



证书管理 SANtricity 11.6

NetApp
February 12, 2024

目录

- 证书管理 1
 - 概念 1
 - 操作说明 3

证书管理

概念

证书的工作原理

证书是数字文件、用于标识网站和服务器等在线实体、以实现Internet上的安全通信。

签名证书

证书可确保Web通信仅在指定服务器和客户端之间以加密格式单独传输、不会被更改。使用Unified Manager、您可以管理主机管理系统上的浏览器证书以及发现的存储阵列中的控制器证书。

证书可以由可信的颁发机构签名、也可以是自签名证书。"签名"只是指有人验证了所有者的身份并确定其设备可以受信任。存储阵列会在每个控制器上随附一个自动生成的自签名证书。您可以继续使用自签名证书、也可以获取CA签名证书、以便在控制器和主机系统之间建立更安全的连接。



虽然CA签名证书可提供更好的安全保护(例如、防止中间人攻击)、但如果您的网络较大、则还需要支付昂贵的费用。相比之下、自签名证书的安全性较低、但它们是免费的。因此、自签名证书最常用于内部测试环境、而不是生产环境。

签名证书由可信的第三方组织证书颁发机构(CA)进行验证。签名证书包括有关实体(通常是服务器或网站)所有者的详细信息、证书问题描述 和到期日期、实体的有效域以及由字母和数字组成的数字签名。

当您打开浏览器并输入Web地址时、系统会在后台执行证书检查过程、以确定您是否要连接到包含有效的CA签名证书的网站。通常、使用签名证书进行安全保护的站点会在地址中包含挂锁图标和https标志。如果您尝试连接到不包含CA签名证书的网站、浏览器将显示一条警告、指出此站点不安全。

CA会在应用程序过程中执行一些步骤来验证您的身份。他们可能会向您的注册业务发送电子邮件、验证您的业务地址以及执行HTTP或DNS验证。应用程序过程完成后、CA会向您发送数字文件、以便在主机管理系统上加载。通常、这些文件包括以下信任链：

- 根-层次结构顶部是根证书、其中包含用于对其他证书进行签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
- 中间证书—从根分层是中间证书。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。
- 服务器—链的底部是服务器证书、用于标识您的特定实体、例如网站或其他设备。存储阵列中的每个控制器都需要一个单独的服务器证书。

自签名证书

存储阵列中的每个控制器都包含一个预安装的自签名证书。自签名证书与CA签名证书类似、只是它由实体所有者而非第三方进行验证。与CA签名证书一样、自签名证书也包含自己的专用密钥、并确保数据经过加密并通过HTTPS连接在服务器和客户端之间发送。

自签名证书不受浏览器“信任”。每次尝试连接到仅包含自签名证书的网站时、浏览器都会显示一条警告消息。您必须单击警告消息中允许您继续访问网站的链接；这样、您实际上就是在接受自签名证书。

Unified Manager的证书

Unified Manager界面随Web服务代理一起安装在主机系统上。打开浏览器并尝试连接到Unified Manager时、浏览器会尝试通过检查数字证书来验证主机是否为可信源。如果浏览器找不到服务器的CA签名证书、则会打开一条警告消息。从该站点、您可以继续访问该网站以接受该会话的自签名证书。或者、您也可以从CA获取签名的数字证书、以便不再显示警告消息。

控制器的证书

在Unified Manager会话期间、当您尝试访问没有CA签名证书的控制器时、可能会看到其他安全消息。在这种情况下、您可以永久信任自签名证书、也可以为控制器导入CA签名证书、以便Web服务代理服务器可以对来自这些控制器的传入客户端请求进行身份验证。

证书术语

以下术语适用于证书管理。

期限	Description
CA	证书颁发机构(Certificate Authority、CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。
CSR	证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述 所需的信息。
证书	出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。
证书链	一种文件层次结构、用于向证书添加一层安全保护。通常、此链包含一个位于层次结构顶部的根证书、一个或多个中间证书以及用于标识实体的服务器证书。
中间证书	一个或多个中间证书从证书链中的根分支。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。
密钥库	密钥库是主机管理系统上的存储库、其中包含私钥及其对应的公有 密钥和证书。这些密钥和证书用于标识您自己的实体、例如控制器。
根证书	根证书位于证书链中的层次结构顶部、其中包含用于对其他证书签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
签名证书	由证书颁发机构(CA)验证的证书。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。此外、签名证书还包括实体所有者的详细信息(通常为服务器或网站)以及由字母和数字组成的数字签名。签名证书使用信任链、因此最常用于生产环境。也称为"CA签名证书"或"管理证书"。

期限	Description
自签名证书	自签名证书由实体的所有者进行验证。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。它还包括由字母和数字组成的数字签名。自签名证书与CA签名证书使用的信任链不同、因此最常用于测试环境。也称为"预安装"证书。
服务器证书	服务器证书位于证书链的底部。它标识您的特定实体、例如网站或其他设备。存储系统中的每个控制器都需要一个单独的服务器证书。
信任存储库	信任存储库是一个存储库、其中包含来自CA等可信第三方的证书。
Web服务代理	Web服务代理可通过标准HTTPS机制提供访问、允许管理员为存储阵列配置管理服务。代理可以安装在Windows或Linux主机上。Unified Manager界面与Web服务代理捆绑在一起。

操作说明

使用CA签名的证书

您可以获取并导入CA签名的证书、以安全访问托管Unified Manager的管理系统。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

使用CA签名证书是一个两步操作步骤。

第1步：完成并提交CSR

您必须先生成证书签名请求(CSR)文件并将其发送到CA。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

此任务介绍如何生成发送给CA的CSR文件、以接收托管Unified Manager和Web服务代理的系统的已签名管理证书。您必须提供有关您的组织的信息以及主机系统的IP地址或DNS名称。



提交给CA后、请勿生成新的CSR。生成CSR时、系统会创建一个专用密钥对和公有 密钥对。公有 密钥是CSR的一部分、而私钥则保留在密钥库中。当您收到签名证书并将其导入到密钥库中时、系统会确保私钥和公有 密钥都是原始对。因此、在向CA提交新的CSR后、您不能生成新的CSR。否则、控制器将生成新密钥、而从CA收到的证书将不起作用。

步骤

1. 选择*证书管理*。

2. 从*管理*选项卡中、选择*完成CSR*。
3. 输入以下信息、然后单击*下一步*：
 - 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
 - 组织单位(可选)—组织中负责处理证书的部门。
 - 城市/位置-主机系统或业务所在的城市。
 - 省/自治区/直辖市(可选)—主机系统或业务所在的省/自治区/直辖市。
 - 国家/地区ISO代码—您所在国家/地区的两位数ISO (国际标准化组织)代码、例如美国。
4. 输入有关主机系统的以下信息：
 - 公用名—安装了Web服务代理的主机系统的IP地址或DNS名称。请确保此地址正确无误；它必须与您在浏览器中输入的地址完全匹配才能访问Unified Manager。请勿包含http://或https://。
 - 备用IP地址-如果公用名称为IP地址、则可以选择为主机系统输入任何其他IP地址或别名。对于多个条目、请使用逗号分隔格式。
 - 备用DNS名称-如果公用名称为DNS名称、请输入主机系统的任何其他DNS名称。对于多个条目、请使用逗号分隔格式。如果没有备用DNS名称、但您在第一个字段中输入了DNS名称、请将此名称复制到此处。
5. 单击 * 完成 *。

此时、CSR文件将下载到本地系统。下载内容的文件夹位置取决于您的浏览器。

6. 将CSR文件提交到CA并请求PEM或DER格式的签名证书。

完成后

等待CA返回证书文件、然后转到 ["第2步：导入管理证书"](#)。

第2步：导入管理证书

收到签名证书后、导入安装了Unified Manager界面的主机系统的证书链。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 您已生成证书签名请求(.csr文件)并将其发送到CA。
- CA返回了可信证书文件。
- 证书文件安装在本地系统上。
- 如果CA提供了链式证书(例如.p7b文件)、则必须将链式文件解压缩到各个文件中：根证书、一个或多个中间证书以及服务器证书。您可以使用Windows `certmgr`实用程序解压缩文件(右键单击并选择*菜单：所有任务[导出]*)。导出完成后、系统将为链中的每个证书文件显示一个CER"文件。

步骤

1. 选择*证书管理*。
2. 从*管理*选项卡中、选择*导入*。

此时将打开一个对话框、用于导入证书文件。

3. 单击*浏览*以首先选择根文件和中间文件、然后选择服务器证书。

文件名将显示在对话框中。

4. 单击 * 导入 *。

结果

这些文件将上传并进行验证。证书信息将显示在证书管理页面上。

重置管理证书

您可以将管理证书还原到原始出厂自签名状态。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

此任务将从安装了Web服务代理和SANtricity 统一管理器的主机系统中删除当前管理证书。重置证书后、主机系统将恢复为使用自签名证书。

步骤

1. 选择*证书管理*。
2. 从*管理*选项卡中、选择*重置*。

此时将打开一个*确认重置管理证书*对话框。

3. 在字段中键入`reset`、然后单击*重置*。

浏览器刷新后、浏览器可能会阻止对目标站点的访问并报告此站点正在使用HTTP严格传输安全性。切换回自签名证书时会出现此情况。要清除阻止访问目标的条件、您必须从浏览器中清除浏览数据。

结果

系统将恢复为使用服务器中的自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

导入阵列的证书

如有必要、您可以导入存储阵列的证书、以便这些证书可以在托管SANtricity Unified Manager的系统中进行身份验证。证书可以由证书颁发机构(CA)签名、也可以是自签名证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 如果要导入可信证书、则必须使用SANtricity 系统管理器为存储阵列控制器导入这些证书。

步骤

1. 选择*证书管理*。
2. 选择*可信*选项卡。

此页面显示为存储阵列报告的所有证书。

3. 选择*菜单：导入[证书]*以导入CA证书、或者选择*菜单：导入[自签名存储阵列证书]*以导入自签名证书。

要限制此视图、您可以使用*显示证书...*筛选字段、也可以单击列标题之一对证书行进行排序。

4. 在对话框中、选择证书、然后单击*导入*。

已上传并验证此证书。

查看证书

您可以查看证书的摘要信息、其中包括使用证书的组织、颁发证书的机构、有效期以及指纹(唯一标识符)。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

步骤

1. 选择*证书管理*。
2. 选择以下选项卡之一：
 - 管理-显示托管Web服务代理的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问Unified Manager。
 - 可信-显示Unified Manager可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。
3. 要查看有关证书的详细信息、请选择其行、选择行末尾的省略号、然后单击*查看*或*导出*。

导出证书

您可以导出证书以查看其完整详细信息。

开始之前

要打开导出的文件、您必须具有证书查看器应用程序。

步骤

1. 选择*证书管理*。
2. 选择以下选项卡之一：
 - 管理-显示托管Web服务代理的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问Unified Manager。
 - 可信-显示Unified Manager可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。
3. 从页面中选择一个证书、然后单击行末尾的省略号。
4. 单击*导出*、然后保存证书文件。
5. 在证书查看器应用程序中打开文件。

删除可信证书

您可以删除一个或多个不再需要的证书、例如已过期的证书。

开始之前

请先导入新证书、然后再删除旧证书。



请注意、删除根证书或中间证书可能会影响多个存储阵列、因为这些阵列可以共享相同的证书文件。

步骤

1. 选择*证书管理*。
2. 选择*可信*选项卡。
3. 在表中选择一个或多个证书、然后单击*删除*。



对于预安装的证书、*删除*功能不可用。

此时将打开确认删除可信证书对话框。

4. 确认删除、然后单击*删除*。

此证书将从表中删除。

解析不可信的证书

如果存储阵列尝试建立与SANtricity Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。在证书页面中、您可以通过从存储阵列导入自签名证书或导入可信第三方颁发的证书颁发机构(CA)证书来解析不可信的证书。

开始之前

- 您必须使用具有安全管理员权限的用户配置文件登录。
- 如果您计划导入CA签名的证书：
 - 您已为存储阵列中的每个控制器生成证书签名请求(.csr文件)、并将其发送给CA。
 - CA返回了可信证书文件。
 - 证书文件可在本地系统上使用。

关于此任务

如果满足以下任一条件、您可能需要安装其他受信任的CA证书：

- 您最近添加了一个存储阵列。
- 一个或两个证书均已过期。
- 一个或两个证书均已撤销。
- 一个或两个证书缺少根证书或中间证书。

步骤

1. 选择*证书管理*。
2. 选择*可信*选项卡。

此页面显示为存储阵列报告的所有证书。

3. 选择*菜单：导入[证书]*。导入CA证书或*菜单：导入[自签名存储阵列证书]*以导入自签名证书。

要限制此视图、您可以使用*显示证书...*筛选字段、也可以单击列标题之一对证书行进行排序。

4. 在对话框中、选择证书、然后单击*导入*。

已上传并验证此证书。

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。