikanın iptal edilip edilmediğini belirler ve sertifikanın güvenilir olup olmadığını belirlemeye yardımcı olur.

“Sertifika İptal Listeleri (CRL'ler)” sayfa 295
CRL ' ler, Sertifika Yetkilisi (CA) tarafından, artık çeşitli nedenlerle güvenilmediği için, özel anahtar kaybedilmiş ya da tehlikeye atıldığı sertifikaların bir listesini içerir.

OCSP (Çevrimiçi Sertifika Durumu Protokolü)

OCSP (Online Certificate Status Protocol; Çevrimiçi Sertifika Durumu Protokolü), bir sertifikanın iptal edilip edilmediğini belirler ve sertifikanın güvenilir olup olmadığını belirlemeye yardımcı olur.

Yerel algılayıcılarda OCSP denetlemesi etkinleştiriyor

Gelişmiş İleti Güvenliği' ta Online Certificate Status Protocol (OCSP) denetimini etkinleştirmek için anahtar deposu yapılandırma dosyasını değiştirmeniz gerekir.

Yordam

Anahtar deposu yapılanış kütüğüne aşağıdaki seçenekleri ekleyin:

Not: Çizelgede sağlanan tek tek seçenekler için değerler varsayılan değerlerdir.

Aşağıdaki değerlerden birini belirlemelisiniz:

- `ocsp.enable=on`
- `ocsp.url=<`*`reposnder_URL`*`>`
- `ocsp.http.proxy.host=<`*`OCSP_proxy`*`>`

Seçenek	Tanım
`ocsp.enable=off`	Denetlenmekte olan sertifikana, OCSP Responder 'ın bulunduğu yerin URI 'sini içeren bir PKIX_AD_OCSP erişim yöntemi içeren bir Yetki Bilgisi Erişim Uzantısı varsa OCSP denetimini geçerli kılın. Olası değerler: `on`/`off`.

Seçenek	Tanım
`ocsp.url=<reposnder_URL>`	OCSP yanıtlayıcıya ilişkin URL adresi.
`ocsp.http.proxy.host=<OCSP_proxy>`	OCSP yetkili sunucusunun URL adresi.
`ocsp.http.proxy.port=<port_number>`	OCSP yetkili sunucusunun kapı numarası.
`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.
`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), Gelişmiş İleti Güvenliği zamanaşımına neden olur.

Java 'da OCSP denetiminde etkinleştirme
OCSP checkin for Java olanağını Gelişmiş İleti Güvenliğiolanağında etkinleştirmek için, `java.security` dosyasını ya da anahtar deposu yapılanış kütüğünü değiştirin.

Bu görev hakkında

There are two ways of enabling OCSP checking in Gelişmiş İleti Güvenliği:

java.securitykullanılıyor
Sertifikanız için Yetki Bilgileri Erişimi (AIA) ayarının olup olmadığını 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";
```

Sertifika İptal Listeleri (CRL'ler)

CRL ' ler, Sertifika Yetkilisi (CA) tarafından, artık çeşitli nedenlerle güvenilmediği için, özel anahtar kaybedilmiş ya da tehlikeye atıldığı sertifikaların bir listesini içerir.

Sertifikaları doğrulamak için Gelişmiş İleti Güvenliği , imzalayanın sertifikasından ve sertifika yetkilisinin (CA ' lar) sertifika zincirinden bir güven çıpası ile oluşan bir sertifika zincirini oluşturur. Güven çıpası, bir sertifikanın güvenilirini göstermek için kullanılan güvenilir bir sertifika ya da güvenilir kök sertifika içeren güvenilir bir anahtar deposu dosyasıdır.IBM WebSphere MQ AMS Bir PKIX doğrulama algoritması kullanarak sertifika yolunu doğrular. Zincir oluşturulduğunda ve doğrulandığında, IBM WebSphere MQ 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. Uzantıya sertifikana uzantı eklenirse, IBM WebSphere MQ AMS , **digitalSignature** ya da **nonRepudiation** da ayarlanıp ayarlanmadığını doğrular. Bunlar değillerse, `MQRC_SECURITY_ERROR` raporlanır ve günlüğe kaydedilir. Daha sonra, IBM WebSphere MQ AMS kütüklerden CRL 'leri ya da yapılanış kütüğünde belirtilen değerlere bağlı olarak LDAP' den CRL ' leri karşıdan yükler. Yalnızca DER biçiminde kodlanan CRL ' ler IBM WebSphere MQ AMStarafından desteklenir. Anahtar deposu yapılandırma dosyasında CRL ile ilgili bir yapılandırma bulunmazsa, IBM WebSphere MQ AMS , CRL geçerlilik denetimi gerçekleştirmez. Her CA sertifikası için IBM WebSphere MQ AMS , CRL 'yi bulmak için CA' nın Ayırt Edici Adları 'nı kullanarak CRL 'ler için LDAP' yi 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

Gelişmiş İleti Güvenliği 'ın LDAP (Lightweight Directory Access Protocol; Temel Dizin Erişimi Protokolü) sunucusundan CLRS' yi yükleyebilmesi için anahtar deposu yapılandırma dosyasını değiştirmeniz gerekir.

Yordam

Yapılanış kütüğüne aşağıdaki seçenekleri ekleyin:

Not: Çizelgede sağlanan tek tek seçenekler için değerler varsayılan değerlerdir.

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. IBM WebSphere MQ AMS Java yakalayıcısı 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.
`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 bekleme süresi (saniye olarak), sonra IBM WebSphere MQ AMS zamanaşımlarından sonra gelir.
`crl.http.cache_size=0`	HTTP önbellek boyutu (bayt).

Java 'da sertifika iptal listesi desteğinin etkinleştirilmesi
Gelişmiş İleti Güvenliğiiçinde CRL desteğini etkinleştirmek için anahtar deposu yapılandırma dosyasını, IBM WebSphere MQ AMS 'ın CRL' leri Lightweight Directory Access Protocol (LDAP) sunucusundan CRL ' yi karşıdan yüklemesini ve java.security dosyasını yapılandırmasını sağlamak için 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. IBM WebSphere MQ AMS Java yakalayıcısı 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.

Parolaları Java 'da koruma

Anahtar deposu ve özel anahtar parolalarının düz metin olarak saklanması, bu nedenle Gelişmiş İleti Güvenliği olanağının, anahtar deposu dosyasında bulunan bir kullanıcının anahtarını kullanarak bu parolaları karıştırabilecek bir araç sağladığına ilişkin bir risk oluşturur.

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 286.

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
```

IBM WebSphere MQ Advanced Message Security güvenlik ilkelerinin yönetilmesi

IBM WebSphere MQ Advanced Message Security , kuyruklar boyunca akan iletileri şifrelemek ve doğrulamak için şifreleme şifreleme ve imza algoritmalarını belirtmek üzere güvenlik ilkelerini kullanır.

Güvenlik ilkelerine genel bakış

IBM Gelişmiş İleti Güvenliği güvenlik ilkeleri, bir iletinin şifrelemeyle şifrelendiğini ve imzalanmış olduğunu açıklayan kavramsal nesnelerdir.

Güvenlik ilkesi özniteliklerine ilişkin ayrıntılar için aşağıdaki alt başlıklara bakın:

İlgili kavramlar

“Koruma kalitesi” sayfa 302
Gelişmiş İleti Güvenliği veri koruma ilkeleri, bir koruma kalitesi (QOP) anlamına gelir.

“Güvenlik ilkesi öznitelikleri” sayfa 301
Verileri korumak için belirli bir algoritma ya da yöntem seçmek üzere Gelişmiş İleti Güvenliği olanağını kullanabilirsiniz.

İlke adı
İlke adı, belirli bir Gelişmiş İleti Güvenliği ilkesini ve bu ilkenin geçerli olduğu kuyruğu tanımlayan benzersiz bir addır.

İlke adı, geçerli olduğu kuyruk adıyla aynı olmalıdır. Bir Gelişmiş İleti Güvenliği (IBM WebSphere MQ AMS) ilkesi ile bir kuyruk arasında bire bir eşleme vardır.

Kuyrukla aynı adı taşıyan bir ilke yaratarak, o kuyruğa ilişkin ilkeyi etkinleştirmenizi sağlar. Eşleşen ilke adlarına sahip olmayan kuyruklar IBM WebSphere MQ AMStarafından korunmaz.

İlkenin kapsamı, yerel kuyruk yöneticisiyle ve kuyruklarıyla ilişkilidir. Uzak kuyruk yöneticilerinin, yönettikleri kuyruklar için kendi yerel tanımlı ilkelerinin olması gerekir.

İmza 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.

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.

Gelişmiş İleti Güvenliği 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.

Tolerans

Tolerans özniteliği, IBM Gelişmiş İleti Güvenliği ' in belirtilen güvenlik ilkesi olmayan 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.

Gönderen ayırt edici adları

Gönderen ayırt edici adları (DN), bir kuyruğa ileti yerleştirmek için yetki verilen kullanıcıları tanımlar.

IBM Gelişmiş İleti Güvenliği (IBM WebSphere MQ AMS), ileti alınıncaya kadar, geçerli bir kullanıcı tarafından veri korumalı bir kuyruğa ileti yerleştirilip verilmediğini denetlemez. Bu sırada, ilke bir ya da daha çok geçerli gönderici öngörse ve iletiyi kuyruğa yerleştiren kullanıcı geçerli gönderenler listesinde değilse, IBM WebSphere MQ AMS uygulama alma işlemi için bir hata döndürür ve iletiyi hata kuyruğuna yerleştirir.

Bir ilkenin, 0 ya da daha fazla gönderen DN 'si belirtilmesine neden olabilir. İlke için gönderen ayırt edici adı (DN) belirtilmediyse, kullanıcının sertifikasına güvenilen herhangi bir kullanıcı, veri korumalı iletileri kuyruğa koyabilir.

Gönderen ayırt edici adları aşağıdaki biçimlere 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.
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 yerleştirebilir.
- Gönderen DN ' ler, belirtildiğinde, iletiyi koyan kullanıcıyla ilişkili dijital sertifikada yer alan DN ile tam olarak eşleşmelidir.

- IBM WebSphere MQ AMS , 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 platforms with UTF-8 coding turned on or with the iKeyman utility. Then you must create a policy from a UNIX platform with UTF-8 coding turned on or use the IBM WebSphere MQ AMS plug-in to WebSphere MQ.

İlgili kavramlar

“Alıcı ayırt edici adları” sayfa 301
Alıcı ayırt edici adları (DN), kuyruktan ileti alma yetkisi olan kullanıcıları tanımlar.

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.
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.
- Gelişmiş İleti Güvenliği , 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 platforms with UTF-8 coding turned on or with the iKeyman utility. Then you must create a policy from a UNIX platform with UTF-8 coding turned on or use the Gelişmiş İleti Güvenliği plug-in to WebSphere MQ.

İlgili kavramlar

“Gönderen ayırt edici adları” sayfa 300
Gönderen ayırt edici adları (DN), bir kuyruğa ileti yerleştirmek için yetki verilen kullanıcıları tanımlar.

Güvenlik ilkesi öznitelikleri

Verileri korumak için belirli bir algoritma ya da yöntem seçmek üzere Gelişmiş İleti Güvenliği olanağını kullanabilirsiniz.

Güvenlik ilkesi, bir iletinin şifrelemeyle şifrelenmiş ve imzalanmış olarak nasıl bir ileti olduğunu tanımlayan kavramsal bir nesnedir. Aşağıdaki çizelge, Gelişmiş İleti Güvenliğiiçinde güvenlik ilkesi özniteliklerini gösterir:

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.

Gelişmiş İleti Güvenliği' 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

Gelişmiş İleti Güvenliği , 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

Gelişmiş İleti Güvenliği veri koruma ilkeleri, bir koruma kalitesi (QOP) anlamına gelir.

Gelişmiş İleti Güvenliği içinde üç koruma düzeyi kalitesi, iletiyi imzalamak ve şifrelemek için kullanılan şifreleme algoritmalarına bağlıdır:

- Gizlilik-kuyruğa yerleştirilen iletiler imzalanmış ve şifrelenmelidir.
- Bütünlük-kuyruğa yerleştirilen iletiler gönderici tarafından imzalanmalıdır.
- 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 imza algoritması ya da şifreleme algoritması belirtmeyen bir ilke, NONE (YOK) QOP ' ye sahip. Gelişmiş İleti Güvenliği Bir QOP NONE QOP 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 yönetim görevleri aşağıdaki yerden çalıştırılır:

- UNIX altyapılarında: `<MQInstallRoot>/bin`
- On Pencereler platforms administrative tasks can be run from any location as the PATH environment variable is updated at the installation.

İlgili görevler

“Güvenlik ilkeleri yaratılması” sayfa 303
Güvenlik ilkeleri, ileti konduğunda bir iletinin nasıl korunacağı ya da bir ileti alındığında nasıl korunmuş olması gerektiğini tanımlar.

“Güvenlik ilkelerinin değiştirilmesi” sayfa 304
Önceden tanımladığınız güvenlik ilkelerinin ayrıntılarını değiştirmek için Gelişmiş İleti Güvenliği ' u kullanabilirsiniz.

“Güvenlik ilkelerini görüntüleme ve boşaltma” sayfa 304
Sağladığınız komut satırı parametrelere bağlı olarak tüm güvenlik ilkelerinin bir listesini ya da adlandırılmış bir ilkeye ilişkin ayrıntıları görüntülemek için `dspmqspl` komutunu kullanın.

“Güvenlik ilkeleri kaldırılıyor” sayfa 306
Gelişmiş İleti Güvenliğiiçindeki güvenlik ilkelerini kaldırmak için `setmqspl` komutunu kullanmanız gerekir.

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.
- Bir güvenlik ilkesinin adı, WebSphere MQ nesnelerinin adlandırılması için kurallaröğesini izlemelidir.
- Bir güvenlik ilkesi oluşturmak için gerekli `+connect +inq +chg` yetkilerine sahip olmanız gerekir. Yetkilendirme değişiklik komutunun tam sözdizimi için bkz. **setmqaut** .
- WebSphere MQ kuyruklarını ve kuyruk yöneticilerini çalıştırmak için gereken izinlere sahip olup olmadığınızı denetleyin. Daha fazla bilgi için, bkz. “OAM izinlerinin verilmesi” sayfa 307

Örnek

Here is an example of creating a policy on queue manager `QMGR`. Bu ilke, iletilerin `SHA1` 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 SHA1 -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 DES algoritması kullanılarak şifreleneceğini belirtir: CN=john, O=IBM, C=US ve CN=jeff, O=IBM, C=US ve DN ile sertifika için MD5 algoritmasıyla imzalanmış: CN=phil, O=IBM, C=TR

```
$ setmqspl -m QMGR -p MY.OTHER.QUEUE -s MD5 -e DES -r CN=john,O=IBM,C=US -r CN=jeff,O=IBM,C=US
-a CN=phil,O=IBM,C=US
```

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

Güvenlik ilkelerinin değiştirilmesi

Önceden tanımladığınız güvenlik ilkelerinin ayrıntılarını değiştirmek için Gelişmiş İleti Güvenliği ' u kullanabilirsiniz.

Başlamadan önce

- Üzerinde işlem yapmak istediğiniz kuyruk yöneticisi çalışıyor olmalıdır.
- Güvenlik ilkeleri oluşturmak için gerekli `+connect +inq +chg` yetkililerine sahip olmanız gerekir. Yetkilendirme değişiklik komutunun tam sözdizimi için bkz. **setmqaut** .

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 will be encrypted using the RC2 algorithm for certificates with DN:CN=bob,O=IBM,C=US and signed with the SHA1 algorithm for certificates with DN:CN=jeff,O=IBM,C=US.

```
setmqspl -m QMGR -p MYQUEUE -e RC2 -s SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

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 SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

İlgili başvurular

setmqspl

Güvenlik ilkelerini görüntüleme ve boşaltma

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.
- Güvenlik ilkelerini görüntülemek ve döküm almak için kuyruk yöneticisine gerekli `+connect +inq +dsp` izinlerine sahip olmanız gerekir. Yetkilendirme değişiklik komutunun tam sözdizimi için bkz. **setmqaut** .

Bu görev hakkında

Aşağıda dspmqspl komut işaretlerinin listesi yer alıyor:

Çizelge 27. 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

Bu örnekte, venus.queue.manageriçin iki güvenlik ilkesi oluşturacağız:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s MD5 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s MD5 -a "CN=another signer,O=IBM,C=US" -e
NONE
```

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: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=signer1,O=IBM,C=US
Recipient DNs: -
Toleration: 0
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

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: MD5
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 MD5 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Bir güvenlik ilkesini içe aktarmak için:

- Windows altyapılarında `policies.bat`komutunu çalıştırın.
- UNIX altyapılarında:
  1. `mqm` WebSphere MQ yönetim grubuna ait bir kullanıcı olarak oturum açın.
  2. Issue `. policies.sh`.

İlgili başvurular
dspmqspl komut özniteliklerinin tam listesi

Güvenlik ilkeleri kaldırılıyor
Gelişmiş İleti Güvenliğiiçindeki güvenlik ilkelerini kaldırmak için `setmqspl` komutunu kullanmanız gerekir.

Başlamadan önce
Güvenlik ilkelerini yönetirken yerine getirilmesi gereken bazı giriş koşulları vardır:

- Kuyruk yöneticisi çalışıyor olmalıdır.
- Güvenlik ilkeleri oluşturmak için gerekli `+connect +inq +chg` yetkililerine sahip olmanız gerekir. Yetkilendirme değişiklik komutunun tam sözdizimi için bkz. **setmqaut** .

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

Sistem kuyruğu koruması
Sistem kuyrukları, WebSphere MQ ile yan uygulamaları arasındaki iletişimi etkinleştirir. Bir kuyruk yöneticisi yaratıldığında, WebSphere MQ iç iletilerini ve verilerini saklamak için bir sistem kuyruğu da yaratılır. Sistem kuyruklarını, yalnızca yetkili kullanıcıların erişebileceği ya da şifresini çözebilmeleri için Gelişmiş İleti Güvenliği ile koruyabilirsiniz.

Sistem kuyruğu koruması, olağan kuyrukların korunmalarıyla aynı örüntüleri izler. Bkz. “Güvenlik ilkeleri yaratılması” sayfa 303.

To use system queue protection on Pencereler platforms, copy the `keystore.conf` file to the following directory:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

`SYSTEM.ADMIN.COMMAND.QUEUE`için koruma sağlamak üzere komut sunucusunun, anahtarlar ve sertifikalara erişebilmesi için anahtarları ve bir yapılandırmayı içeren `keystore` ve `keystore.conf`' ye erişmesi gerekir. `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, İmzalayıcı Ayırt Edici Adı (DN) denetimi geçirmeyen komut iletileri komut sunucusu tarafından yürütülmez ve Gelişmiş İleti Güvenliği hata işleme kuyruğuna yönlendirilmez. WebSphere MQ Gezgini geçici dinamik kuyruklarına yanıt olarak gönderilen iletiler, WebSphere MQ AMS tarafından korunmaz.

Gelişmiş İleti Güvenliği güvenlik ilkelerinde yapılan değişiklikler, WebSphere MQ komut sunucusunu yeniden başlatmanızı gerektirir.

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
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE
- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

OAM izinlerinin verilmesi

Dosya izinleri, tüm kullanıcıların `setmqspl` ve `dspmqspl` komutlarını yürütmesine izin verir. Ancak, IBM Gelişmiş İleti Güvenliği , Object Authority Manager (OAM) olanağına dayanır ve bu komutları WebSphere 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 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
```

Komut ve yapılandırma olayları

Gelişmiş İleti Güvenliğiile, denetim için ilke değişikliklerinin kaydı olarak günlüğe kaydedilebilir ve hizmet verebilen komut ve yapılandırma olayı iletileri oluşturabilirsiniz.

WebSphere MQ tarafından oluşturulan komut ve yapılandırma olayları, adanmış kuyruklara gönderilen PCF biçiminin iletidir.

Yapılandırma olayları iletileri SYSTEM.ADMIN.CONFIG.EVENT kuyruğun oluştuğu kuyruk yöneticisininde kuyruk.

Komut olayları iletileri SYSTEM.ADMIN.COMMAND.EVENT kuyruğun oluştuğu kuyruk yöneticisininde kuyruk.

Olaylar, Gelişmiş İleti Güvenliği güvenlik ilkelerini yönetmek için kullandığınız araçlardan bağımsız olarak oluşturulur.

Gelişmiş İleti Güvenliği' ta, güvenlik ilkelerinde farklı işlemler tarafından oluşturulan dört tip olay vardır:

- “Güvenlik ilkeleri yaratılması” sayfa 303, which generate two WebSphere MQ event messages:
  - Bir yapılandırma olayı
  - Bir komut olayı
- “Güvenlik ilkelerinin değiştirilmesi” sayfa 304, which generates three WebSphere MQ event messages:
  - Eski güvenlik ilkesi değerlerini içeren bir yapılandırma olayı
  - Yeni güvenlik ilkesi değerleri içeren bir yapılandırma olayı
  - Bir komut olayı
- “Güvenlik ilkelerini görüntüleme ve boşaltma” sayfa 304, bir WebSphere MQ olay iletisi oluşturur:
  - Bir komut olayı
- “Güvenlik ilkeleri kaldırılıyor” sayfa 306, which generates two WebSphere MQ event messages:
  - Bir yapılandırma olayı
  - Bir komut olayı

Olay günlüğe kaydetmeyi etkinleştirme ve devre dışı bırakma

Komut ve yapılandırma olaylarını, CONFIG.V ve CMDEV kuyruk yöneticisi özniteliklerini kullanarak denetliyorsunuz. 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

Yapılanış olaylarını etkinleştirmek için, CONFIG.EV öğesini ENABETLEolarak ayarlayın. Yapılandırma olaylarını devre dışı bırakmak için, CONFIG.V öğesini DISABLE(Geçersiz) olarak ayarlayın. Örneğin, aşağıdaki MQSC komutunu kullanarak yapılanış olaylarını etkinleştirebilirsiniz:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Komut olayları

Komut olaylarını etkinleştirmek için CMDEV ' yi ENABETLEolarak ayarlayın. DISPLAY MQSC komutları ve Sorgula PCF komutları dışındaki komutlara ilişkin komut olaylarını etkinleştirmek için CMDEV ' yi NODISPLAY olarak ayarlayın. Komut olaylarını devre dışı bırakmak için CMDEV ' yi DISABLE(Geçersiz) olarak ayarlayın. Örneğin, aşağıdaki MQSC komutunu kullanarak komut olaylarını etkinleştirebilirsiniz:

```
ALTER QMGR CMDEV (ENABLED)
```

İlgili görevler

Websphere MQ' da yapılandırma, komut ve günlüğe kaydedici olayları denetleme

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 paramteter olduğu için. Her grup, uygun parametrelerden oluşur. Olay verileri iki gruptan (CommandContext ve CommandData) oluşur.

CommandContext şunları içerir

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.

EventOrigin

Açıklama:	Olaya neden olan eylemin kökeni.
Tanıtıcı:	MQIACF_EVENT_ORIGIN.
Veri tipi:	MQCFIN.
Değerler:	**MQEVO_CONSOLE** Konsol komutu-komut satırı. **MQEVO_MSG** WebSphere 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.

EventAccountingToken

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.

EventIdentityData

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.

EventApplType

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.

EventApplName

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.

EventApplOrigin

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.

Command

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 WebSphere MQ 7.5 `cmqcfc.` hiçinde tanımlanır.

Döndürülen: Her zaman.

CommandData , PCF komutuna sahip PCF öğelerini içerir.

Yapılandırma olayı ileti biçimi

Yapılandırma olayları, standart Gelişmiş İleti Güvenliği biçimindeki PCF iletileridir.

MQMD ileti tanımlayıcısına ilişkin olası değerler için bakınız: Event message MQMD (message descriptor).

Seçilen MQMD değerleri şunlardır:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR                      //for both CLI and command server
```

İleti arabelleği MQCFH yapısından ve bunu izleyen değiştirge yapısından oluşur. Olası MQCFH değerleri için bakınız: Event message MQCFH (PCF üstbilgisi).

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, komutu ya da çağrıyı verme yetkisini denetlemek için kullanılan kullanıcı kimliğiyle aynıdır; bir kuyruktan alınan komutlar için, bu aynı zamanda komut iletisinin MD ' sinden alınan kullanıcı kimliğidir (UserIdentifier)).

Tanıtıcı: **MQCACF_EVENT_USER_ID**

Veri tipi: MQCFST

Uzunluk üst sınırı: MQ_USER_ID_LENGTH.

Döndürülen: Her zaman.

SecurityId

Açıklama: MQMD.AccountingToken ya da yerel komut için Windows SID 'si.

Tanıtıcı: **MQBACF_EVENT_SECURITY_ID**

Veri tipi: MQCBS.

Uzunluk üst sınırı: MQ_SECURITY_ID_LENGTH.

Döndürülen: Her zaman.

EventOrigin

Açıklama: Olaya neden olan işlemin kaynağı.

Tanıtıcı: **MQIACF_EVENT_ORIGIN**

Veri tipi: MQCFIN.

Değerler:

MQEVO_CONSOLE
Konsol komut satırı.

MQEVO_MSG
WebSphere MQ Explorer eklentisinden komut iletisi.

Döndürülen: Her zaman.

EventQMgr

Açıklama: Komutun ya da çağrım girildiği kuyruk yöneticisi. (Komutun yürütüldüğü ve olayı oluşturan kuyruk yöneticisi olay iletisinin MD ' sinde bulunur).

Tanıtıcı: **MQCACF_EVENT_Q_MGR**

Veri tipi: MQCFST

Uzunluk üst sınırı: MQ_Q_MGR_AD_UZUNLUK

Döndürülen: Her zaman.

ObjectType

Açıklama: Nesne tipi.

Tanıtıcı: **MQIACF_OBJECT_TYPE**

Veri tipi: MQCFIN

Değer:

MQOT_PROT_POLICY
Gelişmiş İleti Güvenliği koruma ilkesi. **1019** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal değer.

Döndürülen: Her zaman.

PolicyName

Açıklama: Gelişmiş İleti Güvenliği ilkesi adı.

Tanıtıcı: **MQCA_POLICY_NAME**.

Veri tipi: MQCFST

Değer: **2112** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal değer.

Uzunluk üst sınırı: MQ_OBJECT_NAME_LENGTH.

Döndürülen: Her zaman.

PolicyVersion

Açıklama: Gelişmiş İleti Güvenliği ilke sürümü.

Tanıtıcı: **MQIA_POLICY_VERSION**

Veri tipi: MQCFIN

Değer **238** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan bir sayısal değer.

Döndürülen: Her zaman

TolerateFlag

Açıklama: Gelişmiş İleti Güvenliği ilke toleransı işareti.

Tanıtıcı: **MQIA_TOLERATE_UNPROTECTED**

Veri tipi: MQCFIN

Değer **235** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal bir değerdir.

Döndürülen: Her zaman.

SignatureAlgorithm

Açıklama: Gelişmiş İleti Güvenliği ilke imza algoritması.

Tanıtıcı: **MQIA_SIGNATURE_ALGORITHM**

Veri tipi: MQCFIN

Değer: **236** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal bir değer.

Döndürülen: Gelişmiş İleti Güvenliği ilkesinde tanımlı bir imza algoritması olduğunda

EncryptionAlgorithm

Açıklama: Gelişmiş İleti Güvenliği ilke şifreleme algoritması.

Tanıtıcı: **MQIA_ENCRYPTION_ALGORITHM**

Veri tipi: MQCFIN

Değer: **237** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal bir değer.

Döndürülen: WebSphere MQ ilkesinde tanımlı bir şifreleme algoritması olduğunda

SignerDNs

Açıklama: İzin verilen imzalayıcıların konu DistinguishedName .

Tanıtıcı: **MQCA_SIGNER_DN**

Veri tipi: MQCFSL

Değer: **2113** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal değer.

Uzunluk üst sınırı: İlkedeki en uzun imzalayıcı DN 'si, ancak bundan sonra MQ_AYIRT edici ad_uzunluk

Döndürülen: WebSphere MQ ilkesinde tanımlandığında.

RecipientDNs

Açıklama: İzin verilen imzalayıcıların konu DistinguishedName .

Tanıtıcı: **MQCA_RECIPIENT_DN**

Veri tipi: MQCFSL

Değer:	**2114** - WebSphere MQ 7.5 ya da `cmqc.h` dosyasında tanımlanan sayısal bir değer.
Uzunluk üst sınırı:	İlkedeki en uzun alıcı ayırt edici adı (DN), ancak artık MQ_AYIRT edici ad_uzun değil.
Döndürülen:	WebSphere MQ ilkesinde tanımlandığında.

Sorunlar ve çözümler

Bu bölümde, IBM kuruluşuyla ortaya çıkabilecek sorunların nasıl çözülebileceği anlatılır. Bu bilgiler, Gelişmiş İleti Güvenliğiile ilgili sorunları belirlemek ve çözmek için bu bilgileri kullanın.

com.ibm.security.pkcsutil.PKCSException: İçindekiler şifrelenirken hata oluştu

`com.ibm.security.pkcsutil.PKCSException: Error encrypting contents` hatası, IBM Gelişmiş İleti Güvenliği ' in şifreleme algoritmalarına erişimle ilgili sorunları olduğunu göstermektedir.

Aşağıdaki hata Gelişmiş İleti Güvenliğitarafından döndürülürse:

```
DRQJP0103E   The IBM WebSphere MQ Advanced Message Security Java interceptor failed to protect
message.
  com.ibm.security.pkcsutil.PKCSException: Error encrypting contents
(java.security.InvalidKeyException: Illegal key size or default parameters)
```

`JAVA_HOME/lib/security/local_policy.jar/*.policy` içindeki JCE güvenlik ilkesinin, MQ AMS ilkesinde kullanılan imza algoritmalarına erişip erişmediğini doğrulayın.

Kullanmak istediğiniz imza algoritması yürürlükteki güvenlik ilkesinde belirlenmediyse, doğru Java ilke dosyasını aşağıdaki konumlardan yükleyin:

- IBM SDK Policy files for Java 1.4.2.
- IBM SDK Policy files for Java 5.0.
- IBM SDK Policy files for Java 6.0.
- IBM SDK Policy files for Java 7.0.

OSGi desteği

To use OSGi bundle with IBM Gelişmiş İleti Güvenliği additional parameters are required.

OSGi kod paketi başlatma sırasında şu değiştirgeyi çalıştırın:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7
```

keystore.conf' da şifrelenmiş parolayı kullanırken, OSGi kod paketi çalışırken aşağıdaki deyimin eklenmesi gerekir:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7,com.ibm.misc
```

Sınırlama: IBM WebSphere MQ AMS , yalnızca OSGi kod paketi içinden korunan kuyruklar için yalnızca MQ Base Java Sınıfları 'nı kullanarak iletişimi destekler.

JMSkullanılırken korunan kuyruklar açılırken birden çok sorun oluştu

IBM WebSphere MQ Advanced Message Securitykullanırken korumalı kuyruklar açtığınızda çeşitli sorunlar ortaya çıkabilir.

You are running JMS and you receive error 2085 (MQRC_UNKNOWN_OBJECT_NAME) together with error JMSMQ2008.

You have verified that you have set up your IBM WebSphere MQ Advanced Message Security as described in “Java istemcileri için Hızlı Başlama Kılavuzu” sayfa 277.

Olası bir neden,IBM Java Runtime Environment olmayan bir Ortam kullanmanıza neden olur. Bu, “Bilinen sınırlamalar” sayfa 265' ta açıklanan bilinen bir sınırlamadır.

AMQ_DISABLE_CLIENT_AMS ortam değişkenini ayarlamadınız.

Sorunun çözümleniyor

Bu sorunun üzerinde çalışılmasına ilişkin dört seçenek vardır:

1. JMS uygulamanızı desteklenen bir IBM Java Runtime Environment (JRE) altında başlatın.
2. Uygulamanızı, kuyruk yöneticinizin çalıştığı aynı makineye taşıyın ve bir bağ tanımlama kipi bağlantısı kullanarak bağını kurun.

   Bağ tanımları kipi bağlantısı, IBM WebSphere MQ API çağrılarını gerçekleştirmek için altyapı yerel kitaplıklarını kullanır. Buna göre, AMS işlemlerini gerçekleştirmek için yerel AMS dinlemesi kullanılır ve JRE ' nin yetenekleriyle ilgili bir bağımlılığın yoktur.
3. MCA dinleyici kullanın; bu işlem, iletilerin kuyruk yöneticisine vardığı anda iletilerin imzalanmasını ve şifrelenmesini sağlar. Bu işlem, müşterinin herhangi bir AMS işlemesini gerçekleştirmesine gerek kalmadan, ileti yöneticisine ulaşmalarını sağlar.

   Koruma kuyruk yöneticisinde uygulandığında, istemciden kuyruk yöneticisine aktarılan iletileri korumak için alternatif bir mekanizma kullanılmalıdır. Bunun en yaygın olarak, uygulama tarafından kullanılan sunucu bağlantısı kanalında SSL/TLS şifrelemesi yapılandırılarak elde edilir.
4. IBM WebSphere MQ Advanced Message Securitykullanmak istemezseniz, AMQ_DISABLE_CLIENT_AMS ortam değişkenini ayarlayın.

Ek bilgi için “Message Channel Agent (MCA) etkileşimi” sayfa 288 ' e bakın.

Not: MCA Interceptor olanağının ileti göndereceği her kuyruk için bir güvenlik ilkesi bulunmalıdır. Diğer bir deyişle, hedef kuyruğun, imzalayan ve alıcının MCA Interceptor 'a atanan sertifikayla eşleşen ayırt edici adı (DN) ile birlikte bir AMS güvenlik ilkesi olması gerekir. Yani, kuyruk yöneticisi tarafından kullanılan `keystore.conf` içindeki `cms.certificate.channel.SYSTEM.DEF.SVRCONN` özelliği tarafından belirlenen sertifikana ilişkin ayırt edici ad.

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 IBM 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: