配置安全密钥

SANtricity software

NetApp
March 27, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/e-series-santricity-117/sm-settings/create-internal-security-key.html on March 27, 2025. Always check docs.netapp.com for the latest.

目录

配置安全密钥 1
创建内部安全密钥 1
创建外部安全密钥 2

配置安全密钥

创建内部安全密钥

要使用驱动器安全功能、您可以创建一个内部安全密钥、该密钥由存储阵列中的控制器和支持安全功能的驱动器共享。内部密钥会保留在控制器的永久性内存上。

开始之前

- 存储阵列中必须安装支持安全功能的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
- 必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。

如果存储阵列中同时安装了FDE和FIPS驱动器、则它们将共享同一个安全密钥。

关于此任务

在此任务中、您可以定义要与内部安全密钥关联的标识符和密码短语。

驱动器安全密码短语与存储阵列的管理员密码无关。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*创建内部密钥*。

   如果尚未生成安全密钥、则会打开创建安全密钥对话框。

3. 在以下字段中输入信息：

   - 定义安全密钥标识符-您可以接受默认值(存储阵列名称和时间戳、此名称和时间戳由控制器固件生成)、也可以输入您自己的值。最多可以输入189个字母数字字符、不带空格、标点符号或符号。

     系统会自动生成附加到您输入的字符串两端的其他字符。生成的字符可确保标识符是唯一的。

   - 定义密码短语/重新输入密码短语-输入并确认密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
     - 大写字母(一个或多个)。请注意、密码短语区分大小写。
     - 一个数字(一个或多个)。
     - 非字母数字字符、例如！、*、@(一个或多个)。

     请务必记录您的条目以供日后使用。如果您需要从存储阵列移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

4. 单击 * 创建 * 。

安全密钥存储在控制器上的不可访问位置。除了实际密钥之外、还会从浏览器下载一个加密密钥文件。

下载文件的路径可能取决于浏览器的默认下载位置。

5. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

结果

现在、您可以创建启用了安全保护的卷组或池、也可以在现有卷组和池上启用安全性。

每当关闭驱动器电源然后再次打开时、所有启用了安全保护的驱动器都会更改为安全锁定状态。在这种状态下、只有在驱动器初始化期间控制器应用正确的安全密钥后、才能访问数据。如果有人以物理方式删除已锁定的驱动器并将其安装到其他系统中、则安全锁定状态将阻止对其数据进行未经授权的访问。

完成后

您应验证此安全密钥、以确保此密钥文件未损坏。

创建外部安全密钥

要对密钥管理服务器使用驱动器安全功能、必须创建一个外部密钥、该密钥由密钥管理服务器和存储阵列中支持安全功能的驱动器共享。

开始之前

- 阵列中必须安装支持安全功能的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。

  如果存储阵列中同时安装了FDE和FIPS驱动器、则它们将共享同一个安全密钥。

- 必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。
- 您已为存储阵列的控制器创建一个签名客户端证书文件、并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。

关于此任务

在此任务中、您可以定义密钥管理服务器的IP地址及其使用的端口号、然后加载用于外部密钥管理的证书。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*创建外部密钥*。

如果当前已配置内部密钥管理、则会打开一个对话框、要求您确认是否要切换到外部密钥管理。

此时将打开创建外部安全密钥对话框。

3. 在*连接到密钥服务器*下、在以下字段中输入信息。

   - 密钥管理服务器地址—输入用于密钥管理的服务器的完全限定域名或IP地址(IPv4或IPv6)。
   - 密钥管理端口号-输入用于KMIP通信的端口号。用于密钥管理服务器通信的最常见端口号是5696。

     可选：*如果要配置备份密钥服务器、请单击*添加密钥服务器、然后输入该服务器的信息。如果无法访问主密钥服务器、则会使用第二个密钥服务器。确保每个密钥服务器都可以访问同一个密钥数据库；否则、阵列将发布错误、并且无法使用备份服务器。

     一次仅使用一个密钥服务器。如果存储阵列无法访问主密钥服务器、则该阵列将联系备份密钥服务器。请注意、必须在两个服务器之间保持奇偶校验；否则可能会导致错误。

   - 选择客户端证书-单击第一个*浏览*按钮以选择存储阵列控制器的证书文件。
   - 选择密钥管理服务器的服务器证书-单击第二个*浏览*按钮以选择密钥管理服务器的证书文件。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。
4. 单击 * 下一步 * 。
5. 在*创建/备份密钥*下、您可以出于安全目的创建备份密钥。

   - (建议)要创建备份密钥、请保持选中状态、然后输入并确认密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
     - 大写字母(一个或多个)。请注意、密码短语区分大小写。
     - 一个数字(一个或多个)。
     - 非字母数字字符、例如！、*、@(一个或多个)。

     请务必记录您的条目以供日后使用。如果您需要从存储阵列中移动启用了安全保护的驱动器、则必须知道解锁驱动器数据的密码短语。

   +

   - 如果不想创建备份密钥、请取消选中此复选框。

     请注意、如果您无法访问外部密钥服务器、并且没有备份密钥、则在将驱动器迁移到另一存储阵列时、您将无法访问这些驱动器上的数据。此选项是在System Manager中创建备份密钥的唯一方法。
6. 单击 * 完成 * 。

   系统将使用您输入的凭据连接到密钥管理服务器。然后、安全密钥的副本将存储在本地系统上。

   下载文件的路径可能取决于浏览器的默认下载位置。
7. 记下您的密码短语以及下载的密钥文件的位置、然后单击*关闭*。

此页面将显示以下消息、其中包含用于外部密钥管理的其他链接：

```
Current key management method: External
```

8. 选择*测试通信*以测试存储阵列与密钥管理服务器之间的连接。

   测试结果将显示在对话框中。

结果

启用外部密钥管理后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

> 每当关闭驱动器电源然后再次打开时、所有启用了安全保护的驱动器都会更改为安全锁定状态。在这种状态下、只有在驱动器初始化期间控制器应用正确的安全密钥后、才能访问数据。如果有人以物理方式删除已锁定的驱动器并将其安装到其他系统中、则安全锁定状态将阻止对其数据进行未经授权的访问。

完成后

您应验证此安全密钥、以确保此密钥文件未损坏。

版权信息

版权所有 © 2025 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。