外部キー管理を設定
ONTAP 9

NetApp
April 24, 2024

目次

外部キー管理を設定

外部キー管理の概要の設定

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、 Key Management Interoperability Protocol （ KMIP ）を使用してノードにキーを提供します。

ONTAP 9.1 以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理 LIF を割り当てる必要があります。

ONTAP 9.1 以降では、オンボードキーマネージャを使用して NetApp Volume Encryption （ NVE ）を実装できます。ONTAP 9.3 以降では、 NVE を外部キー管理（ KMIP ）およびオンボードキーマネージャとともに実装できます。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照してください クラスタ化されたキーサーバを設定

ONTAP 9.2 以前でネットワーク情報を収集

ONTAP 9.2 以前を使用している場合は、外部キー管理を有効にする前にネットワーク設定ワークシートに情報を記入してください。

ONTAP 9.3 以降では、必要なすべてのネットワーク情報が自動的に検出されます。

項目	注：	価値
キー管理ネットワークインターフェイスの名前		
キー管理ネットワークインターフェイスの IP アドレス	ノード管理 LIF の IPv4 形式または IPv6 形式の IP アドレス	
キー管理ネットワークインターフェイスの IPv6 ネットワークプレフィックス長	IPv6 を使用している場合、 IPv6 ネットワークプレフィックス長	
キー管理ネットワークインターフェイスのサブネットマスク		
キー管理ネットワークインターフェイスのゲートウェイの IP アドレス		
クラスタネットワークインターフェイスの IPv6 アドレス	キー管理ネットワークインターフェイスに IPv6 を使用している場合にのみ必要です	

各 KMIP サーバのポート番号	任意。すべての KMIP サーバで同じポート番号を使用してください。ポート番号を指定しなかった場合は、デフォルトでポート 5696 が使用されます。これは、 Internet Assigned Numbers Authority （ IANA ）が KMIP に割り当てているポートです。	
キータグ名	任意。キータグ名は、ノードに属するすべてのキーを識別するために使用されます。デフォルトのキータグ名はノード名です。	

関連情報

"ネットアップテクニカルレポート 3954 ：『 NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager 』"

"ネットアップテクニカルレポート 4074 ：『 NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure 』"

クラスタに SSL 証明書をインストールします

クラスタと KMIP サーバの間では、相互の ID を検証して SSL 接続を確立するために KMIP SSL 証明書を使用します。KMIP サーバとの SSL 接続を設定する前に、クラスタの KMIP クライアント SSL 証明書、および KMIP サーバのルート Certificate Authority （ CA ；認証局）の SSL パブリック証明書をインストールする必要があります。

このタスクについて

HA ペア構成では、両方のノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。複数の HA ペアを同じ KMIP サーバに接続する場合は、 HA ペアのすべてのノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。

作業を開始する前に

- 証明書を作成するサーバ、 KMIP サーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリック SSL KMIP クライアント証明書を入手しておく必要があります。
- クラスタの SSL KMIP クライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIP クライアント証明書は、パスワードで保護しないでください。
- KMIP サーバのルート認証局（ CA ）の SSL パブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。

> KMIP サーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

手順

1. クラスタに SSL KMIP クライアント証明書をインストールします。

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   SSL KMIP パブリック証明書とプライベート証明書を入力するように求められます。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. KMIP サーバのルート認証局（ CA ）の SSL パブリック証明書をインストールします。

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

ONTAP 9.6 以降で外部キー管理を有効にする（ハードウェアベース）

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

ONTAP 9.11.1以降では、プライマリキーサーバごとに最大3つのセカンダリキーサーバを追加して、クラスタ化されたキーサーバを作成できます。詳細については、を参照してください クラスタ構成の外部キーサーバを構成。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、 MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスタにKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   - 。 `security key-manager external enable` コマンドは、に置き換わるものです `security key-manager setup` コマンドを実行しますを実行できます `security key-manager external modify` コマンドを使用して、外部キー管理の設定を変更します。コマンド構文全体については、マニュアルページを参照してください。
   - MetroCluster 環境で管理SVMに外部キー管理を設定する場合は、を繰り返す必要があります `security key-manager external enable` パートナークラスタに対して実行します。

次のコマンドは、の外部キー管理を有効にします `cluster1` 3つの外部キーサーバで構成されます。最初のキーサーバはホスト名とポートで指定し、 2 番目のキーサーバは IP アドレスとデフォルトポートで指定し、 3 番目のキーサーバは IPv6 アドレスとポートで指定します。

```
clusterl::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 設定したすべての KMIP サーバが接続されていることを確認します。

   `security key-manager external show-status -node node_name -vserver SVM -key -server host_name|IP_address:port -key-server-status available|not-responding|unknown`

   > 。 `security key-manager external show-status` コマンドは、に置き換わるものです `security key-manager show -status` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

ONTAP 9.5 以前で外部キー管理を有効にします

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

このタスクについて

ONTAP は、クラスタ内のすべてのノードについて KMIP サーバの接続を設定します。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、 MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスタにKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタノードのキー管理ツールの接続を設定します。

   ```
   security key-manager setup
   ```

   キー管理ツールのセットアップが開始されます。

   > MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

2. 各プロンプトで適切な応答を入力します。
3. KMIP サーバを追加します。

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

4. 冗長性を確保するために KMIP サーバをもう 1 つ追加します。

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

5. 設定したすべての KMIP サーバが接続されていることを確認します。

   ```
   security key-manager show -status
   ```

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager show -status

Node             Port      Registered Key Manager  Status
--------------   ----      -----------------------  ---------------
cluster1-01      5696      20.1.1.1                 available
cluster1-01      5696      20.1.1.2                 available
cluster1-02      5696      20.1.1.1                 available
cluster1-02      5696      20.1.1.2                 available
```

6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   `volume encryption conversion start`

   ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

クラスタ構成の外部キーサーバを構成

ONTAP 9.11.1以降では、SVM上のクラスタ化された外部キー管理サーバへの接続を設定できます。クラスタ化されたキーサーバを使用すると、SVMのプライマリキーサーバとセカンダリキーサーバを指定できます。キーを登録すると、ONTAP は、処理が正常に完了するまで、プライマリキーサーバへのアクセスを順次試行する前に、キーの重複を防止します。

外部キーサーバは、NSE、NVE、NAE、およびSEDのキーに使用できます。SVMでは、最大4つのプライマリ外部KMIPサーバをサポートできます。各プライマリサーバは、最大3台のセカンダリキーサーバをサポートできます。

作業を開始する前に

- "SVMでKMIPキー管理が有効になっている必要があります。"。
- このプロセスでサポートされるのは、KMIPを使用するキーサーバのみです。サポートされているキーサーバの一覧については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
- クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- サーバの順序は、で引数をリストします `-secondary-key-servers` パラメータには、外部キー管理（KMIP）サーバのアクセス順序が反映されます。

クラスタ化されたキーサーバを作成します

設定手順 は、プライマリキーサーバを設定したかどうかによって異なります。

SVMにプライマリキーサーバとセカンダリキーサーバを追加する

1. クラスタでキー管理が有効になっていないことを確認します。
   `security key-manager external show -vserver` *`svm_name`*
   SVMですでに最大4つのプライマリキーサーバが有効になっている場合は、新しいプライマリキーサーバを追加する前に既存のプライマリキーサーバの1つを削除する必要があります。
2. プライマリキー管理ツールを有効にします。
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

既存のプライマリキーサーバにセカンダリキーサーバを追加する

1. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   セカンダリキーサーバの詳細については、を参照してください [mod-secondary]。

クラスタ化されたキーサーバを変更

外部キーサーバクラスタの変更では、特定のキーサーバのステータス（プライマリまたはセカンダリ）を変更したり、セカンダリキーサーバを追加および削除したり、セカンダリキーサーバのアクセス順序を変更したりできます。

プライマリキーサーバとセカンダリキーサーバの変換

プライマリキーサーバをセカンダリキーサーバに変換するには、まずを使用してSVMからプライマリキーサーバを削除する必要があります `security key-manager external remove-servers` コマンドを実行します

セカンダリキーサーバをプライマリキーサーバに変換するには、まず既存のプライマリキーサーバからセカンダリキーサーバを削除する必要があります。を参照してください [mod-secondary]。既存のキーの削除中にセカンダリキーサーバをプライマリサーバに変換する場合、削除および変換を実行する前に新しいサーバを追加しようとすると、キーが重複する可能性があります。

セカンダリキーサーバを変更します。

セカンダリキーサーバの管理はで行います `-secondary-key-servers` のパラメータ `security key-manager external modify-server` コマンドを実行します。 `-secondary-key-servers` パラメータにはカンマで区切ったリストを指定できます。リスト内で指定されたセカンダリキーサーバの順序によって、セカンダリキーサーバのアクセスシーケンスが決まります。アクセス順序は、コマンドを実行して変更できます `security key-manager external modify-server` セカンダリキーサーバを別の順序で入力します。

セカンダリキーサーバを削除するには、を実行します `-secondary-key-servers` 引数には、削除するキーサーバを省略して保持するキーサーバを指定する必要があります。すべてのセカンダリキーサーバを削除する

には、引数を使用します –「なし」を意味します。

追加情報 の場合は、を参照してください `security key-manager external` ページのを参照してください "ONTAP コマンドリファレンス"。

ONTAP 9.6 以降で認証キーを作成します

を使用できます `security key-manager key create` コマンドを使用してノードの認証キーを作成し、設定したKMIPサーバに格納します。

このタスクについて

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPSへの準拠にデータアクセスと同じ認証キーを使用できます。

ONTAP では、クラスタ内のすべてのノードに対して認証キーが作成されます。

- このコマンドは、オンボードキーマネージャが有効になっている場合はサポートされません。ただし、オンボードキーマネージャを有効にすると、 2 つの認証キーが自動的に作成されます。キーを表示するには、次のコマンドを使用します。

  ```
  security key-manager key query -key-type NSE-AK
  ```

- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されます。
- を使用できます `security key-manager key delete` 使用されていないキーを削除するコマンド。。 `security key-manager key delete` 指定したキーがONTAP で現在使用されている場合、コマンドは失敗します。(このコマンドを使用するには 'admin より大きい特権が必要です)

> MetroCluster 環境でキーを削除する前に、キーがパートナークラスタで使用されていないことを確認する必要があります。パートナークラスタで次のコマンドを使用して、キーが使用されていないことを確認できます。
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

> 設定 `prompt-for-key=true` 暗号化されたドライブを認証するときに、クラスタ管理者に使用するパスフレーズの入力を求めるプロンプトが表示されます。設定しない場合は、32 バイトのパスフレーズが自動的に生成されます。 。 `security key-manager key create` コマンドは、に置き換わるものです `security key-manager create-key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーを作成します `cluster1`では、32バイトのパスフレーズが自動的に生成されます。

```
cluster1::> security key-manager key create
Key ID:
00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. 認証キーが作成されたことを確認します。

   `security key-manager key query -node node`

   > 。 `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。 出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

   次の例は、の認証キーが作成されたことを確認します `cluster1`：

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

ONTAP 9.5 以前で認証キーを作成します

を使用できます `security key-manager create-key` コマンドを使用してノードの認証キーを作成し、設定したKMIPサーバに格納します。

このタスクについて

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、 FIPS 準拠の認証キーをデータアクセスにも使用できます。

ONTAP では、クラスタ内のすべてのノードに対して認証キーが作成されます。

- このコマンドは、オンボードキー管理が有効な場合はサポートされません。

- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されます。

  キー管理サーバソフトウェアを使用して未使用のキーを削除し、もう一度コマンドを実行できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

   ```
   security key-manager create-key
   ```

   コマンド構文全体については、コマンドのマニュアルページを参照してください。

   > 出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

   次の例は、の認証キーを作成します `cluster1`：

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 認証キーが作成されたことを確認します。

   ```
   security key-manager query
   ```

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は、の認証キーが作成されたことを確認します `cluster1`：

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

FIPS ドライブまたは SED にデータ認証キーを割り当てる（外部キー管理）

を使用できます `storage encryption disk modify` コマンドを使用してFIPSドライブまたはSEDにデータ認証キーを割り当てることができます。このキーは、クラスタノードでドライブ上の暗号化されたデータをロックまたはロック解除する際に使用します。

このタスクについて

自己暗号化ドライブの認証キー ID がデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。Manufacturer Secure ID （ MSID ；メーカーのセキュア ID ）のキー ID が 0x0 になり、 SAS ドライブの標準のデフォルト値になります。NVMe ドライブの場合、標準のデフォルト値は null キーで、空のキー ID として表されます。キー ID を自己暗号化ドライブに割り当てると、認証キー ID がデフォルト以外の値に変更されます。

この手順 はシステムの停止を伴いません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   コマンド構文全体については、コマンドのマニュアルページを参照してください。

   > を使用できます `security key-manager query -key-type NSE-AK` キーIDを表示するコマンド。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

   コマンド構文全体については、マニュアルページを参照してください。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```