使用证书验证远程服务器的身份

ONTAP 9

NetApp
April 24, 2024

目录

使用证书验证远程服务器的身份

使用证书概述验证远程服务器的身份

ONTAP 支持使用安全证书功能来验证远程服务器的身份。

ONTAP 软件支持使用以下数字证书功能和协议进行安全连接：

- 联机证书状态协议（ Online Certificate Status Protocol ， OCSP ）使用 SSL 和传输层安全（ Transport Layer Security ， TLS ）连接验证 ONTAP 服务发出的数字证书请求的状态。默认情况下，此功能处于禁用状态。
- ONTAP 软件附带了一组默认的可信根证书。
- 密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）证书支持对集群和 KMIP 服务器进行相互身份验证。

使用 **OCSP** 验证数字证书是否有效

从 ONTAP 9.2 开始，启用联机证书状态协议（ Online Certificate Status Protocol ， OCSP ）后，使用传输层安全（ Transport Layer Security ， TLS ）通信的 ONTAP 应用程序可以接收数字证书状态。您可以随时为特定应用程序启用或禁用 OCSP 证书状态检查。默认情况下， OCSP 证书状态检查处于禁用状态。

您需要的内容

要执行此任务、您需要具有高级权限级别访问权限。

关于此任务

OCSP 支持以下应用程序：

- AutoSupport
- 事件管理系统（ EMS ）
- 基于 TLS 的 LDAP
- 密钥管理互操作性协议（ KMIP ）
- 审核日志记录
- FabricPool
- SSH (从ONTAP 9.13.1开始)

步骤

1. 将权限级别设置为高级： `set -privilege advanced`。
2. 要为特定 ONTAP 应用程序启用或禁用 OCSP 证书状态检查，请使用相应的命令。

某些应用程序的 **OCSP** 证书状态检查	使用命令 **...**
enabled	`security config ocsp enable -app app name`
已禁用	`security config ocsp disable -app app name`

以下命令可为 AutoSupport 和 EMS 启用 OCSP 支持。

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

启用 OCSP 后，应用程序将收到以下响应之一：

- 良好—证书有效，通信继续进行。
- 已撤销—证书被其颁发证书颁发机构永久视为不可信，通信无法继续。
- 未知 - 服务器没有任何有关证书的状态信息，通信无法继续。
- 证书中缺少 OCSP 服务器信息—此服务器就像禁用了 OCSP 一样，并继续进行 TLS 通信，但不会进行状态检查。
- OCSP 服务器无响应—应用程序无法继续。

3. 要对使用 TLS 通信的所有应用程序启用或禁用 OCSP 证书状态检查，请使用相应的命令。

希望所有应用程序的 **OCSP** 证书状态检查为 **...**	使用命令 **...**

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

已禁用	`security config ocsp disable`
	
	`-app all`

启用后，所有应用程序都会收到签名响应，表示指定的证书正常，已撤销或未知。如果证书已被撤销，则应用程序将无法继续。如果应用程序无法从 OCSP 服务器收到响应，或者服务器无法访问，则应用程序将无法继续。

4. 使用 `security config ocsp show` 命令以显示支持OCSP的所有应用程序及其支持状态。

```
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.
```

查看基于 TLS 的应用程序的默认证书

从 ONTAP 9.2 开始， ONTAP 为使用传输层安全（ Transport Layer Security ， TLS ）的 ONTAP 应用程序提供了一组默认的可信根证书。

您需要的内容

只有在创建管理 SVM 期间或在升级到 ONTAP 9.2 期间，才会安装默认证书。

关于此任务

当前用作客户端并需要证书验证的应用程序包括 AutoSupport ， EMS ， LDAP ，审核日志记录， FabricPool ， 和 KMIP 。

证书过期后，系统会调用一条 EMS 消息，请求用户删除证书。只能在高级权限级别删除默认证书。

> 删除默认证书可能会导致某些 ONTAP 应用程序无法按预期运行（例如， AutoSupport 和审核日志记录）。

步骤

1. 您可以使用 security certificate show 命令查看管理员 SVM 上安装的默认证书：

   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
```