驱动器安全性
SANtricity 11.7

NetApp
February 12, 2024

目录

驱动器安全性

驱动器安全性概述

您可以从安全密钥管理页面配置驱动器安全性和密钥管理。

什么是驱动器安全性?

_Drive Security_是一项功能、可防止在从存储阵列中删除启用了安全功能的驱动器上的数据时未经授权进行访问。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。从阵列中物理删除FDE或FIPS驱动器后、这些驱动器将无法运行、除非将其安装在另一个阵列中、此时、这些驱动器将处于安全锁定状态、直到提供正确的安全密钥为止。安全密钥_是指此类驱动器与存储阵列中的控制器之间共享的字符串。

了解更多信息。

- "驱动器安全功能的工作原理"
- "安全密钥管理的工作原理"
- "驱动器安全术语"

如何配置密钥管理?

要实施驱动器安全性、阵列中必须安装FDE驱动器或FIPS驱动器。要为这些驱动器配置密钥管理、请转到菜单：设置[系统>安全密钥管理]、在此可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。最后、您可以通过在卷设置中选择"安全功能"来为池和卷组启用驱动器安全性。

了解更多信息。

- "创建内部安全密钥"
- "创建外部安全密钥"
- "手动创建池"
- "创建卷组"

如何解锁驱动器?

如果您配置了密钥管理、然后将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将安全密钥重新分配给新存储阵列、才能访问驱动器上的加密数据。

了解更多信息。

- "使用内部密钥管理时解锁驱动器"
- "使用外部密钥管理时解锁驱动器"

相关信息

详细了解与密钥管理相关的任务：

- "使用CA签名的证书通过密钥管理服务器进行身份验证"
- "备份安全密钥"

概念

驱动器安全功能的工作原理

驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS ）驱动器提供额外的安全层。

如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。

如何实施驱动器安全性

要实施驱动器安全性、请执行以下步骤。

1. 为存储阵列配备支持安全保护的驱动器、可以是FDE驱动器、也可以是FIPS驱动器。(对于需要FIPS支持的卷、请仅使用FIPS驱动器。在卷组或池中混用FIPS和FDE驱动器将导致所有驱动器被视为FDE驱动器。此外、FDE驱动器不能添加到纯FIPS卷组或池中或用作备用磁盘。)
2. 创建一个安全密钥、该密钥是一个字符串、由控制器和驱动器共享、用于进行读/写访问。您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。对于外部密钥管理、必须使用密钥管理服务器建立身份验证。
3. 为池和卷组启用驱动器安全性：
   - 创建池或卷组(在候选项表的*安全功能*列中查找*是*)。
   - 创建新卷时、请选择池或卷组(在Pool and volume group candidates表中、查找*安全功能*旁边的*是*)。

驱动器安全在驱动器级别的工作原理

支持安全的驱动器(FDE或FIPS)可在写入期间对数据进行加密、并在读取期间对数据进行解密。此加密和解密不会影响性能或用户工作流。每个驱动器都有自己唯一的加密密钥、永远不能从该驱动器传输该密钥。

驱动器安全功能可通过支持安全功能的驱动器提供额外的保护层。如果为驱动器安全选择了这些驱动器上的卷组或池、则这些驱动器会先查找安全密钥、然后再允许访问数据。您可以随时为池和卷组启用驱动器安全性、而不会影响驱动器上的现有数据。但是、如果不擦除驱动器上的所有数据、则无法禁用驱动器安全性。

驱动器安全性在存储阵列级别的工作原理

使用驱动器安全功能、您可以创建一个安全密钥、该安全密钥可在存储阵列中启用了安全保护的驱动器和控制器之间共享。无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。

如果从存储阵列中删除启用了安全保护的驱动器并将其重新安装在其他存储阵列中、则该驱动器将处于安全锁定状态。重新定位的驱动器会先查找安全密钥、然后再使数据可再次访问。要解锁数据、请应用源存储阵列中的安全密钥。成功解锁过程后、重新定位的驱动器将使用已存储在目标存储阵列中的安全密钥、并且不再需要导入的安全密钥文件。

对于内部密钥管理、实际安全密钥存储在控制器上不可访问的位置。它不是以人为可读的格式提供的、也不是用户可访问的格式。

驱动器安全在卷级别的工作原理

从支持安全的驱动器创建池或卷组时、您还可以为这些池或卷组启用驱动器安全性。"驱动器安全性"选项可确保驱动器以及关联的卷组和池的安全-*enabled*.

在创建启用了安全保护的卷组和池之前、请牢记以下准则：

- 卷组和池必须全部由具有安全功能的驱动器组成。(对于需要FIPS支持的卷、请仅使用FIPS驱动器。在卷组或池中混用FIPS和FDE驱动器将导致所有驱动器被视为FDE驱动器。此外、FDE驱动器不能添加到纯FIPS卷组或池中或用作备用磁盘。)
- 卷组和池必须处于最佳状态。

安全密钥管理的工作原理

在实施驱动器安全功能时、启用了安全保护的驱动器(FIPS或FDE)需要一个安全密钥才能进行数据访问。安全密钥是指这些类型的驱动器与存储阵列中的控制器之间共享的字符串。

无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。如果从存储阵列中删除启用了安全保护的驱动器、则该驱动器的数据将被锁定。在将驱动器重新安装到其他存储阵列中时、它会先查找安全密钥、然后再重新访问数据。要解锁数据、必须应用原始安全密钥。

您可以使用以下方法之一创建和管理安全密钥：

- 控制器永久性内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

内部密钥管理

在控制器永久性内存的不可访问位置维护内部密钥并"`hidden`"。要实施内部密钥管理、请执行以下步骤：

1. 在存储阵列中安装支持安全保护的驱动器。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。
2. 确保已启用驱动器安全功能。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。
3. 创建内部安全密钥、其中包括定义标识符和密码短语。标识符是与安全密钥关联的字符串、存储在控制器以及与该密钥关联的所有驱动器上。密码短语用于对安全密钥进行加密、以用于备份。要创建内部密钥、请转到菜单：设置[系统>安全密钥管理>创建内部密钥]。

安全密钥存储在控制器上的一个隐藏的不可访问位置。然后、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。

外部密钥管理

外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上进行维护。要实施外部密钥管理、请执行以下步骤：

1. 在存储阵列中安装支持安全保护的驱动器。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。
2. 确保已启用驱动器安全功能。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。
3. 获取签名的客户端证书文件。客户端证书用于验证存储阵列的控制器、以便密钥管理服务器可以信任其KMIP请求。
   a. 首先、您需要完成并下载客户端证书签名请求(CSR)。转到菜单：设置[证书>密钥管理>完成CSR]。
   b. 接下来、您需要从密钥管理服务器信任的CA请求签名客户端证书。(您也可以使用CSR文件从密钥管理服务器创建和下载客户端证书。)
   c. 拥有客户端证书文件后、将该文件复制到要访问System Manager的主机。
4. 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。
5. 创建外部密钥、其中包括定义密钥管理服务器的IP地址以及用于KMIP通信的端口号。在此过程中、您还可以加载证书文件。要创建外部密钥、请转到菜单：设置[系统>安全密钥管理>创建外部密钥]。

系统将使用您输入的凭据连接到密钥管理服务器。然后、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。

驱动器安全术语

了解驱动器安全术语如何应用于存储阵列。

期限	**Description**
驱动器安全功能	驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ，FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ，FIPS ）驱动器提供额外的安全层。如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。
FDE驱动器	全磁盘加密(Full Disk Encryption、FDE)驱动器在硬件级别对磁盘驱动器执行加密。硬盘驱动器包含一个ASIC芯片、用于在写入期间对数据进行加密、然后在读取期间对数据进行解密。
FIPS驱动器	FIPS驱动器使用联邦信息处理标准(FIPS) 140-2级别2。它们本质上是FDE驱动器、符合美国政府标准、可确保强大的加密算法和方法。FIPS驱动器的安全标准高于FDE驱动器。
管理客户端	一种本地系统(计算机、平板电脑等)、其中包括用于访问System Manager的浏览器。

期限	Description
密码短语	密码短语用于对安全密钥进行加密、以用于备份。在因驱动器迁移或机头交换而导入备份的安全密钥时、必须提供用于加密安全密钥的相同密码短语。密码短语可以包含8到32个字符。 驱动器安全密码短语与存储阵列的管理员密码无关。
支持安全的驱动器	支持安全的驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器、这些驱动器可在写入期间对数据进行加密、并在读取期间对数据进行解密。这些驱动器被视为安全驱动器-*capable"*、因为可以使用驱动器安全功能提高安全性。如果为这些驱动器使用的卷组和池启用了驱动器安全功能、则这些驱动器将变为*secure—_enabled*.
已启用安全保护的驱动器	启用了安全保护的驱动器与驱动器安全功能结合使用。启用驱动器安全功能后、如果将驱动器安全应用于安全-*capable"*驱动器上的池或卷组、则这些驱动器将变为安全-enabled__。只能通过配置了正确安全密钥的控制器进行读写访问。这种增强的安全性可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。
安全密钥	安全密钥是指在存储阵列中启用了安全保护的驱动器和控制器之间共享的字符串。无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。如果从存储阵列中删除启用了安全保护的驱动器、则该驱动器的数据将被锁定。在将驱动器重新安装到其他存储阵列中时、它会先查找安全密钥、然后再重新访问数据。要解锁数据、必须应用原始安全密钥。您可以使用以下方法之一创建和管理安全密钥： • 内部密钥管理—在控制器的永久性内存上创建和维护安全密钥。 • 外部密钥管理—在外部密钥管理服务器上创建和维护安全密钥。
安全密钥标识符	安全密钥标识符是在创建密钥期间与安全密钥关联的字符串。标识符存储在控制器以及与安全密钥关联的所有驱动器上。

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。

管理安全密钥

更改安全密钥

您可以随时将安全密钥替换为新密钥。如果您的公司存在潜在的安全违规行为、并且希望确保未经授权的人员无法访问驱动器数据、您可能需要更改安全密钥。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*更改密钥*。

   此时将打开更改安全密钥对话框。

3. 在以下字段中输入信息。
   - 定义安全密钥标识符-(仅适用于内部安全密钥。) 接受默认值(由控制器固件生成的存储阵列名称和时间戳)或输入您自己的值。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。

     系统会自动生成其他字符、并将其附加到您输入的字符串的两端。生成的字符有助于确保标识符是唯一的。

   - 定义密码短语/重新输入密码短语—在每个字段中输入您的密码短语。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)。
4. 对于外部安全密钥、如果要在创建新安全密钥时删除旧安全密钥、请选中对话框底部的"删除当前安全密钥…"复选框。

   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、则必须知道用于解锁驱动器数据的标识符和密码短语。

5. 单击 * 更改 * 。

   新的安全密钥会覆盖上一个密钥、而上一个密钥不再有效。

   下载文件的路径可能取决于浏览器的默认下载位置。

6. 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*。

完成后

您应验证此安全密钥、以确保此密钥文件未损坏。

从外部密钥管理切换到内部密钥管理

您可以将驱动器安全管理方法从外部密钥服务器更改为存储阵列使用的内部方法。然后、以前为外部密钥管理定义的安全密钥将用于内部密钥管理。

关于此任务

在此任务中、您可以禁用外部密钥管理并将新的备份副本下载到本地主机。现有密钥仍用于驱动器安全、但将在存储阵列中进行内部管理。

步骤

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

   此时将打开禁用外部密钥管理对话框。

3. 在*定义密码短语/重新输入密码短语*中、输入并确认用于备份密钥的密码短语。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 * 禁用 * 。

   备份密钥将下载到本地主机。

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、驱动器安全性可通过存储阵列在内部进行管理。

完成后

您应验证此安全密钥、以确保此密钥文件未损坏。

编辑密钥管理服务器设置

如果您配置了外部密钥管理、则可以随时查看和编辑密钥管理服务器设置。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*查看/编辑密钥管理服务器设置*。
3. 编辑以下字段中的信息：
   - 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-输入用于密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)通信的端口号。

     *可选：*您可以通过单击*添加密钥服务器*来包括另一个密钥服务器。
4. 单击 * 保存 * 。

备份安全密钥

创建或更改安全密钥后、您可以为密钥文件创建备份副本、以防其损坏。

关于此任务

此任务介绍如何备份先前创建的安全密钥。在此操作步骤 期间、您将为备份创建一个新的密码短语。此密码短语不需要与创建原始密钥或上次更改时使用的密码短语匹配。密码短语仅适用于您要创建的备份。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*备份密钥*。

   此时将打开备份安全密钥对话框。
3. 在*定义密码短语/重新输入密码短语*字段中、输入并确认此备份的密码短语。

   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)
   - 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。要访问此安全密钥的备份、您需要使用密码短语。
4. 单击*备份*。

   安全密钥的备份将下载到本地主机、然后打开*确认/记录安全密钥备份*对话框。

   下载的安全密钥文件的路径可能取决于浏览器的默认下载位置。
5. 在安全位置记下您的密码短语、然后单击*关闭*。

完成后

您应验证备份安全密钥。

验证安全密钥

您可以验证安全密钥、以确保其未损坏、并验证您是否具有正确的密码短语。

关于此任务

此任务介绍如何验证您先前创建的安全密钥。这是确保密钥文件未损坏且密码短语正确的重要步骤、它可确保在将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列后、您可以访问驱动器数据。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*验证密钥*。

   此时将打开验证安全密钥对话框。

3. 单击*Browse*，然后选择密钥文件(例如， `drivesecurity.slk`）。
4. 输入与选定密钥关联的密码短语。

   选择有效的密钥文件和密码短语后、*验证*按钮将变为可用。

5. 单击*验证*。

   验证结果将显示在对话框中。

6. 如果结果显示"The security key validated successfully"、请单击*关闭*。如果显示错误消息、请按照对话框中显示的建议说明进行操作。

使用内部密钥管理时解锁驱动器

如果您配置了内部密钥管理、然后将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将安全密钥重新分配给新存储阵列、才能访问驱动器上的加密数据。

开始之前

- 在源阵列(要删除驱动器的阵列)上、您已导出卷组并删除驱动器。在目标阵列上、您已重新安装驱动器。

  > System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

  有关迁移卷组的详细说明、请参见 "NetApp 知识库"。请务必按照适用于System Manager管理的较新阵列或旧系统的相应说明进行操作。

- 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。
- 您必须知道与要解锁的驱动器关联的安全密钥。
- 管理客户端(具有用于访问System Manager的浏览器的系统)上提供了安全密钥文件。如果要将驱动器移动到由其他系统管理的存储阵列、则需要将安全密钥文件移动到该管理客户端。

关于此任务

使用内部密钥管理时、安全密钥将存储在本地存储在存储阵列上。安全密钥是指控制器和驱动器共享的字符串、

用于进行读/写访问。如果从阵列中物理删除驱动器并将其安装在另一个阵列中、则这些驱动器将无法运行、除非您提供正确的安全密钥。

> 您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。本主题介绍使用_internal_密钥管理时解锁数据。如果您使用的是_external_密钥管理、请参见 "使用外部密钥管理时解锁驱动器"。如果要执行控制器升级并将所有控制器更换为最新硬件、则必须按照中E系列和SANtricity 文档中心所述的不同步骤进行操作 "解锁驱动器"。

在另一个阵列中重新安装启用了安全保护的驱动器后、该阵列将发现这些驱动器、并显示"需要注意"情况以及"需要安全密钥"状态。 要解锁驱动器数据、请选择安全密钥文件并输入密钥的密码短语。(此密码短语与存储阵列的管理员密码不同。)

如果新存储阵列中安装了其他启用了安全保护的驱动器、则这些驱动器使用的安全密钥可能与您要导入的安全密钥不同。在导入过程中、旧安全密钥仅用于解锁要安装的驱动器的数据。成功完成解锁过程后、新安装的驱动器将重新密钥到目标存储阵列的安全密钥。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*解锁安全驱动器*。

   此时将打开解除安全驱动器锁定对话框。表中显示了需要安全密钥的所有驱动器。
3. *可选：*将鼠标悬停在驱动器编号上可查看驱动器的位置(磁盘架编号和托架编号)。
4. 单击*浏览*、然后选择与要解锁的驱动器对应的安全密钥文件。

   您选择的密钥文件将显示在对话框中。
5. 输入与此密钥文件关联的密码短语。

   输入的字符将被屏蔽。
6. 单击*解锁*。

   如果解锁操作成功、则对话框将显示："The associated secure drives have been unlocked"。

结果

锁定并解除锁定所有驱动器后、存储阵列中的每个控制器都将重新启动。但是、如果目标存储阵列中已有一些未锁定的驱动器、则控制器不会重新启动。

完成后

在目标阵列(包含新安装驱动器的阵列)上、您现在可以导入卷组。

> System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

有关迁移卷组的详细说明、请参见 "NetApp 知识库"。

使用外部密钥管理时解锁驱动器

如果您配置了外部密钥管理、然后将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将安全密钥重新分配给新存储阵列、才能访问驱动器上的加密数据。

开始之前

- 在源阵列(要删除驱动器的阵列)上、您已导出卷组并删除驱动器。在目标阵列上、您已重新安装驱动器。

> System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

有关迁移卷组的详细说明、请参见 "NetApp 知识库"。请务必按照适用于System Manager管理的较新阵列或旧系统的相应说明进行操作。

- 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。
- 您必须知道密钥管理服务器的IP地址和端口号。
- 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

使用外部密钥管理时、安全密钥会存储在外部的服务器上、用于保护安全密钥。安全密钥是指控制器和驱动器共享的字符串、用于进行读/写访问。如果从阵列中物理删除驱动器并将其安装在另一个阵列中、则这些驱动器将无法运行、除非您提供正确的安全密钥。

> 您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。本主题介绍使用_external_密钥管理时解锁数据。如果您使用_internal_密钥管理、请参见 "使用内部密钥管理时解锁驱动器"。如果要执行控制器升级并将所有控制器更换为最新硬件、则必须按照中E系列和SANtricity 文档中心所述的不同步骤进行操作 "解锁驱动器"。

在另一个阵列中重新安装启用了安全保护的驱动器后、该阵列将发现这些驱动器、并显示"需要注意"情况以及"需要安全密钥"状态。 要解锁驱动器数据、请导入安全密钥文件并输入密钥的密码短语。(此密码短语与存储阵列的管理员密码不同。) 在此过程中、您可以将存储阵列配置为使用外部密钥管理服务器、然后便可访问安全密钥。您需要提供存储阵列连接和检索安全密钥所需的服务器联系信息。

如果新存储阵列中安装了其他启用了安全保护的驱动器、则这些驱动器使用的安全密钥可能与您要导入的安全密钥不同。在导入过程中、旧安全密钥仅用于解锁要安装的驱动器的数据。成功完成解锁过程后、新安装的驱动器将重新密钥到目标存储阵列的安全密钥。

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*。

3. 使用前提条件连接信息和证书完成向导。
4. 单击*测试通信*以确保能够访问外部密钥管理服务器。
5. 选择*解锁安全驱动器*。

   此时将打开解除安全驱动器锁定对话框。表中显示了需要安全密钥的所有驱动器。

6. *可选：*将鼠标悬停在驱动器编号上可查看驱动器的位置(磁盘架编号和托架编号)。
7. 单击*浏览*、然后选择与要解锁的驱动器对应的安全密钥文件。

   您选择的密钥文件将显示在对话框中。

8. 输入与此密钥文件关联的密码短语。

   输入的字符将被屏蔽。

9. 单击*解锁*。

   如果解锁操作成功、则对话框将显示："The associated secure drives have been unlocked"。

结果

锁定并解除锁定所有驱动器后、存储阵列中的每个控制器都将重新启动。但是、如果目标存储阵列中已有一些未锁定的驱动器、则控制器不会重新启动。

完成后

在目标阵列(包含新安装驱动器的阵列)上、您现在可以导入卷组。

> System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

有关迁移卷组的详细说明、请参见 "NetApp 知识库"。

常见问题解答

在创建安全密钥之前、我需要了解哪些信息？

安全密钥由存储阵列中的控制器和启用了安全保护的驱动器共享。如果从存储阵列中删除了启用了安全保护的驱动器、则安全密钥可防止数据遭受未经授权的访问。

您可以使用以下方法之一创建和管理安全密钥：

- 控制器永久性内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

内部密钥管理

在控制器永久性内存的不可访问位置维护内部密钥并"`hidden`"。在创建内部安全密钥之前、必须执行以下操作：

1. 在存储阵列中安装支持安全保护的驱动器。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。
2. 确保已启用驱动器安全功能。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。

然后、您可以创建内部安全密钥、其中包括定义标识符和密码短语。标识符是与安全密钥关联的字符串、存储在控制器以及与该密钥关联的所有驱动器上。密码短语用于对安全密钥进行加密、以用于备份。完成后、安全密钥将存储在控制器上不可访问的位置。然后、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。

外部密钥管理

外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上进行维护。在创建外部安全密钥之前、必须执行以下操作：

1. 在存储阵列中安装支持安全保护的驱动器。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。
2. 确保已启用驱动器安全功能。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。
3. 获取签名的客户端证书文件。客户端证书用于验证存储阵列的控制器、以便密钥管理服务器可以信任其KMIP请求。
    a. 首先、您需要完成并下载客户端证书签名请求(CSR)。转到菜单：设置[证书>密钥管理>完成CSR]。
    b. 接下来、您需要从密钥管理服务器信任的CA请求签名客户端证书。(您也可以使用下载的CSR文件从密钥管理服务器创建和下载客户端证书。)
    c. 拥有客户端证书文件后、将该文件复制到要访问System Manager的主机。
4. 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。

然后、您可以创建外部密钥、其中包括定义密钥管理服务器的IP地址以及用于KMIP通信的端口号。在此过程中、您还可以加载证书文件。完成后、系统将使用您输入的凭据连接到密钥管理服务器。然后、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。

为什么需要定义密码短语?

密码短语用于对存储在本地管理客户端上的安全密钥文件进行加密和解密。如果没有密码短语、则无法对安全密钥进行解密、并使用此安全密钥从启用了安全功能的驱动器中解锁数据、如果此驱动器重新安装在另一个存储阵列中。

为什么记录安全密钥信息很重要?

如果丢失安全密钥信息并且没有备份、则在重新定位启用了安全保护的驱动器或升级控制器时可能会丢失数据。您需要使用安全密钥来解锁驱动器上的数据。

请务必记录安全密钥标识符、关联的密码短语以及安全密钥文件保存在本地主机上的位置。

备份安全密钥前需要了解哪些信息?

如果原始安全密钥损坏、并且您没有备份、则在驱动器从一个存储阵列迁移到另一个存储

阵列时、您将无法访问这些驱动器上的数据。

备份安全密钥之前、请记住以下准则：

- 确保您知道原始密钥文件的安全密钥标识符和密码短语。

> 只有内部密钥使用标识符。创建标识符时、系统会自动生成其他字符并将其附加到标识符字符串的两端。生成的字符可确保标识符是唯一的。

- 您可以为备份创建新的密码短语。此密码短语不需要与创建原始密钥或上次更改时使用的密码短语匹配。密码短语仅适用于您要创建的备份。

> 驱动器安全密码短语不应与存储阵列的管理员密码相混淆。Drive Security的密码短语用于保护安全密钥的备份。管理员密码可保护整个存储阵列、防止未经授权的访问。

- 备份安全密钥文件将下载到管理客户端。下载文件的路径可能取决于浏览器的默认下载位置。请务必记录安全密钥信息的存储位置。

在解除安全驱动器锁定之前、我需要了解哪些信息？

要从启用了安全的驱动器解锁数据、必须导入其安全密钥。

在解除锁定启用了安全保护的驱动器之前、请记住以下准则：

- 存储阵列必须已具有安全密钥。迁移的驱动器将重新密钥设置到目标存储阵列。
- 对于要迁移的驱动器、您必须知道安全密钥标识符以及与安全密钥文件对应的密码短语。
- 管理客户端(具有用于访问System Manager的浏览器的系统)上必须具有安全密钥文件。
- 如果要重置锁定的NVMe驱动器、必须输入驱动器的安全ID。要找到安全ID、您必须物理移除驱动器、并在驱动器标签上找到PSID字符串(最多32个字符)。在开始操作之前、请确保已重新安装驱动器。

什么是读/写可访问性？

驱动器设置窗口包含有关驱动器安全属性的信息。"读/写可访问"是驱动器数据已锁定时显示的属性之一。

要查看驱动器安全属性、请转到硬件页面。选择一个驱动器、单击*查看设置*、然后单击*显示更多设置*。如果驱动器已解锁、则页面底部的读/写可访问属性值为*是*。驱动器锁定时、读/写可访问属性值为*否、安全密钥无效*。您可以通过导入安全密钥来解锁安全驱动器(转到菜单：设置(系统>解锁安全驱动器)。

验证安全密钥时需要了解哪些信息？

创建安全密钥后、您应验证密钥文件以确保其未损坏。

如果验证失败、请执行以下操作：

- 如果安全密钥标识符与控制器上的标识符不匹配、请找到正确的安全密钥文件、然后重试验证。
- 如果控制器无法对安全密钥进行解密以进行验证、则您输入的密码短语可能不正确。仔细检查密码短语、必要时重新输入、然后重试验证。如果此错误消息再次出现、请选择密钥文件的备份(如果可用)、然后重试验

证。

- 如果仍然无法验证安全密钥、则原始文件可能已损坏。创建密钥的新备份并验证该副本。

内部安全密钥与外部安全密钥管理有何区别?

在实施驱动器安全功能时、当从存储阵列中删除启用了安全保护的驱动器时、您可以使用内部安全密钥或外部安全密钥锁定数据。

安全密钥是一个字符串、在存储阵列中启用了安全保护的驱动器和控制器之间共享。内部密钥会保留在控制器的永久性内存上。外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上进行维护。