



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 1
 - 使用证书概述验证远程服务器的身份 1
 - 使用 OCSP 验证数字证书是否有效 1
 - 查看基于 TLS 的应用程序的默认证书 3

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	<code>security config ocsp enable -app app name</code>
已禁用	<code>security config ocsp disable -app app name</code>

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	<code>security config ocsp enable</code> <code>-app all</code>
已禁用	<code>security config ocsp disable</code> <code>-app all</code>

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 ocsf 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                AACertificateServices
server-ca
  Certificate Authority: AAA Certificate Services
    Expiration Date: Sun Dec 31 18:59:59 2028
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。