



## 证书 SANtricity 11.6

NetApp  
February 12, 2024

# 目录

- 证书 ..... 1
  - 概念 ..... 1
  - 操作说明..... 3
  - 常见问题解答 ..... 10

# 证书

## 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。

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System Manager、您可以管理主机管理系统(充当客户端)上的浏览器与存储系统中的控制器(充当服务器)之间的证书。

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

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：

- root—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。
- intermediate—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。但是、自签名证书与CA签名证书使用的信任链不同。

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。

用于密钥管理服务器的证书

如果您使用的是具有驱动器安全功能的外部密钥管理服务器、则还可以管理用于在该服务器和控制器之间进行身份验证的证书。

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端之间建立安全连接。
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。
客户端证书	对于安全密钥管理、客户端证书会验证存储阵列的控制器、以便密钥管理服务器可以信任其IP地址。
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。
密钥管理服务器证书	对于安全密钥管理、密钥管理服务器证书会对服务器进行验证、以便存储阵列可以信任其IP地址。
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。
OCSP服务器	联机证书状态协议(OCSP)服务器可确定证书颁发机构(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服务器。
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。

## 操作说明

### 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。

关于此任务

使用CA签名证书是一个三步操作步骤。

#### 第1步：完成并提交控制器的**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、然后将此文件提交给证书颁发机构(CA)。

开始之前

- 您必须知道每个控制器的IP地址或DNS名称。

关于此任务

CSR可提供有关您的组织、控制器的IP地址或DNS名称以及用于标识控制器中Web服务器的密钥对的信息。在此任务期间、如果存储阵列中只有一个控制器、则会生成一个CSR文件；如果有两个控制器、则会生成两个CSR文件。



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\*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。
- 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。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. 找到已下载的CSR文件。文件夹位置取决于您的浏览器。
7. 将CSR文件提交到CA并请求PEM格式的签名证书。
8. 等待CA返回证书、然后转到 [\[第2步：导入控制器的签名证书\]](#)。

## 第2步：导入控制器的签名证书

收到签名证书后、您可以导入控制器的文件。

### 开始之前

- CA返回签名证书文件。
- 这些文件位于本地系统上。
- 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用于标识控制器的服务器证书。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。

#### 关于此任务

此任务介绍如何上传证书文件。

#### 步骤

1. 选择\*菜单：设置[证书]\*。
2. 从\*阵列管理\*选项卡中、选择\*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、首先选择根文件和中间文件、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。

文件名将显示在对话框中。

4. 单击 \* 导入 \*。

文件已上传并进行验证。

#### 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. 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

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。 <ul style="list-style-type: none"><li>• 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。</li><li>• 预安装。存储阵列附带的自签名证书。</li></ul>
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：不常见任务[删除]\*

此时将打开确认删除可信证书对话框。

5. 在字段中键入`delete`、然后单击\*删除\*。

### 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。

#### 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CSR文件、然后使用此文件从密钥管理服务器信任的CA请求签名客户端证书。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。在此任务期间、您必须提供有关您的组织的信息。

#### 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。

### 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服务器证书文件、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。



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。

### 关于此任务

此任务介绍如何在存储阵列控制器和密钥管理服务器之间上传用于身份验证的证书文件。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。

### 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。

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\*。

## 常见问题解答

为什么会显示"无法访问其他控制器"对话框？

在执行与CA证书相关的某些操作(例如、导入证书)时、您可能会看到一个对话框、提示您接受第二个控制器的自签名证书。

在具有两个控制器的存储阵列(双工配置)中、如果SANtricity 系统管理器无法与第二个控制器通信、或者您的浏览器在操作的某个时间点无法接受证书、则有时会显示此对话框。

如果此对话框打开、请单击\*接受自签名证书\*以继续。如果另一个对话框提示您输入密码、请输入用于访问System Manager的管理员密码。

如果此对话框再次出现、并且您无法完成证书任务、请尝试以下过程之一：

- 使用其他浏览器类型访问此控制器、接受证书并继续。
- 使用System Manager访问第二个控制器、接受自签名证书、然后返回到第一个控制器并继续。

如何知道需要将哪些证书上传到**System Manager**才能进行外部密钥管理？

对于外部密钥管理、您可以导入两种类型的证书、以便在存储阵列和密钥管理服务器之间

进行身份验证、从而使这两个实体可以相互信任。

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。要获取客户端证书、请使用System Manager为存储阵列完成CSR。然后、您可以将CSR上传到密钥管理服务器并从该服务器生成客户端证书。获得客户端证书后、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。从密钥管理服务器检索服务器证书文件、然后将该文件复制到要访问System Manager的主机。

关于证书撤消检查、我需要了解哪些信息？

使用System Manager、您可以使用联机证书状态协议(Online Certificate Status Protocol、OCSP)服务器来检查已撤销的证书、而不是上传证书撤消列表(Certificate Revocation List、CRL)。

已撤销的证书不应再受信任。证书可能会因多种原因而被撤销；例如、如果证书颁发机构(CA)颁发的证书不正确、私钥被泄露或标识的实体不符合策略要求。

在System Manager中与OCSP服务器建立连接后、存储阵列将在连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时执行撤消检查。存储阵列会尝试验证这些服务器的证书、以确保它们未被撤消。然后、服务器将为该证书返回"good"、"revoked"或"unknown"值。如果证书已撤销或阵列无法与OCSP服务器联系、则连接将被拒绝。



在System Manager或命令行界面(CLI)中指定OCSP响应程序地址会覆盖在证书文件中找到的OCSP地址。

将为哪些类型的服务器启用撤消检查？

每当存储阵列连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时、它都会执行撤消检查。

## 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。