管理安全密钥

SANtricity 11.8

NetApp
December 16, 2024

目录

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(存储阵列名称和时间戳、由控制器固件生成)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。如果使用了_External密钥管理，请参见"使用外部密钥管理时解锁驱动器"。如果您要执行控制器升级并将所有控制器更换为最新硬件，则必须按照中的E系列和SANtricity文档中心所述执行不同的步骤"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"需要引起注意"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。如果使用了_INTERNAL_密钥管理，请参见"使用内部密钥管理时解锁驱动器"。如果您要执行控制器升级并将所有控制器更换为最新硬件，则必须按照中的E系列和SANtricity文档中心所述执行不同的步骤"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"需要引起注意"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、您需要将存储阵列配置为使用外部密钥管理服务器、然后才能访问此安全密钥。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"。