証明書を使用してリモートサーバの ID を確認します

ONTAP 9

NetApp
September 12, 2024

目次

証明書を使用してリモートサーバの ID を確認します

証明書の概要を使用してリモートサーバの ID を確認します

ONTAP は、リモートサーバの ID を検証するセキュリティ証明書機能をサポートしています。

ONTAP ソフトウェアでは、次のデジタル証明書機能とプロトコルを使用して安全に接続できます。

- Online Certificate Status Protocol （ OCSP ）は、 SSL 接続と Transport Layer Security （ TLS ）接続を使用して、 ONTAP サービスからのデジタル証明書要求のステータスを検証します。この機能はデフォルトでは無効になっています。
- ONTAP ソフトウェアには、信頼されたルート証明書のデフォルトセットが付属しています。
- Key Management Interoperability Protocol （ KMIP ）の証明書を使用して、クラスタと KMIP サーバの相互認証を有効にできます。

OCSP を使用してデジタル証明書が有効であることを確認します

ONTAP 9.2 以降では、 Online Certificate Status Protocol （ OCSP ）を有効にすることで、 Transport Layer Security （ TLS ）通信を使用する ONTAP アプリケーションでデジタル証明書のステータスを受信できます。OCSP による証明書のステータスチェックは、特定のアプリケーションに対していつでも有効または無効にできます。デフォルトでは、 OCSP による証明書のステータスチェックは無効になっています。

必要なもの

このタスクを実行するには、advanced権限レベルのアクセス権が必要です。

このタスクについて

OCSP は、次のアプリケーションをサポートしています。

- AutoSupport
- イベント管理システム（ EMS ）
- LDAP over TLS
- Key Management Interoperability Protocol （ KMIP ）
- 監査ログ
- FabricPool
- SSH（ONTAP 9.13.1以降）

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`。

2. 特定の ONTAP アプリケーションで OCSP による証明書のステータスチェックを有効または無効にするには、次の該当するコマンドを使用します。

一部のアプリケーションで **OCSP** による証明書のステータスチェックを有効または無効にする場合	使用するコマンド
有効	`security config ocsp enable -app app name`
無効	`security config ocsp disable -app app name`

次のコマンドは、 AutoSupport および EMS の OCSP サポートを有効にします。

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSP を有効にすると、アプリケーションは次のいずれかの応答を受信します。

- Good - 証明書は有効で、通信可能な状態です。
- Revoked - 証明書は発行元の認証局によって永続的に信頼できないと判断されており、通信不可能な状態です。
- Unknown - サーバが証明書に関するステータス情報を持っていないため、通信不可能な状態です。
- OCSP server information is missing in the certificate - TLS 通信は続行していますが、サーバで OCSP が無効であると判断されているため、ステータスチェックは実行されません。
- No response from OCSP server - アプリケーションを実行できない状態です。

3. TLS を使用するすべてのアプリケーションで OCSP による証明書のステータスチェックを有効または無効にするには、次の該当するコマンドを使用します。

すべてのアプリケーションで **OCSP** による証明書のステータスチェックを有効または無効にする場合	使用するコマンド

有効	`security config ocsp enable`
	
	`-app all`

無効	`security config ocsp disable`
	
	`-app all`

有効にすると、指定した証明書が「有効」、「失効」、「不明」のいずれであるかを示す署名済みの応答が、すべてのアプリケーションに送信されます。証明書のステータスが revoked の場合は、アプリケーションは実行できません。アプリケーションが OCSP サーバから応答を受信できない場合、または OCSP サーバにアクセスできない場合、アプリケーションは続行できません。

4. を使用します `security config ocsp show` コマンドを使用して、OCSPをサポートするすべてのアプリケーションとそのサポートステータスを表示します。

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

TLS ベースのアプリケーションのデフォルト証明書を表示します

ONTAP 9.2 以降では、 ONTAP に、 Transport Layer Security （ TLS ）を使用する ONTAP アプリケーション用の信頼されたルート証明書のデフォルトセットが付属しています。

必要なもの

デフォルトの証明書は、管理 SVM の作成時、または ONTAP 9.2 へのアップグレード時に、管理 SVM にのみインストールされます。

このタスクについて

現在クライアントとして機能し、証明書の検証が必要なアプリケーションは、 AutoSupport 、 EMS 、 LDAP 、監査ログ、 FabricPool 、 および KMIP を使用できます。

証明書の有効期限が切れると、ユーザに証明書を削除するよう要求する EMS メッセージが起動します。デフォルトの証明書は、 advanced 権限レベルでのみ削除できます。

> デフォルトの証明書を削除すると、一部の ONTAP アプリケーションが正常に機能しなくなる場合があります（ AutoSupport 、監査ログなど）。

ステップ

1. 管理 SVM にインストールされているデフォルトの証明書を表示するには、 security certificate show コマンドを使用します。

   `security certificate show -vserver -type server-ca`

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                             Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```