CHAPTER 8

管理通信のセキュア鍵の設定

この章では、Cisco ACE XML ゲートウェイ および Manager 間の管理通信のセキュリティに使用するデフォルトのキーの変更方法について説明します。内容は次のとおりです。

概要

Manager が管理対象の Gateway を使用して SSL 接続を確立することによりポリシーを実施する場合またはその他の管理機能を実行する場合には、X.509 クライアント証明書を提示し、Gateway がこれに自身のサーバ証明書を提示して応答することを求めます。Manager もまた証明書を使用して Manager 監査ログに署名し、記録された情報の完全性を保証します。

セキュリティを強化するには、これらの目的にデフォルトの証明書ではなく、独自の証明書を使用する必要があります。各 X.509 証明書の固有のアイデンティティは、一連の PKI 鍵に基づいて決まります。初期設定時に新しい証明書をインストールする以外に、定期的に、またはセキュリティ侵犯の発生に備えて、新しい鍵をインストールすることもできます。

証明書では、ソフトウェアベースまたはハードウェアベースの暗号鍵を使用できます。デフォルトではソフトウェアベースの鍵が使用されています。セキュリティを強化するため、ハードウェアベースのキーストアを使用して鍵の作成および保護を実行することを推奨します。

ハードウェアベースの鍵を使用するには、第 7 章「ハードウェア キーストアおよびセキュリティ ワールドの使用」で説明されているように、アプライアンスに nCipher ハードウェアベース キーストアを装備し、それらを使用するようにアプライアンスを設定する必要があります。

ハードウェアベースの証明書のインストール

ハードウェアベースの鍵を使用して双方向認証を行うようにアプライアンスを設定するプロセスは、2 つの手順からなります。

- クラスタの各 ACE XML Gateway に新しいサーバ証明書をインストールし、ACE XML Gateway が双方向認証にこの証明書を提示することを Manager に通知する必要があります。

- Manager に新しいクライアント証明書をインストールし、Manager が双方向認証用にこの証明書を提示することを各 ACE XML Gateway に通知する必要があります。

インストール手順は考え方としては似ていますが、細部は多少異なります。正しくインストールするために、必ず各セクションの手順を 1 つずつ慎重に実行してください。

（注） 個々のハードウェアベースの証明書をインストールするには、Manager アプライアンス上で特定のコマンドを実行し、Gateway アプライアンス上で他のコマンドを実行する必要があります。Gateway クラスタに双方向認証の証明書をインストールする場合には、クラスタの各 Gateway アプライアンス上で Gateway ベースのコマンドを実行する必要があります。

実行する前に、次の前提条件を満たしていることを確認してください。

- 管理証明書に署名するために 1 つまたは複数の trusted CA（認証局）が使用できなければなりません。同じ CA の使用には Manager および Gateway は必要でないことに注意してください。
- 各アプライアンスを Gateway、Manager、または独立型マシンとして設定しておく必要があります。
- 第 7 章「ハードウェア キーストアおよびセキュリティ ワールドの使用」の手順にしたがって、nCipher セキュリティ ワールドを使用するように各アプライアンスを設定しておく必要があります。
- ハードウェアベースの SSL エンジンを使用可能にしておく必要があります。詳細については、「SSL アクセラレーションの有効化」（P.9-1）を参照してください。

手順は 2 つの作業にわかれています。

- 「Gateway から Manager への認証」（P.8-2）
- 「Manager から Gateway への認証」（P.8-5）

Gateway から Manager への認証

双方向認証にハードウェアベースの鍵を使用するように ACE XML Gateway マシンを設定するには、次の作業が必要です。

- 双方向認証で Gateway が提示する証明書に署名した CA を Manager に通知します。
- ACE XML Gateway 上で Certificate Signing Request（CSR; 証明書署名要求）を作成します。
- Gateway の trusted CA に CSR を送信し、Gateway のサーバ証明書に変換します。
- Gateway にサーバ証明書をインストールします。

各手順の詳細は、次のとおりです。

注意 作業を続ける前に、メッセージ トラフィックが設定対象の Gateway を迂回するようにしてください。これを実行するには、ネットワーク上で Gateway をその手前にあるロードバランサでオフラインにします。Gateway をオフラインにしなかった場合は、手順の実行中に進行中のトランザクションが中断される可能性があります。また、アプライアンス シェルからすべての Gateway サービスを非アクティブに設定して停止させます（つまり、[Network Configuration] > [Cluster Configuration] の順にメニュー項目を選択します）。

ハードウェアベースの証明書を ACE XML Gateway にインストールするには、次の手順に従います。

ステップ 1　Manager アプライアンス上で、`root` ユーザとして `bash` を実行します。

ステップ 2　Gateway の trusted CA の自己署名ルート証明書のコピーを Manager アプライアンスの /usr/local/reactivity/private ディレクトリに保存します。

ファイルは任意の方法でコピーできます。たとえば、Gateway の bash シェルから Manager マシンに ssh を実行し、さらに scp コマンドを使用して CA 証明書をコピーできます。ここでは、この証明書を Gateway CA 証明書と呼びます。

（注）　この Manager が制御するすべての Gateway が同じ Gateway CA 証明書を提示する必要があります。異なるシステム設定が必要な場合は、シスコのサポート担当者に問い合わせてください。Manager および Gateway が同じ CA を使用する必要はないことに注意してください。ただし、双方向証明書交換の両者が同じ CA を使用しない場合は、必ず各マシンに正しい CA 証明書をインストールしてください。

ステップ 3　Manager シェルでは、次のようにディレクトリを private ディレクトリに変更します。

```
cd /usr/local/reactivity/private/
```

ステップ 4　次のコマンドを実行して、trusted CA に関する Manager の現在のデータベースをバックアップします。

```
mv trustkeystore private/trustkeystore.bak
```

このコマンドによって、trustkeystore ファイルの名前が trustkeystore.bak ファイルに変更されます。trustkeystore ファイルは、Manager が信頼する CA のリストです。次のステップで、新しい trustkeystore ファイルを作成します。

（注）　次の例およびこの章の残りの部分では、1 行に収まらないコマンドは折り返して次の行に表示しています。バックスラッシュ（「\」）は、このようにして折り返された行を意味します。bash シェルにこれらの例（または独自のコマンド）を入力するときには、バックスラッシュを省いてください。

ステップ 5　Manager シェルで次のコマンドを実行し、新しくインストールした Gateway CA 証明書に対応するエントリを含む、新しい trusted CA データベースを作成します。

```
/usr/java/j2sdk1.4.2_04/bin/keytool \
    -import -trustcacerts -alias ca_cert \
    -keystore trustkeystore \
     -storetype jks -file GCACERT.CRT \
    -storepass approuter
```

この場合、*GCACERT.CRT* は、インストールした Gateway CA 証明書のローカル コピーのファイル名です。

ステップ 6　[Trust this certificate?] プロンプトに yes を入力します。

キーストアに新しい証明書が追加され、[Certificate was added to keystore] メッセージが表示されます。

ステップ 7　Gateway マシン上で、root ユーザとして bash を実行します。

コマンド プロンプトが表示されます。これ以降の手順では、この端末セッションを Gateway シェルと呼びます。

ステップ 8　シェルで、private ディレクトリに移動します。

```
cd /usr/local/reactivity/private/
```

ステップ 9　次のコマンドを実行し、Gateway の現在の管理サーバ証明書をバックアップします。

```
mv server.pem server.pem.bak
```

（注）　Gateway クラスタに証明書をインストールするには、クラスタの各 Gateway マシン上でこのような Gateway ベース コマンドを実行する必要があります。

ステップ 10　次の手順にしたがって Gateway シェルで、nCipher で保護される新規の秘密鍵および対応する Certificate Signing Request（CSR; 証明書署名要求）を Gateway に作成するための `generatekey` コマンドを実行して、鍵および対応する CSR を作成します。

```
/opt/nfast/bin/generatekey --batch embed \
protect=module recovery=1 size=1024 \
embedsavefile=server.pem \
x509dnscommon="gatewayhost" \
x509org="OrganizationName" x509locality="Belmont" \
x509province="California" x509country="US"
```

コマンドの中で、イタリック体のテキストは各自の状況に適した値に置き換えます。`x509dnscommon` パラメータの値には、Gateway と通信するために Manager が使用する完全修飾ホスト名を推奨しますが、絶対条件ではありません。

システムによって CSR が `private/server_req.pem` に書き込まれ、鍵生成処理に関する情報が表示されます。処理が正常に完了すると、出力の末尾に [Key successfully generated] が表示されます。

ステップ 11　Gateway の trusted CA に CSR データ（`server_req.pem` ファイル）を送信し、署名入りの X.509 証明書に変換します。

CA は応答として、署名入り証明書を送信します。この証明書は Gateway のサーバ証明書、つまり Gateway が Manager に提示する証明書です。

ステップ 12　CA から電子メールの本文として署名入り証明書を受け取った場合は、証明書の内容だけをテキストファイルに保存します。

- `BEGIN CERTIFICATE` の行全体から `END CERTIFICATE` の行全体までをすべて含めます。
- ローカル ファイル システムで、有効な Linux ファイル名を使用してファイルを保存します。このファイル名にはスペース、アポストロフィ、アンパサンド、およびその他の特殊文字を使用しないでください。

ステップ 13　Gateway シェルで、次のコマンドを `private` ディレクトリで実行して署名入り証明書を Gateway にインストールします。

```
$ cat GCERT.CRT >> server.pem
```

実際のコマンドでは、*GCERT.CRT* を署名入り証明書のファイル名に置き換えます。

（注）　必ず出力リダイレクト演算子 >> を使用して、署名入り証明書を `server.pem` ファイルに追加します（このファイルを置き換えないでください）。このファイルが置き換えられると、`generatekey` ツールでこのファイルに格納した秘密鍵が失われてしまうため、キーストアが証明書の有効性を認識できなくなります。このエラーを修復するには、ここでの全手順を繰り返し、新しい鍵、新しい CSR、および新しい証明書を作成してインストールする必要があります。

これらの手順が正しく完了すると、Gateway はハードウェアベースの鍵を双方向証明書交換に使用するように設定されます。つまり、Gateway のハードウェアベースの管理証明書がインストールされ、Gateway に Manager が提示する証明書を検証する際に使用する CA が通知されます。

これ以降、クラスタ内の他の Gateway を同様に設定できます。

Manager から Gateway への認証

双方向認証にハードウェアベースの鍵を使用するように Manager を設定するには、次の作業が必要です。

- 双方向認証で Manager が提示する証明書に署名した CA を ACE XML Gateway に通知します。この作業は、クラスタ内の各 ACE XML Gateway で実行する必要があります。
- Manager 上でハードウェアベースの鍵を使用する CSR 作成します。
- Manager の trusted CA に CSR を送信し、Manager のクライアント証明書に変換します。
- Manager にクライアント証明書をインストールします。

次の手順でハードウェアベースの管理クライアント証明書を Manager にインストールします。

ステップ 1　この Manager が制御する各 Gateway マシンの次のディレクトリに、Manager の trusted CA の自己署名ルート証明書のコピーを保存します。

```
/usr/local/reactivity/private/
```

scp または任意のセキュア ファイル転送メカニズムを使用して、ファイルをコピーします。scp ユーティリティを使用する場合は、次のように、Manager の `bash` シェルから実行し、Manager の CA 証明書を Gateway アプライアンスにコピーします。

```
ssh gatewaymachine -l root
cd /usr/local/reactivity/private/
scp root@manangername:/pathToMCACert/MCAERT.CRT .
```

この例では、*MCACERT.CRT* ファイルは、Manager が Gateway に提示する証明書に署名した CA の自己署名ルート証明書です。これ以後の手順では、この証明書を Manager CA 証明書と呼びます。上記の例では、このファイルは *pathToMCACert* ディレクトリの *managername* コンピュータ上にあります。このファイルは、`scp` コマンドによって、`gatewaymachine` Gateway アプライアンスの */usr/local/reactivity/private* ディレクトリにコピーされます。

MCACERT.CRT ファイルは、双方向証明書交換で Manager が提示する証明書に署名した CA の、PEM フォーマットの自己署名ルート証明書でなければなりません。Gateway と Manager は、それぞれに提示された証明書の検証に、両方で同じ CA を使用する必要はありません。しかし、双方向証明書交換の両者が同じ CA を使用しない場合は、各マシンに正しい CA 証明書をインストールするよう注意する必要があります。

ステップ 2　Gateway マシン上で、`root` ユーザとして `bash` を実行します。

ステップ 3　Gateway シェルで次のコマンドを実行し、作業ディレクトリを最上位ディレクトリに設定します。

```
cd /usr/local/reactivity/private/
```

ステップ 4　Gateway シェルで次のコマンドを実行し、Gateway に現在インストールされている Manager CA 証明書をバックアップします。

```
mv ca.crt ca.crt.bak
```

このコマンドラインによって、`ca.crt` ファイルの名前が `ca.crt.bak` ファイルに変更されます。このあと、新しい `ca.crt` ファイルをインストールします。

ステップ 5　Gateway シェルで次のコマンドを実行し、新しい Manager CA 証明書を Gateway にインストールします。

```
cp MCACERT.CRT ca.crt
```

MCACERT.CRT を、インストールした CA 証明書のローカル コピーのファイル名に置き換えます。

ステップ 6　Manager アプライアンス上で、`root` ユーザとして `bash` を実行します。

ステップ 7　Manager シェルで、次のように private ディレクトリに変更します。

```
cd /usr/local/reactivity/private/
```

ステップ 8　シェルで次のコマンドを実行し、Manager の現在のハードウェア鍵データベースをバックアップします。

```
mv client.ncipher client.ncipher.bak
```

このコマンドによって、client.ncipher ファイルの名前が client.ncipher.bak に変更されます。このファイルには、Manager が管理する Gateway に接続するために Manager が使用するハードウェアベースの秘密鍵が保存されます。次のステップで、新しい client.ncipher ファイルを作成します。

ステップ 9　Manager シェルで reactivity ディレクトリから次のコマンドを実行し、Manager の Web ベース インターフェイスが提示する証明書で使用する、nCipher によって保護される新しい秘密鍵を作成します。

```
bin/ncipherkeytool -genkey -keystore private/client.ncipher -alias mykey -keyalg RSA
-keysize 1024 -dname "CN=managerhostname, O=CompanyName,L=Belmont,ST=California,C=US"
```

[CN]、[O]、[L]、および [ST] フィールドの*イタリック体*の値を各自の状況に適した値に置き換えます。特に CN= 値は、証明書をインストールする Manager マシンの完全修飾ホスト名にする必要があります。

ステップ 10　Manager シェルで次のコマンドを入力し、nCipher によって保護される新しい秘密鍵に基づいた CSR を作成します。

```
bin/ncipherkeytool -certreq -keystore private/client.ncipher -alias mykey -file
client.req
```

システムによって CSR が client.req ファイルに書き込まれます。必要に応じて、このファイルに有効な CSR が含まれていることを確認できます。

ステップ 11　Manager の trusted CA に CSR データ（client.req ファイル）を送信し、署名入りの X.509 証明書に変換します。

この証明書は Manager のクライアント証明書、つまり Manager が Gateway に提示する証明書であることに注意してください。

ステップ 12　CA から電子メールの本文として署名入り証明書を受け取った場合は、証明書の内容だけをテキストファイルにペーストします。

- BEGIN CERTIFICATE の行全体から END CERTIFICATE の行全体までをすべて含めます。
- ローカル ファイル システムで、有効な Linux ファイル名を使用してファイルを保存します。このファイル名にはスペース、アポストロフィ、アンパサンド、およびその他の特殊文字を使用しないでください。

ステップ 13　Manager シェルで次のコマンドを実行し、nCipher で保護される Manager のキーストアに Manager の trusted CA 証明書をインストールします。

```
bin/ncipherkeytool -import -trustcacerts \
   -keystore private/client.ncipher -alias ca_cert -file MCACERT.CRT
```

このコマンドを入力するときは、*MCACERT.CRT* パラメータを、インストールした Manager CA 証明書のローカル コピーのファイル名に置き換えます。

シェルから、処理の確認が求められます。次のような出力が表示されます。

```
Owner: EMAILADDRESS=name@example.com,
  CN=Some CA, OU=Engineering, O="Beagle, Inc.",
  L=Belmont, ST=California, C=US Issuer:
  EMAILADDRESS=name@example.com, CN=Some CA,
  OU=Engineering, O="Beagle, Inc.", L=Belmont,
  ST=California, C=US Serial number: 0
Valid from: Thu Dec 09 20:31:59 UTC 2004
     until: Wed Dec 09 20:31:59 UTC
  2009
Certificate fingerprints:
           MD5:  XX:   hellip  :XX
           SHA1: XX:   hellip  :XX
Trust this certificate? [no]:
```

Manager および Gateway は、提示された証明書の検証に、同じ CA を使用する必要はありません。しかし、双方向証明書交換の両者が同じ CA を使用しない場合は、各マシンに正しい CA 証明書をインストールするよう注意する必要があります。

ステップ 14　Manager シェルで `yes` を入力し、この証明書を信頼することを確認します。

シェルによってキーストアに新しい証明書が追加され、[Certificate was added to keystore] メッセージが表示されます。

ステップ 15　Manager シェルで次のコマンドを実行し、Manager の nCipher キーストアに新しい Manager クライアント証明書をインストールします。

```
bin/ncipherkeytool -import  \
     -keystore private/client.ncipher \
     -alias mykey -file MCERT.CRT
```

このコマンドを入力するときは、*MCERT.CRT* パラメータを、CSR への応答として Manager の trusted CA が返した署名入り X.509 証明書のローカル コピーのファイル名に置き換えます。

ncipherkeytool コマンドによって Manager のクライアント証明書が正常にインストールされると、[Certificate reply was installed in keystore] メッセージが表示されます。

ステップ 16　ブラウザを Web コンソールに接続するために使用する新しい証明書を Manager に提示させるには、次の手順に従います。

a. 次の Manager プロパティ ファイルを開いて編集します。
`/usr/local/reactivity/config/webapp.properties`

b. 次の行を変更します。

```
ssl.client.keystore=/usr/local/reactivity/private/client.p12
```

次のように変更します。

```
ssl.client.keystore=/usr/local/reactivity/private/client.ncipher
```

c. 次の行を

```
ssl.client.storetype=pkcs12
```

次のように変更します。

```
ssl.client.storetype=ncipher.sworld
```

ステップ 17　Manager シェルで次のコマンドを実行し、agateway を webapp.properties ファイルのオーナーおよびグループとして設定します。

```
chown agateway:agateway
   /usr/local/reactivity/config/webapp.properties
```

ステップ 18　次のコマンドを入力し、所有権が変更されたことを確認します。

```
ls -la /usr/local/reactivity/config
```

シェルによって、`config` ディレクトリの内容が表示されます。次の出力では、`webapp.properties` ファイルに割り当てられたオーナーおよびグループは agateway となっています。

```
-rw-r--r-- 1 agateway agateway 2874 Feb 8 00:34 webapp.properties
```

これらの手順の完了後、Manager はハードウェアベースの鍵を双方向証明書交換に使用します。さらに、この Manager が制御するすべての Gateway を設定すると、Manager と Gateway は双方向認証に新しくインストールされたハードウェアベースの証明書を使用できるようになります。

証明書の変更をテストするには、「管理証明書交換のテスト」（P.8-12）を参照してください。

ソフトウェアベースの証明書のインストール

ハードウェアベースの鍵の代わりに、双方向認証に新しくソフトウェアベースの鍵をインストールできます。このプロセスは 2 つにわかれます。

- クラスタの各 ACE XML Gateway に新しいサーバ証明書をインストールし、ACE XML Gateway が双方向認証にこの証明書を提示することを Manager に通知する必要があります。
- Manager に新しいクライアント証明書をインストールし、Manager が双方向認証用にこの証明書を提示することを各 ACE XML Gateway に通知する必要があります。

インストール手順は考え方としては似ていますが、細部は多少異なります。正しくインストールするために、必ず各セクションの手順を 1 つずつ慎重に実行してください。

実行する前に、次の前提条件を満たしていることを確認してください。

- 管理証明書に署名するために 1 つまたは複数の trusted CA（認証局）が使用できなければなりません。同じ CA の使用には Manager および Gateway は必要でないことに注意してください。
- 各アプライアンスを Gateway、Manager、または独立型マシンとして設定しておく必要があります。

手順は 2 つの作業にわかれています。

- 「Gateway から Manager への認証」（P.8-8）
- 「Manager から Gateway への認証」（P.8-10）

Gateway から Manager への認証

双方向認証にソフトウェアベースの鍵を使用するように ACE XML Gateway マシンを設定するには、次の作業が必要です。

- 双方向認証で Gateway が提示する証明書に署名した CA を Manager に通知します。
- ACE XML Gateway 上で Certificate Signing Request（CSR; 証明書署名要求）を作成します。
- Gateway の trusted CA に CSR を送信し、Gateway のサーバ証明書に変換します。
- Gateway にサーバ証明書をインストールします。

各手順の詳細は、次のとおりです。

注意　作業を続ける前に、メッセージ トラフィックが設定対象の Gateway を迂回するようにしてください。これを実行するには、ネットワーク上で Gateway をその手前にあるロードバランサでオフラインにします。Gateway をオフラインにしなかった場合は、手順の実行中に進行中のトランザクションが中断される可能性があります。また、アプライアンス シェルからすべての Gateway サービスを非アクティブに設定して停止させます（つまり、[Network Configuration] > [Cluster Configuration] の順にメニュー項目を選択します）。

ソフトウェアの証明書を ACE XML Gateway にインストールするには、次の手順に従います。

ステップ 1　Manager アプライアンス上で、`root` ユーザとして `bash` を実行します。

ステップ 2　Gateway の trusted CA の自己署名ルート証明書のコピーを Manager アプライアンスの `/usr/local/reactivity/private` ディレクトリに保存します。

ファイルは任意の方法でコピーできます。たとえば、Gateway の `bash` シェルから Manager マシンに `ssh` を実行し、さらに `scp` コマンドを使用して CA 証明書をコピーできます。ここでは、この証明書を Gateway CA 証明書と呼びます。

（注）　この Manager が制御するすべての Gateway が同じ Gateway CA 証明書を提示する必要があります。異なるシステム設定が必要な場合は、シスコのサポート担当者に問い合わせてください。Manager および Gateway が同じ CA を使用する必要はないことに注意してください。ただし、双方向証明書交換の両者が同じ CA を使用しない場合は、必ず各マシンに正しい CA 証明書をインストールしてください。

ステップ 3　Manager シェルで、ディレクトリを次のディレクトリに変更します。

```
cd /usr/local/reactivity/private/
```

ステップ 4　次のコマンドを実行して、trusted CA に関する Manager の現在のデータベースをバックアップします。

```
mv trustkeystore trustkeystore.bak
```

このコマンドによって、`trustkeystore` ファイルの名前が `trustkeystore.bak` ファイルに変更されます。`trustkeystore` ファイルは、Manager が信頼する CA のリストです。次のステップで、新しい `trustkeystore` ファイルを作成します。

（注）　次の例およびこの章の残りの部分では、1 行に収まらないコマンドは折り返して次の行に表示しています。バックスラッシュ（「\」）は、このようにして折り返された行を意味します。`bash` シェルにこれらの例（または独自のコマンド）を入力するときには、バックスラッシュを省いてください。

ステップ 5　Manager シェルで次のコマンドを実行し、新しくインストールした Gateway CA 証明書に対応するエントリを含む、新しい trusted CA データベースを作成します。

```
/usr/java/j2sdk1.4.2_04/bin/keytool \
    -import -trustcacerts -alias ca_cert \
    -keystore private/trustkeystore \
     -storetype jks -file GCACERT.CRT \
    -storepass approuter
```

この場合、*GCACERT.CRT* は、インストールした Gateway CA 証明書のローカル コピーのファイル名です。

ステップ 6　[Trust this certificate?] プロンプトに yes を入力します。

キーストアに新しい証明書が追加され、[Certificate was added to keystore] メッセージが表示されます。

ステップ 7　Gateway マシン上で、root ユーザとして bash を実行します。

コマンド プロンプトが表示されます。これ以降の手順では、この端末セッションを Gateway シェルと呼びます。

ステップ 8　Gateway シェルで、次のディレクトリに移動します。

```
cd /usr/local/reactivity/private/
```

ステップ 9　次のコマンドを実行し、Gateway の現在の管理サーバ証明書をバックアップします。

```
mv server.pem server.pem.bak
```

（注）　Gateway クラスタに証明書をインストールするには、クラスタの各 Gateway マシン上でこのような Gateway ベース コマンドを実行する必要があります。

ステップ 10　Gateway シェルで、次の 2 つのコマンドを入力して鍵および対応する CSR を作成します。

```
$ openssl genrsa -out server.pem 1024
$ openssl req -key server.pem \
-out server_req.pem -new -subj \
"/CN=gatewayhost/OU=myorgunit/O=MyCompany/L=Belmont/ST=California/C=US"
```

コマンドの中で、イタリック体のテキストは各自の状況に適した値に置き換えます。CN の値には、Gateway と通信するために Manager が使用する完全修飾ホスト名を推奨しますが、絶対条件ではありません。

ステップ 11　Gateway の trusted CA に CSR データ（`server_req.pem` ファイル）を送信し、署名入りの X.509 証明書に変換します。

CA は応答として、署名入り証明書を送信します。この証明書は Gateway のサーバ証明書、つまり Gateway が Manager に提示する証明書です。

ステップ 12　CA から電子メールの本文として署名入り証明書を受け取った場合は、証明書の内容だけをテキストファイルに保存します。

- `BEGIN CERTIFICATE` の行全体から `END CERTIFICATE` の行全体までをすべて含めます。
- ローカル ファイル システムで、有効な Linux ファイル名を使用してファイルを保存します。このファイル名にはスペース、アポストロフィ、アンパサンド、およびその他の特殊文字を使用しないでください。

ステップ 13　Gateway シェルから、次のコマンドを private ディレクトリで実行して署名入り証明書を Gateway にインストールします。

```
$ cat GCERT.CRT >> server.pem
```

実際のコマンドでは、*GCERT.CRT* を署名入り証明書のファイル名に置き換えます。

（注）　必ず出力リダイレクト演算子 >> を使用して、署名入り証明書を `server.pem` ファイルに追加します（このファイルを置き換えないでください）。このファイルが置き換えられると、`generatekey` ツールでこのファイルに格納した秘密鍵が失われてしまうため、キーストアが証明書の有効性を認識できなくなります。このエラーを修復するには、ここでの全手順を繰り返し、新しい鍵、新しい CSR、および新しい証明書を作成してインストールする必要があります。

これらの手順がすべて正しく完了すると、この Gateway 双方向認証に新しい鍵を使用するように設定されます。つまり、Gateway の管理証明書がインストールされ、Gateway に Manager が提示する証明書の検証に使用する CA が通知されます。

これ以降、クラスタ内の他の Gateway を同様に設定できます。

Manager から Gateway への認証

Manager が Gateway との通信のために双方向認証にソフトウェアベースの鍵を使用するように設定するには、次の作業を行います。

- 双方向認証で Manager が提示する証明書に署名した CA を ACE XML Gateway に通知します。この作業は、クラスタ内の各 ACE XML Gateway で実行する必要があります。
- Manager でこの鍵の CSR を作成します。
- CSR を CA に送信して、Manager のクライアント証明書に変換します。
- Manager にクライアント証明書をインストールします。

Manager にソフトウェアベースのクライアント証明書をインストールするには、次の手順に従います。

ステップ 1　この Manager が制御する各 Gateway マシンの次のディレクトリに、Manager の trusted CA の自己署名ルート証明書のコピーを保存します。

```
/usr/local/reactivity/private/
```

scp または任意のセキュア ファイル転送メカニズムを使用して、ファイルをコピーします。scp ユーティリティを使用する場合は、次のように、Manager の `bash` シェルから実行し、Manager の CA 証明書を Gateway アプライアンスにコピーします。

```
ssh gatewaymachine -l root
cd /usr/local/reactivity/private/
scp root@manangername:/pathToMCACert/MCAERT.CRT .
```

この例では、*`MCACERT.CRT`* ファイルは、Manager が Gateway に提示する証明書に署名した CA の自己署名ルート証明書です。これ以後の手順では、この証明書を Manager CA 証明書と呼びます。上記の例では、このファイルは *`pathToMCACert`* ディレクトリの *`managername`* コンピュータ上にあります。このファイルは、`scp` コマンドによって、`gatewaymachine` Gateway アプライアンスの */usr/local/reactivity/private* ディレクトリにコピーされます。

`MCACERT.CRT` ファイルは、双方向証明書交換で Manager が提示する証明書に署名した CA の、PEM フォーマットの自己署名ルート証明書でなければなりません。Gateway と Manager は、それぞれに提示された証明書の検証に、両方で同じ CA を使用する必要はありません。しかし、双方向証明書交換の両者が同じ CA を使用しない場合は、各マシンに正しい CA 証明書をインストールするよう注意する必要があります。

ステップ 2　Gateway マシン上で、`root` ユーザとして `bash` を実行します。

ステップ 3　Gateway シェルで次のコマンドを実行し、作業ディレクトリを最上位ディレクトリに設定します。

```
cd /usr/local/reactivity/
```

ステップ 4　Gateway シェルで次のコマンドを実行し、Gateway に現在インストールされている Manager CA 証明書をバックアップします。

```
mv ca.crt ca.crt.bak
```

このコマンドラインによって、`ca.crt` ファイルの名前が `ca.crt.bak` ファイルに変更されます。このあと、新しい `ca.crt` ファイルをインストールします。

ステップ 5　Gateway シェルで次のコマンドを実行し、新しい Manager CA 証明書を Gateway にインストールします。

```
cp MCACERT.CRT ca.crt
```

`MCACERT.CRT` を、インストールした CA 証明書のローカル コピーのファイル名に置き換えます。

ステップ 6　Manager アプライアンス上で、`root` ユーザとして `bash` を実行します。

ステップ 7　Manager シェルで、次のようにディレクトリを移動します。

```
cd /usr/local/reactivity/private/
```

ステップ 8　`private` ディレクトリから次のコマンドを実行し、Manager の現在の鍵データベースをバックアップします。

```
mv client.p12 client.p12.bak
```

このコマンドによって、ファイル名が `client.p12` から `client.p12.bak` に変更されます。このファイルには、Manager が管理する Gateway に接続するために Manager が使用するハードウェアベースの秘密鍵が保存されます。次のステップで、新しい `client.p12` ファイルを作成します。

ステップ 9　次の 2 つのコマンドを入力して鍵および対応する CSR を作成します。

```
$ openssl genrsa -out client.pem 1024
$ openssl req -key client.pem \
-out client_req.pem -new -subj \
"/CN=gatewayhost/OU=myorgunit/O=MyCompany/L=Belmont/ST=California/C=US"
```

コマンドの中で、イタリック体のテキストは各自の状況に適した値に置き換えます。

ステップ 10　trusted CA に CSR データ（client_req.pem ファイル）を送信し、署名入りの X.509 証明書に変換します。

ステップ 11　CA から電子メールの本文として署名入り証明書を受け取った場合は、証明書の内容だけをテキストファイルに保存します。

- BEGIN CERTIFICATE の行全体から END CERTIFICATE の行全体までをすべて含めます。
- ローカル ファイル システムで、有効な Linux ファイル名を使用してファイルを保存します。このファイル名にはスペース、アポストロフィ、アンパサンド、およびその他の特殊文字を使用しないでください。

署名入り証明書を Manager のファイル システムに移動します。

ステップ 12　Manager シェルの private ディレクトリ で、次のコマンドを実行して client.pem ファイルに署名入り証明書をインストールします。

```
$ cat GCERT.CRT >> client.pem
```

実際のコマンドでは、*GCERT.CRT* を署名入り証明書のファイル名に置き換えます。

（注）　必ず出力リダイレクト演算子 >> を使用して、署名入り証明書を client.pem ファイルに追加してください（このファイルを置き換えないでください）。このファイルが置き換えられると、generatekey ツールでこのファイルに格納した秘密鍵が失われてしまうため、キーストアが証明書の有効性を認識できなくなります。このエラーを修復するには、ここでの全手順を繰り返し、新しい鍵、新しい CSR、および新しい証明書を作成してインストールする必要があります。

ステップ 13　次のコマンドにより、クライアント PEM ファイルを PKCS#12 ファイルに変換します。

```
openssl pkcs12 -export -out client.p12 -in client.pem
```

ステップ 14　エクスポートのパスワードを入力するためのプロンプトが表示されたら、approuter をパスワードとして入力してください。プロンプトで要求された場合には、入力したパスワードを確認してください。

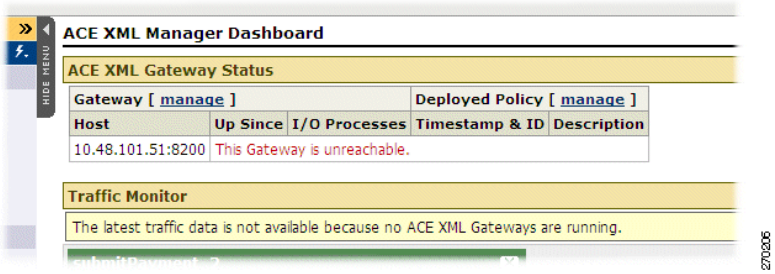
これらの手順が完了すると、Manager は新しい鍵を双方向証明書交換に使用します。証明書交換をテストするには、次の 「管理証明書交換のテスト」（P.8-12）で説明されているように Manager を再起動して Gateway との接続を確認します。

管理証明書交換のテスト

これまでの説明にしたがって Manager および Gateway を設定した後、Manager の Web コンソールでイベント ログを表示することによって、インストールをテストできます。イベント ログに移動するには、Manager が管理対象の各 Gateway に対して双方向証明書交換を実行し、ログのエントリを取得する必要があります。

Manager の Web コンソールにログイン後、Manager が Gateway クラスタ メンバにアクセスできないことを示す警告が Dashboard に表示されていないことを確認します。図 8-1 に例を示します。

図 8-1　到達不能な Gateway



インストール プロセスの他の部分を正しく完了しないまま証明書を置き換えた場合、完全なインストールではなくても、Manager の Web コンソールにログインしたり、Manager や Gateway との端末セッションを確立したりできる場合があります。ハードウェアベース鍵をインストールする前に Gateway が正しく設定されていても、証明書のロードまたはキーストアの読み込みに関連するエラーが原因で、Gateway が正常に起動しない場合があります。このメッセージが表示された場合、Event Log を検証することによって、問題を特定できる可能性があります。

Event Log を表示し、ハードウェア キーストア関連の問題またはその他の起動時の問題を示す **Notice**、**Warning** 、または **Alert** メッセージを確認します。

Event Log にエントリを入力するには、ポーリングによって新しいイベントを検出し、ログに入力する前提条件として、Manager はクラスタ内の各 Gateway と双方向証明書交換を実行する必要があります。したがって、**Notice** 以上のレベルに設定された **Event Log** を表示し、その中に証明書、ハードウェア キーストア、または Manager およびその Gateway クラスタ間の通信に関連する問題が含まれていない場合は、双方向の証明書交換に使用される証明書が正しくインストールされていることになります。

監査ログ署名クレデンシャルの変更

Console Audit Log は、Manager の Web コンソール ページであり、ポリシーの配布、現在のポリシーの変更、管理アカウントのユーザ権限に関する変更など、システムに影響を与える管理レベルの変更が表示されます。監査ログには、行われた変更のほかに、その変更を行った担当者も示されます。

監査ログでは、PKI クレデンシャルを使用し、プロセスを認証してから、プロセスに対して監査ログの編集および署名を許可します。ここでは、このクレデンシャルで通常使用されるソフトウェアベースの鍵の代わりに、ハードウェアベースの鍵を使用する方法について説明します。

作業を開始する前に、次の準備が必要です。

- ハードウェアベース SSL エンジンを使用可能にします。詳細については、「SSL アクセラレーションの有効化」（P.9-1）を参照してください。
- nCipher セキュリティ ワールドにアプライアンスを追加します。

監査ログ署名クレデンシャルを変更するには次の手順に従います。

ステップ 1　Manager マシン上で、`root` ユーザとしてアプライアンス シェルにログインします。

ステップ 2　メニューから [Manage Gateway Processes] を選択します。

ステップ 3　[Manage Gateway Processes] メニューで、[Stop Manager] を選択します。

アプライアンスによって Manager プロセスがシャットダウンされ、この処理が正常に実行されたことを示すステータス画面が表示されます。

ステップ 4　**Enter** キーを押して、ステータス画面を閉じます。

ステップ 5　[Manage Gateway Processes] メニューで [Return to Main Menu] を選択します。

ステップ 6　[Main Menu] から [Advanced Options] を選択します。

ステップ 7　[Advanced Options] メニューから [Run bash] を選択します。

ステップ 8　bash コマンド プロンプトで、次のディレクトリに移動します。

```
cd /usr/local/reactivity
```

ステップ 9　監査ログ署名用の新しい nCipher 保護キーストアと自己署名証明書を作成するために、次のコマンドを実行します。

```
$ bin/ncipherkeytool -genkey
   -keystore private/auditlog.ncipher
   -alias client -keyalg RSA -keysize 1024
   -dname "CN=auditlog"
```

コマンドが正常に実行されたことを確認するには、/usr/local/reactivity/private ディレクトリの内容を表示し、新しく作成された auditlog.ncipher ファイルが存在しているかどうかを確認します。たとえば、次のコマンドを使用できます。

```
ls -lt private
```

ステップ 10　次のコマンドを入力し、現在の監査ログ証明書をバックアップします。

```
$ mv private/auditlog.crt private/auditlog.crt.bak
```

このコマンドによって、auditlog.crt の名前が auditlog.crt.bak に変更されます。処理を確認するために、private ディレクトリの内容を表示します。名前変更の処理が正常に完了した場合は、このディレクトリに auditlog.crt.bak ファイルが存在し、auditlog.crt ファイルは存在しません。

ステップ 11　次のコマンドを実行し、ログ検証ユーティリティに使用させる新しい監査ログ証明書をキーストアから抽出します。

```
$ bin/ncipherkeytool -export -rfc -keystore private/auditlog.ncipher
     -alias client -file private/auditlog.crt
```

[Certificate stored in file <private/auditlog.crt>] メッセージが表示されます。

ステップ 12　/usr/local/reactivity/config/webapp.properties を次のように編集します。

a.　次の行の p12 を ncipher に変更します。

```
audit.log.private.key.pcks12= /usr/local/reactivity/private/auditlog.p12
```

次のように変更します。

```
audit.log.private.key.pcks12= /usr/local/reactivity/private/auditlog.ncipher
```

b.　次の行の pkcs12 を ncipher.sworld に変更します。

```
audit.log.signing.keystore.type=pkcs12
```

次のように変更します。

```
audit.log.signing.keystore.type=ncipher.sworld
```

ステップ 13　Manager シェルで次のコマンドを実行し、agateway を webapp.properties のオーナーおよびグループとして設定します。

```
chown agateway:agateway /usr/local/reactivity/config/webapp.properties
```

ステップ 14　次のコマンドを実行し、webapp.properties ファイルに割り当てられたオーナーおよびグループを表示して、ファイル所有権の変更を確認します。

```
ls -la /usr/local/reactivity/config
```

シェルによって、config ディレクトリの内容が表示されます。次の出力では、webapp.properties ファイルに割り当てられたオーナーおよびグループは agateway となっています。

```
-rw-r--r-- 1 agateway agateway 2874 Feb 8 00:34 webapp.properties
```

ステップ 15　次のコマンドを入力し、監査ログの署名状態をリセットします。

```
$ rm auditlogs/audit.console.current
```

このコマンドによって、現在の監査ログが削除されます。以降の手順で、ハードウェアベース証明書で署名された新しい監査ログを作成します。

ステップ 16　`bash` シェルを終了します。

ステップ 17　[Advanced Options] メニューで [Return to Main Menu] を選択します。

ステップ 18　メニューから [Manage Gateway Processes] を選択します。

ステップ 19　[Start Manager] を選択します。

アプライアンスによって Manager プロセスの再起動が試行され、この処理の状況を示すステータス画面が表示されます。

ステップ 20　**Enter** キーを押して、ステータス画面を閉じます。

[Manage Gateway Processes] メニューが再び表示されます。

ステップ 21　（アプライアンスのシェルではなく）Manager の Web コンソールに、管理者のロールが与えられたユーザとしてログインします。

[Dashboard] が表示されます。

ステップ 22　[Reports and Tools] > [Event Log] リンクをクリックします。

Event Log に次のメッセージが表示されます。

A "/usr/local/reactivity/auditlogs/audit.console.current" not found.This file should only be missing on a newly installed Manager web console.

前の手順で `audit.console.current` ファイルを削除したため、これは予期されたエラー メッセージです。削除したファイルの代わりに、Manager が新しいログ ファイルを書き込むため、以後のログイン時にこのメッセージが表示されることはありません。