使用证书
SANtricity 11.7

NetApp
February 12, 2024

目录

使用证书

对控制器使用CA签名的证书

您可以获取CA签名的证书、以便在控制器与用于访问System Manager的浏览器之间进行安全通信。

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。
- 您必须知道每个控制器的IP地址或DNS名称。

关于此任务

使用CA签名证书是一个三步操作步骤。

第1步：完成控制器的CSR

您必须先为存储阵列中的每个控制器生成证书签名请求(CSR)文件。

关于此任务

此任务介绍如何从System Manager生成CSR文件。CSR可提供有关您的组织的信息、以及控制器的IP地址或DNS名称。在此任务期间、如果存储阵列具有一个控制器、则会生成一个CSR文件；如果存储阵列具有两个控制器、则会生成两个CSR文件。

或者、您也可以使用OpenSSL等工具生成CSR文件、并可跳至 第2步：提交CSR文件。

步骤

1. 选择菜单：设置[证书]。
2. 从阵列管理选项卡中、选择*完成CSR*。

   如果显示一个对话框、提示您接受第二个控制器的自签名证书、请单击*接受自签名证书*以继续。

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—存储阵列或业务所在的城市。
   - 省/自治区/直辖市(可选)—存储阵列或业务所在的省/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。

   某些字段可能会预先填充相应的信息、例如控制器的IP地址。请勿更改预先填充的值、除非您确定这些值不正确。例如、如果尚未完成CSR、则控制器IP地址将设置为"`localhost.`"。在这种情况下、您必须将"`localhost`"更改为控制器的DNS名称或IP地址。

4. 验证或输入有关存储阵列中控制器A的以下信息：

   - 控制器**A**公用名-默认情况下、显示控制器A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内容完全匹配、才能访问System Manager。DNS名称不能以通配符开头。
   - 控制器**A**备用**IP**地址-如果公用名称为IP地址、则可以选择为控制器A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。
   - 控制器**A**备用**DNS**名称-如果公用名是DNS名称、请为控制器A输入任何其他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。DNS名称不能以通配符开头。 如果存储阵列只有一个控制器、则可以使用*完成*按钮。

     如果存储阵列有两个控制器、则可以使用*下一步*按钮。

   首次创建CSR请求时、请勿单击*跳过此步骤*链接。在错误恢复情况下提供此链接。在极少数情况下、一个控制器上的CSR请求可能会失败、而另一个控制器上的CSR请求则可能不会失败。通过此链接、您可以跳过在已定义的控制器A上创建CSR请求的步骤、并继续执行在控制器B上重新创建CSR请求的下一步

5. 如果只有一个控制器、请单击*完成*。如果有两个控制器、请单击*下一步*以输入控制器B的信息(与上述相同)、然后单击*完成*。

   对于单个控制器、会将一个CSR文件下载到本地系统。对于双控制器、将下载两个CSR文件。下载内容的文件夹位置取决于您的浏览器。

6. 转至 第2步：提交CSR文件。

第2步：提交CSR文件

创建证书签名请求(CSR)文件后、请将这些文件发送到证书颁发机构(CA)。E系列系统要求对签名证书使用PEM格式(Base64 ASCII编码)、其中包括以下文件类型：PEM、.crt、.cer或.key。

步骤

1. 找到已下载的CSR文件。
2. 将CSR文件提交到CA (例如VeriSign或DigiCert)、并请求PEM格式的签名证书。

   *将CSR文件提交给CA后、请勿重新生成另一个CSR文件。*每当生成CSR时、系统都会创建一个专用和公有 密钥对。公有 密钥是CSR的一部分、而私钥则保留在系统的密钥库中。当您收到签名证书并将其导入时、系统会确保私钥和公有 密钥都是原始对。如果密钥不匹配、则签名证书将不起作用、您必须从CA请求新证书。

3. 当CA返回签名证书时、转到 [第3步：导入控制器的签名证书]。

第3步：导入控制器的签名证书

从证书颁发机构(CA)收到签名证书后、导入控制器的文件。

开始之前

- CA返回签名证书文件。这些文件包括根证书、一个或多个中间证书以及服务器证书。
- 如果CA提供了一个链式证书文件(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

多个中间证书以及用于标识控制器的服务器证书。您可以使用Windows `certmgr` 用于解压缩文件的实用程序(右键单击并选择菜单：所有任务[导出])。建议使用64位编码。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。

- 您已将证书文件复制到访问System Manager的主机系统。

步骤

1. 选择菜单：设置[证书]
2. 从阵列管理选项卡中、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*按钮、首先选择根证书和中间证书文件、然后选择控制器的每个服务器证书。两个控制器的根文件和中间文件相同。对于每个控制器、只有服务器证书是唯一的。如果从外部工具生成CSR、则还必须导入随CSR一起创建的私钥文件。

   文件名将显示在对话框中。

4. 单击 * 导入 * 。

   这些文件将上传并进行验证。

结果

会话将自动终止。要使证书生效、您必须重新登录。重新登录后、新的CA签名证书将用于会话。

重置管理证书

您可以将控制器上的证书从使用CA签名证书还原到出厂设置的自签名证书。

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。
- 必须事先导入CA签名的证书。

关于此任务

重置功能会从每个控制器中删除当前CA签名的证书文件。然后、这些控制器将还原为使用自签名证书。

步骤

1. 选择菜单：设置[证书]。
2. 从阵列管理选项卡中、选择*重置*。

   此时将打开确认重置管理证书对话框。

3. Type `reset` 在字段中，然后单击*Reset (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

控制器将还原为使用自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

查看导入的证书信息

在证书页面中、您可以查看存储阵列的证书类型、颁发机构和有效日期范围。

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. 选择菜单：设置[证书]。
2. 选择一个选项卡以查看有关证书的信息。

选项卡	**Description**
阵列管理	查看有关为每个控制器导入的CA签名证书的信息、包括根文件、中间文件和服务器文件。
值得信赖	查看有关为控制器导入的所有其他类型证书的信息。 使用*显示证书…*下的筛选器字段可查看用户安装或预安装的证书。 • 用户安装—用户上传到存储阵列的证书、如果控制器充当客户端(而不是服务器)、LDAPS证书和身份联合证书、则这些证书可能包括可信证书。 • 预安装—存储阵列附带的自签名证书。
密钥管理	查看有关为外部密钥管理服务器导入的CA签名证书的信息。

作为客户端时导入控制器的证书

如果控制器因无法验证网络服务器的信任链而拒绝连接、您可以从"可信"选项卡导入证书、以使控制器(充当客户端)能够接受来自该服务器的通信。

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。
- 证书文件安装在本地系统上。

关于此任务

如果要允许其他服务器(例如使用TLS的LDAP服务器或系统日志服务器)与控制器联系、则可能需要从"受信任"选项卡导入证书。

步骤

1. 选择菜单：设置[证书]。
2. 从可信选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入可信证书文件。

3. 单击*浏览*以选择控制器的证书文件。

   文件名显示在对话框中。

4. 单击 * 导入 * 。

结果

这些文件将上传并进行验证。

启用证书撤消检查

您可以启用对已撤销证书的自动检查、以便联机证书状态协议(OCSP)服务器阻止用户进行非安全连接。

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。
- 在两个控制器上都配置了DNS服务器、这样可以为OCSP服务器使用完全限定域名。此任务可从硬件页面访问。
- 如果要指定自己的OCSP服务器、则必须知道该服务器的URL。

关于此任务

如果CA颁发的证书不正确或私钥受到损坏、则自动撤消检查非常有用。

在此任务期间、您可以配置OCSP服务器或使用证书文件中指定的服务器。OCSP服务器会确定CA是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问站点。

步骤

1. 选择菜单：设置[证书]。
2. 选择*可信*选项卡。

   您还可以从*密钥管理*选项卡启用撤消检查。

3. 单击*不常见任务*、然后从下拉菜单中选择*启用撤消检查*。
4. 选择*我要启用撤消检查*、以便复选框中显示复选标记、对话框中显示其他字段。
5. 在* OCSP响应器地址*字段中、您可以选择输入OCSP响应器服务器的URL。如果不输入地址、系统将使用证书文件中的OCSP服务器URL。
6. 单击*测试地址*以确保系统可以打开与指定URL的连接。
7. 单击 * 保存 * 。

结果

如果存储阵列尝试使用已撤销的证书连接到服务器、则连接将被拒绝并记录事件。

删除可信证书

您可以从"受信任"选项卡中删除先前导入的用户安装的证书。

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。
- 如果要使用新版本更新受信任证书、则必须先导入更新后的证书、然后才能删除旧证书。

> 如果在导入替代证书之前删除用于对控制器和其他服务器(例如LDAP服务器)进行身份验证的证书、则可能无法访问系统。

关于此任务

此任务介绍如何删除用户安装的证书。无法删除预安装的自签名证书。

步骤

1. 选择菜单：设置[证书]。
2. 选择*可信*选项卡。

   此表显示了存储阵列的受信任证书。
3. 从表中、选择要删除的证书。
4. 单击菜单：uncommon Tasks[Delete]。

   此时将打开确认删除可信证书对话框。
5. Type `delete` 在字段中，然后单击*Delete*。

使用CA签名的证书通过密钥管理服务器进行身份验证

要在密钥管理服务器和存储阵列控制器之间实现安全通信、您必须配置相应的证书集。

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

在控制器和密钥管理服务器之间进行身份验证是一个两步操作步骤。

第1步：完成并提交CSR、以便使用密钥管理服务器进行身份验证

您必须先生成证书签名请求(CSR)文件、然后使用CSR从密钥管理服务器信任的证书颁发机构(CA)请求签名客户端证书。您还可以使用下载的CSR文件从密钥管理服务器创建和下载客户端证书。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。

步骤

1. 选择菜单：设置[证书]。
2. 从密钥管理选项卡中、选择*完成CSR*。
3. 输入以下信息：

- 公用名—用于标识此CSR的名称、例如存储阵列名称、该名称将显示在证书文件中。
- 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-组织所在的城市或位置。
- 省/自治区/直辖市(可选)—组织所在的省/自治区/直辖市。
- 国家/地区**ISO**代码—贵组织所在的两位数ISO (国际标准化组织)代码、例如美国。

4. 单击 * 下载 * 。

   此时、CSR文件将保存到本地系统。

5. 从密钥管理服务器信任的CA请求签名客户端证书。
6. 拥有客户端证书后、请转到 [第2步：导入密钥管理服务器的证书]。

第2步：导入密钥管理服务器的证书

下一步是、在存储阵列和密钥管理服务器之间导入用于身份验证的证书。证书有两种类型：客户端证书用于验证存储阵列的控制器、而密钥管理服务器证书用于验证服务器。您必须加载控制器的客户端证书文件和密钥管理服务器的服务器证书文件。

开始之前

- 您有一个签名的客户端证书文件(请参见 第1步：完成并提交CSR、以便使用密钥管理服务器进行身份验证)、并且您已将该文件复制到要访问System Manager的主机。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。
- 您必须从密钥管理服务器检索证书文件、然后将该文件复制到要访问System Manager的主机。密钥管理服务器证书用于验证密钥管理服务器、以便存储阵列可以信任其IP地址。您可以对密钥管理服务器使用根证书、中间证书或服务器证书。

> 有关服务器证书的详细信息、请参见密钥管理服务器的文档。

步骤

1. 选择菜单：设置[证书]。
2. 从密钥管理选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入证书文件。

3. 在*选择客户端证书*旁边、单击*浏览*按钮为存储阵列的控制器选择客户端证书文件。

   此时、文件名将显示在对话框中。

4. 在*选择密钥管理服务器的服务器证书*旁边、单击*浏览*按钮为密钥管理服务器选择服务器证书文件。您可以为密钥管理服务器选择根证书、中间证书或服务器证书。

   此时、文件名将显示在对话框中。

5. 单击 * 导入 * 。

这些文件将上传并进行验证。

导出密钥管理服务器证书

您可以将密钥管理服务器的证书保存到本地计算机。

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。
- 必须事先导入证书。

步骤

1. 选择菜单：设置[证书]。
2. 选择*密钥管理*选项卡。
3. 从表中、选择要导出的证书、然后单击*导出*。

   此时将打开保存对话框。

4. 输入文件名并单击*保存*。