Dell EMC PowerStore
安全配置指南

1.x

July 2020
Rev. A02

注意、小心和警告

注： “注意”表示帮助您更好地使用该产品的重要信息。

小心： **“小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。**

警告： **“警告”表示可能会导致财产损失、人身伤害甚至死亡。**

目录

序言

为了不断改进，我们将定期发布软件和硬件产品的修订版。本文档中介绍的一些功能可能不被当前使用的软件或硬件的所有版本支持。本产品发行说明提供了有关产品功能的新信息。如果某产品不能正常运行或其功能与本文档的描述不符，请与您的技术支持专业人员联系。

从何处获得帮助

可以按如下方式获取支持、产品和许可信息：

- **产品信息**

  有关产品和功能的文档或发行说明，请访问 PowerStore 文档页面，地址为 www.dell.com/powerstoredocs。

- **故障排除**

  有关产品、软件更新、许可和服务的信息，请转到 www.dell.com/support，并找到相应的产品支持页面。

- **技术支持**

  如需技术支持，如有服务请求，请转至 www.dell.com/support 并找到 **Service Requests** 页面。要提交服务请求，您必须具有有效的支持协议。请联系销售代表，以了解有关获取有效的支持协议的详细信息，或者回答有关您的帐户的任何问题。

1

身份验证和访问

本章包含以下信息：

主题：

验证和管理用户帐户、角色和权限

对群集的访问是基于用户帐户的凭据执行身份验证的。用户帐户的创建和随后的管理是通过 **Users** 页面进行的，在 PowerStore Manager 中通过 **Settings** > **Users** > **Users** 可查看此页面。适用的授权取决于与用户帐户相关联的角色。当在 Web 浏览器中指定群集的网络地址作为 URL 时，用户将看到登录页，在该页面中，用户能以本地用户身份进行身份验证。系统将对用户提供的凭据进行身份验证，而且将在系统上创建一个会话。随后，用户可在为其分配的角色的能力范围内监视和管理群集。

群集通过与管理服务器的安全连接来验证用户名和密码，从而对用户进行身份验证。

出厂默认管理

设备附带了出厂默认用户帐户设置，用于进行设备的初始访问和配置。

注: 对于 1.0.x 版，建议使用 PowerStore Manager UI（而不是使用 API、CLI 或服务脚本界面）对 PowerStore 进行初始配置。这将确保更改所有默认密码。

帐户类型	用户名	密码	权限
系统管理	admin	Password123#	用于重置默认密码、配置设备设置和管理用户帐户的管理员权限。
服务	service	service	可执行服务操作。 **注:** 服务用户可执行安全外壳 (SSH) 访问。但是，您不可以使用服务用户登录 PowerStore Manager。

会话规则

群集中的会话具有以下特点：

- 一小时有效期。

注: 会话处于非活动状态达一小时后，用户将自动从群集中注销。

- 会话超时不可配置。

用户名和密码的使用

系统帐户用户名必须符合以下要求：

限制	用户名要求
结构	必须以字母数字字符开头和结尾。
情形	所有用户名都不区分大小写
最少字母数字字符数	1
最多字母数字字符数	64
支持的特殊字符	.（点）

系统帐户密码必须满足以下要求：

限制	密码要求
最少字符数	8
最少大写字符数	1
最少小写字符数	1
最少数字字符数	1
最少特殊字符数 • 支持的字符：! @ # $ % ^ * _ ~ ? **注:** 密码不能包含单引号 (')、与符号 (&) 或空格字符。	1
最多字符数	40

注: 禁止重复使用上五个密码。按照顺序，一个以前的密码在第五次之后可重复使用。

ESXi 密码

应用装置上 ESXi 的默认 root 密码 PowerStore X model 采用以下格式： ***< Service_Tag >_123!***，其中*< Service_Tag >*是应用装置的七字符 Dell 服务标签。

在初始群集配置完成之前，请勿更改默认 ESXi 密码。有关更改 ESXi 密码的详细信息，请参阅 VMware ESXi 说明文件。

小心: 千万不要丢失 ESXi 密码。如果 ESXi 停机，而您没有密码，则必须重新初始化一体机。此行为对于 ESXi 是正常的，但是由于丢失密码而重新初始化可能会导致数据丢失。

小心: 默认 ESXi 密码针对每个应用装置进行了唯一配置 PowerStore X model 。当应用装置中的节点添加到 vCenter 群集时，该密码用于通过 ESXi 主机进行身份验证。如果在完全配置群集之前更改了默认密码，则必须重新初始化应用装置。

角色和权限

基于角色的访问控制允许用户拥有不同的权限。这提供了一种隔离管理角色以更好地与技能集和责任相符合的方法。

系统支持以下角色和权限：

注: 框中一个 ✔ 号表示这是该角色一项受支持的权限，空框表示对于该角色此权限不受支持。

任务	运算符	虚拟机管理员	安全性管理员	存储管理员	管理员
更改系统本地密码	✓	✓	✓	✓	✓
查看系统设置、状态和性能信息	✓		✓	✓	✓
修改系统设置					✓
创建、修改、删除资源和保护策略，以及启用/禁用 SSH				✓	✓
连接到 vCenter		✓		✓	✓
查看本地帐户的列表			✓		✓
添加、删除或修改本地帐户			✓		✓
通过连接到系统 VASA 提供程序的 vCenter 服务器查看系统存储信息，并注册/重新注册 VMware 证书颁发机构 (VMCA)/CA 证书		✓			✓

与文件相关的角色和权限

系统支持以下与文件相关的角色和权限：

注: 框中一个 ✓ 号表示这是该角色一项受支持的权限，空框表示对于该角色此权限不受支持。

任务	运算符	虚拟机管理员	安全性管理员	存储管理员	管理员
查看以下内容： • 文件系统警报 • NAS 服务器列表 • 文件系统列表 • 文件用户配额列表 • 文件接口路由列表 • 文件接口列表 • SMB 共享列表 • NFS 导出列表	✓		✓	✓	✓
查看以下内容： • 文件 DNS 服务器列表或指定的 DNS 服务器 • 文件 FTP 服务器列表或指定的 FTP 服务器 • 文件接口列表或指定的文件接口 • 文件接口路由列表或指定的接口路由 • 文件 Kerberos 服务器列表或指定的 Kerberos 服务器 • 文件 LDAP 服务器列表或指定的 LDAP 服务器 • 文件 NDMP 服务器列表或指定的 NDMP 服务器	✓		✓	✓	✓

任务	运算符	虚拟机管理员	安全性管理员	存储管理员	管理员
• 文件 NIS 服务器列表或指定的 NIS 服务器 • 文件系统列表或指定的文件系统 • 文件树配额列表或指定的文件树配额 • 文件用户配额列表或指定的用户配额 • 文件病毒检查程序列表或指定的文件病毒检查程序 • NAS 服务器列表或指定的 NAS 服务器 • NFS 导出列表或指定的 NFS 导出 • NFS 服务器列表或指定的 NFS 服务器 • SMB 服务器列表或指定的 SMB 服务器 • SMB 共享列表或指定的 SMB 共享					
添加、修改、删除或 ping 指定的 NAS 服务器，或将密码、主机或组上传到指定的 NAS 服务器				✓	✓
查看指定 NAS 服务器的密码或主机			✓		✓
添加文件系统，修改或删除现有 NAS 服务器上的指定文件系统				✓	✓
将克隆或快照添加到指定文件系统，或者刷新或恢复指定的文件系统，或者刷新指定文件系统的配额				✓	✓
添加文件树配额，或修改、删除、刷新指定文件树配额				✓	✓
添加文件用户配额，或修改、删除、刷新指定文件用户配额				✓	✓
添加文件病毒检查程序，或修改、删除指定的文件病毒检查程序，或上传指定的文件病毒检查程序配置					✓
下载指定的文件病毒检查程序配置			✓		✓
添加 SMB 或 NFS 服务器，或修改、删除、加入、脱离指定的 SMB 或 NFS 服务器				✓	✓
添加 SMB 共享，或修改、删除指定的 SMB 共享				✓	✓
添加 NFS 导出，或修改、删除指定的 NFS 导出				✓	✓
添加文件接口，或修改、删除指定的文件接口				✓	✓
添加文件接口路由，或修改、删除指定的文件接口路由				✓	✓

任务	运算符	虚拟机管理员	安全性管理员	存储管理员	管理员
添加文件 DNS、文件 FTP、文件 Kerberos、文件 LDAP、文件 NDMP 或文件 NIS 服务器，或修改、删除指定的文件 DNS、文件 FTP、文件 Kerberos、文件 LDAP、文件 NDMP 或文件 NIS 服务器				✓	✓
上传文件 Kerberos 密钥表					✓
下载文件 Kerberos 密钥表	✓		✓		✓
上传文件 LDAP 配置或 LDAP 证书					✓
下载文件 LDAP 证书			✓		✓

基于角色权限的用户帐户管理

具有 Administrator 或 Security Administrator 角色的用户可以执行以下与用户帐户管理相关的操作：

- 创建新的用户帐户。
- 删除除内置 Administrator 帐户以外的任何用户帐户。

  注: 内置的 Administrator 帐户无法删除。
- 将另一用户更改为任何角色。
- 重置另一个用户的密码。
- 锁定或解锁另一个用户帐户。

  注: 具有 Administrator 或 Security Administrator 角色的已登录用户不可以锁定他们自己的帐户。

已登录用户无法删除自己的用户帐户。此外，已登录用户只能更改自己的密码，具有 Security Administrator 或 Administrator 角色的用户除外。用户必须提供其旧密码才能更改其密码。已登录用户无法重置自己的密码、更改自己的角色、锁定或解锁自己的帐户。

不能编辑内置的 Administrator 帐户配置文件（具有 Administrator 角色），也不能将其锁定。

当用户的角色或锁定状态被更改，用户被删除，或其密码被 Security Administrator 或 Administrator 更改时，与该用户绑定的所有会话都会失效。

注: 如果用户在会话中更新自己的密码，会话将保持活动状态。

重置管理员和服务帐户密码

设备附带默认的管理员用户帐户，能让能够执行初始配置。另外，它还附带默认的服务用户帐户，能让您执行专门的服务功能。建议您最初使用 PowerStore Manager UI（而不是其他方法，如 REST API 或 CLI）配置 PowerStore。使用 PowerStore Manager UI 可确保更改所有默认密码。如果您忘记了新密码，可以将密码重置为默认值：

重置这些密码的方法取决于设备是 PowerStore T model 还是 PowerStore X model。使用与您的设备相对应的方法来重置管理员和/或服务密码。

将 PowerStore T model 设备中的管理员帐户和服务帐户密码重置为默认值

关于此任务

对于 PowerStore T model 设备，重置管理员或服务用户密码的主要方法是使用 USB 驱动器。支持的文件系统包括 FAT32 和 ISO 9660。

注: 要在设备处于服务模式时重置密码，请使用以下步骤，但有一个差别。为每个节点应用 USB 重置流程。当系统恢复为正常模式且 PowerStore Manager 登录时，此操作可确保提示您为管理员和服务用户提供新密码。

步骤

1. 如果 USB 驱动器已格式化，请转至下一步；否则，请使用命令提示符，例如 `format <d:> /FS:FAT32`，来格式化驱动器。
   其中 `d:` 是您已插入笔记本电脑或 PC 的 USB 驱动器的盘符。
2. 使用以下命令设置标签：

```
label d:
RSTPWD
```

   注: 设备将不会装载不带 `RSTPWD` 标签的 USB 驱动器。标记 USB 驱动器后，为您想要重置的帐户密码插入一个空文件。您可以重置管理员和/或服务帐户密码。

3. 要在驱动器上创建空文件，请根据需要使用以下一个或两个命令：

```
copy NUL d:\admin
copy NUL d:\service
```

4. 将 USB 驱动器插入设备任一节点的 USB 端口，等待 10 秒钟，然后将其拔下。
   您重置的每个帐户的密码现在均为默认值。
5. 使用群集 IP 地址通过浏览器连接到群集，并使用默认初始密码 **Password123#** 以管理员身份登录。
   应该会出现一个提示，要求重置管理员密码和/或服务密码。如果您更愿意使用安全外壳 (SSH) 重置服务密码，则服务帐户的初始默认密码是 **service**。
6. 将管理员密码从默认值更改为用户指定的密码。
7. 如果您想要将服务帐户密码设置为不同于管理员密码，请清除相关复选框。

结果

如果您在执行此过程后仍不提示您重置密码，请联系您的服务提供商。

将 PowerStore X model 设备中的管理员帐户和服务帐户密码重置为默认值

前提条件

了解主设备的主节点名称（例如，PSTX-44W1BW2-A 和 PowerStore D6013）。如有必要，请生成 `reset.iso` 文件。

关于此任务

对于 PowerStore X model 设备，可使用 ISO 映像并从 vSphere 中装载它。可从 www.dell.com/support 下载提前创建的映像文件。您还可以使用以下一个或两个触控命令从 Linux 系统创建自己的映像，具体取决于必须重置的密码：

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

注: ISO 映像 `reset.iso` 必须驻留在一个数据存储区上，然后才可以作为一个虚拟 CD 从 vSphere 装载。

注: 要在设备处于服务模式时重置密码，请使用以下步骤，但有两个差别。首先，您必须将 ISO 映像上传到控制器虚拟机 (VM) 本身的 PRIVATE-C9P42W2.A.INTERNAL 数据存储，因为公共数据存储不可用。其次，将 `reset.iso` 文件上传并应用于两个控制器虚拟机节点 A 和 B。当系统恢复为正常模式且提供 PowerStore Manager 访问时，此操作可确保提示您为管理员和服务用户提供新密码。

步骤

1. 在 vSphere 中的 **Storage** 下，选择您的 PowerStore X model 设备。
   例如，**DataCenter-WX-D6013** > **PowerStore D6013**
2. 在 **Files** 下，选择 **ISOs**。

3. 选择 **Upload** 并上传 `reset.iso` 文件，该文件可以是 www.dell.com/support 中预先创建的映像文件，或者是您在 Linux 系统中自行创建的映像文件。
   `reset.iso` 文件将出现在 **ISOs** 文件夹中。
4. 在 vSphere 中的 **Host and Clusters** 下，选择群集中主 PowerStore X model 设备的主节点。

   例如，**DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. 在 **Summary** 下，单击 **CD/DVD drive 1**，然后选择 **Connect to datastore ISO file**。
   此时将显示 **Choose an ISO image to mount** 窗口。
6. 在 **Datastores** 下，单击群集中的主 PowerStore X model 设备，然后选择 **ISOs** 文件夹。
   `reset.iso` 文件应显示在 **Contents** 下。
7. 选择 `reset.iso` 文件并单击 **OK**。
   在 **Summary** 下，**CD/DVD drive 1** 应显示为 **Connected** 约 10 秒，然后更改为 **Disconnected**。群集管理员密码和/或服务密码现已重置为默认值。
8. 使用群集 IP 地址通过浏览器连接到群集，并使用默认初始密码 **`Password123#`** 以管理员身份登录。
   应该会出现一个提示，要求重置管理员密码和/或服务密码。如果您更愿意使用 SSH 重置服务密码，则服务帐户的初始默认密码是 **`service`**。
9. 将管理员密码从默认值更改为用户指定的密码。
10. 如果您想要将服务帐户密码设置为不同于管理员密码，请清除相关复选框。

结果

如果您在执行此过程后仍不提示您重置密码，请联系您的服务提供商。

证书

PowerStore 的证书存储区中的数据是持久的。证书存储区存储以下类型的证书：

- 证书颁发机构 (CA) 证书
- 客户端证书
- 服务器证书

查看证书

关于此任务

对于存储在设备上的每个证书，PowerStore Manager 中将显示以下信息：

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

注: 使用 REST API 或 CLI 查看其他证书信息。

要查看证书信息，请执行以下操作：

步骤

1. 启动 PowerStore Manager。
2. 单击 **Settings**，然后在 **Security** 下单击 **Certificates**。
   此时将显示有关设备上所存储证书的信息。
3. 要查看构成证书的证书链及服务的关联信息，请单击特定服务。
   View Certificate Chain 将显示出来，并列出有关构成证书的证书链的信息。

保护群集中的 PowerStore 设备之间的通信

在群集创建过程中，群集主设备的主节点会创建一个证书颁发机构 (CA) 证书（也称为群集 CA）。主设备将群集 CA 证书传递给加入群集的设备。

群集中的每个 PowerStore 设备都会生成自己唯一的 IPsec 证书，该证书由群集 CA 证书签名。PowerStore 设备通过其群集网络传输的敏感数据受 IPsec 和 TLS 保护，使数据的安全性和完整性得到保证。

用于复制和数据导入的安全通信

PowerStore 的证书和凭据基础架构允许交换服务器和客户端证书，以及用户凭据。本过程包括：

- 在 TLS 握手期间检索和验证服务器证书
- 将受信任的 CA 证书从远程系统添加到凭据库
- 将受信任的服务器/客户端证书添加到凭据库
- 在建立信任后协助建立安全连接

PowerStore 支持以下证书管理功能：

- 对于复制，在两个 PowerStore 群集之间交换证书以建立受信任的管理通信。为简化 PowerStore 群集之间的复制，必须在群集之间建立双向信任，以便在发出复制 REST 控制请求时进行相互 TLS 身份验证。
- 对于数据导入，执行具有持久性的证书和凭据交换，以在 Dell EMC 存储系统（VNX、Unity、Storage Center (SC) 或对等存储 (PS) 系统）和 PowerStore 群集之间建立安全连接。

vSphere Storage API for Storage Awareness 支持

vSphere Storage API for Storage Awareness (VASA) 是一种由 VMware 定义的与供应商无关的 API，用于进行存储识别。VASA 提供程序包含了协作处理传入 VASA API 请求的多个组件。VASA API 网关接收所有传入的 VASA API，它部署在 PowerStore 群集中的主设备（拥有浮动管理 IP 的那一个）上。ESXi 主机和 vCenter Server 连接到 VASA 提供程序，获取有关可用存储拓扑、功能和状态的信息。接下来，vCenter 服务器将这些信息提供给 vSphere 客户端。VASA 由 VMware 客户端而不是 PowerStore Manager 客户端使用。

vSphere 用户必须将此 VASA 提供程序实例配置为群集的 VASA 信息提供程序。如果主导设备停止工作，相关流程（以及 VASA 提供程序）将在成为下一主设备的设备上重新启动。IP 地址自动进行故障切换。在内部，该协议在从新的活动 VASA 提供程序获取配置更改事件时将发现故障，但这会导致 VASA 对象的自动重新同步，无需用户干预。

PowerStore 为 vSphere 6.5 和 6.7 提供 VASA 3.0 接口。

VASA 3.0 支持虚拟卷 (VVol)。VASA 3.0 支持一些用于查询存储抽象（如 VVol 和存储容器）的接口。这些信息可帮助基于存储策略的管理 (SPBM) 在虚拟驱动器放置和遵从性方面作出决策。VASA 3.0 还支持用于调配和管理用于备份虚拟驱动器的 VVol 生命周期的接口。ESXi 主机直接调用这些接口。

有关与 VASA、vSphere 和 VVol 相关的详细信息，请参阅 VMware 文档和 PowerStore Manager 联机帮助。

与 VASA 相关的身份认证

要启动从 vCenter 到 PowerStore Manager VASA 提供程序的连接，请使用 vSphere 客户端输入以下信息：

- VASA 提供程序的 URL，对于 VASA 3.0 使用以下格式：https://<Management IP address>:8443/version.xml。
- PowerStore Manager 用户的用户名（角色必须为 VM 管理员或管理员）。

  注: VM 管理员角色仅用作一种注册证书的方法。
- 与该用户关联的密码。

此处使用的 PowerStore Manager 凭据将只在该连接的第一步使用。如果 PowerStore Manager 凭据对于目标群集有效，则将向群集自动注册 vCenter 服务器的证书。该证书用于验证来自 vCenter 的所有后续请求。安装或向 VASA 提供程序上传该证书不需要手动步骤。如果证书已过期，vCenter 必须注册新证书才能支持新会话。如果用户撤消了证书，则会话将失效且连接将断开。

vCenter 会话、安全连接和凭据

当 vSphere 管理员使用 vSphere Client 来为 vCenter Server 提供 VASA 提供程序 URL 和登录凭据时，vCenter 会话即开始。vCenter Server 使用 URL、凭据和 VASA 提供程序的 SSL 证书来建立与 VASA 提供程序的安全连接。发生以下某个事件时，vCenter 会话结束：

- 管理员使用 vSphere Client 从 vCenter 配置中删除 VASA 提供程序，并由 vCenter Server 终止连接。
- vCenter Server 发生故障或 vCenter Server 服务发生故障，并终止连接。如果 vCenter 或 vCenter Server 服务无法重新建立 SSL 连接，则将启动一个新连接。
- VASA Provider 发生故障，并终止连接。当 VASA Provider 启动时，它可响应来自 vCenter Server 的通信以重新建立 SSL 连接和 VASA 会话。

vCenter 会话基于 vCenter Server 和 VASA 提供程序之间的安全 HTTPS 通信。在 VASA 3.0 中，vCenter Server 充当 VMware 证书颁发机构 (VMCA)。VASA 提供程序会在授权请求后针对该请求传输一个自签名证书。它将 VMCA 证书添加到其信任存储区，然后发出证书签名请求，再将其自签名证书替换为 VMCA 签名的证书。VASA 提供程序将使用对照以前注册的根签名证书进行验证的客户端存储监视服务 (SMS) 证书，来对以后的连接进行身份验证。VASA 提供程序为存储实体对象生成唯一标识符，然后 vCenter Server 使用该标识符为特定实体请求数据。

VASA 提供程序使用 SSL 证书和 VASA 会话标识符验证 VASA 会话。建立会话后，VASA 提供程序必须验证 SSL 证书和 VASA 会话标识符（与从 vCenter Server 每次调用的函数关联）。VASA 提供程序使用存储在其信任存储区中的 VMCA 证书验证与从 vCenter SMS 调用的函数相关联的证书。VASA 会话在多个 SSL 连接之间延续。如果 SSL 连接中断，则 vCenter Server 将与 VASA 提供程序执行 SSL 握手，在同一 VASA 会话的上下文中重新建立 SSL 连接。如果 SSL 证书到期，则 vSphere 管理员必须生成新证书。vCenter Server 将建立新 SSL 连接，然后向 VASA 提供程序注册该新证书。

小心: SMS 不会针对 3.0 VASA 提供程序调用 `unregisterVASACertificate` 函数。因此，即使在注销后，VASA 提供程序也可以继续使用从 SMS 获取的 VMCA 签名证书。

CHAP 身份认证

质询握手身份验证协议 (CHAP) 是一种对 iSCSI 启动器（主机）和目标（卷和快照）进行身份验证的方法。CHAP 公开了 iSCSI 存储，并确保了安全、标准的存储协议。身份验证依赖于身份验证方和对等方均知道的一项秘密（类似于密码）。CHAP 协议有两种变体：

- 单向 CHAP 身份验证允许 iSCSI 目标对启动器进行身份验证。当启动器尝试连接到目标时（正常模式或通过发现模式），会向目标提供一个用户名和密码。
- 除了单向 CHAP 外，还应用双向 CHAP 身份验证。双向 CHAP 允许 iSCSI 目标和启动器彼此进行身份验证。组中呈现的每个 iSCSI 目标都会由 iSCSI 启动器进行身份验证。当启动器尝试连接到目标时，目标会向启动器提供用户名和密码。启动器将提供的用户名和密码与它所持有的信息进行比较。如果匹配，则启动器可连接到目标。

注: 如果您的环境中将使用 CHAP，建议您在准备卷以接收数据之前设置并启用 CHAP 身份验证。如果在设置并启用 CHAP 身份验证之前准备用来接收数据的驱动器，您可能会失去对卷的访问权。

PowerStore 不支持 iSCSI CHAP 发现模式。下表显示了与 ISCSI CHAP 发现模式相关的 PowerStore 限制。

表. 1: iSCSI CHAP 发现模式限制

CHAP 模式	单一模式（启动器已启用）	相互模式（启动器和目标已启用）
发现	PowerStore 不会对主机进行身份验证（质询）。不能使用身份验证来阻止目标被发现。这不会导致意外访问用户数据。	PowerStore 将不响应来自主机的身份验证请求（质询），如果主机质询 PowerStore，发现将会失败。
正常	按预期发挥作用。PowerStore 对凭据进行测试。	按预期发挥作用。由 PowerStore 传输凭据。

对于源和目标设备之间的远程复制，验证和更新过程会检测本地和远程系统中的更改并重新建立数据连接，同时还会考虑 CHAP 设置。

配置 CHAP

可在 PowerStore 群集上启用 CHAP 单向（启动器已启用）或双向（启动器和目标已启用）身份验证。可对具有一个设备或多个 PowerStore 设备和外部主机的群集实施启用 CHAP。

启用单向身份验证时，在添加外部主机时需要输入每个启动器的用户名和密码。启用双向身份验证时，还需要输入群集的用户名和密码。当添加主机并添加启用 CHAP 的启动器时，启动器密码必须是唯一的，您不能在主机的各个启动器中使用相同的密码。有关如何配置外部主机的 CHAP 配置的具体详细信息将因情况而异。要利用此功能，您需要熟悉主机的操作系统以及如何配置它。

注: 一旦在系统上配置了主机之后，启用 CHAP 对于外部主机将是一种会造成中断的操作。它会导致 I/O 中断，直到在外部主机和设备上的配置均设置好。建议您在将外部主机添加到设备之前，确定要实施的 CHAP 配置的类型（如果有）。

如果在添加主机后启用 CHAP，则更新每个主机的启动器。如果主机启用了 CHAP，则不能将它添加到没有 CHAP 凭据的主机组。如果是在启用 CHAP 之后添加一个主机，则需要在 PowerStore Manager 中手动注册该主机，方法是在 **Compute** 之下选择 **Hosts & Host Groups**。您需要在 iSCSI 级别输入凭据，以供身份验证之用。在这种情况下，请从主机拷贝 IQN，然后为每个启动器添加相关 CHAP 凭据。

可以通过以下任一方式为群集配置 CHAP：

- **CHAP** — 一个您可以从 PowerStore Manager 访问的 CHAP 页面（单击 **Settings**，在 **Security** 下选择 **CHAP**）。
- REST API 服务器 — 可以接收配置 CHAP 设置的 REST API 请求的应用程序接口。有关 REST API 的更多信息，请参阅 *PowerStore REST API Reference Guide*。

要确定 CHAP 的状态，请在 PowerStore Manager 中单击 **Settings**，并在 **Security** 之下选择 **CHAP**。

外部 SSH 访问

每个设备可以选择启用对设备 IP 地址的 SSH 端口的外部安全外壳 (SSH) 访问，这会将用户转到设备主节点上的服务功能。设备 IP 地址将在设备的两个节点之间随着主节点指定的改变而浮动。如果禁用外部 SSH，则不允许授予 SSH 访问权限。

当设备首次启动并且未配置时，SSH 默认处于启用状态，这样如果在将设备添加到群集之前遇到问题，可以对设备进行维护。当创建新群集或执行群集合并操作时，所有设备都应将 SSH 初始设置为禁用。

配置外部 SSH 访问

您可以通过使用以下任一方式，配置外部 SSH 对群集中设备的访问：

- **SSH Management** — 一个您可以从 PowerStore Manager 访问的 SSH 设置页面（单击 **Settings**，在 **Security** 下选择 **SSH Management**）。
- REST API 服务器 — 可以接收 REST API 请求，以配置 SSH 设置的应用程序接口。有关 REST API 的更多信息，请参阅 *PowerStore REST API Reference Guide*。
- `svc_service_config` — 一种服务命令，您作为设备上的服务用户可以直接输入。有关此命令的详细信息，请参阅 *PowerStore Service Scripts Guide*。

要确定群集中设备上 SSH 的状态，请在 PowerStore Manager 中单击 **Settings**，并在 **Security** 下选择 **SSH Management**。您还可以在所选的一个或多个设备上启用或禁用 SSH。

成功启用 SSH 服务后，使用任何 SSH 客户端登录到设备 IP 地址。访问设备需要服务用户凭据。

通过服务帐户，用户可以执行以下功能：

- 执行专门的设备服务脚本，以便对设备系统设置和运行情况进行监视和故障排除。
- 仅操作一组有限的命令，这些命令在受限 shell 模式下分配给非特权 Linux 用户帐户的成员。此帐户无权访问专有系统文件、配置文件或者用户或客户数据。

为使设备达到最大安全性，建议一直将外部 SSH 服务接口保持禁用，除非专门需要它在设备上执行服务操作。在执行必要的服务操作之后，应禁用 SSH 接口以确保设备安全。

SSH 会话

系统会根据 SSH 客户端建立的设置，对 PowerStore SSH 服务界面会话进行维护。会话特征由 SSH 客户端配置设置决定。

服务帐户密码

服务帐户是服务人员可用来执行基本 Linux 命令的帐户。

在设备的初始配置过程中，您必须更改默认服务密码。服务密码限制与应用于系统管理帐户的密码限制相同（请参见用户名和密码的使用 页面上的 7）。

SSH 授权

服务帐户基于以下因素进行授权：

- 应用程序隔离 — PowerStore 软件使用可隔离应用程序的容器技术。服务容器提供了设备服务的访问权限，只有一组服务脚本和一组 Linux 命令可用。服务帐户无法访问向用户提供文件系统和数据块 I/O 的其他容器。
- Linux 文件系统权限 — 以任何方式修改系统操作的大多数 Linux 工具和应用程序对于服务用户不可用，需要超级用户帐户权限。由于服务帐户没有此类访问权限，因此它无法使用需要拥有对其的执行权限才能使用的 Linux 工具和应用工具，也无法编辑需要 root 访问权限才能读取或修改或执行上述两种操作的配置文件。
- 访问控制 — 除了容器技术提供的应用程序隔离之外，设备上的访问控制列表 (ACL) 机制会使用非常具体的规则列表来明确授予或拒绝服务帐户对系统资源的访问权限。这些规则会指定服务帐户对设备其他方面的权限，这些权限并未由标准 Linux 文件系统权限另行定义。

设备服务脚本

设备的软件版本上安装了一组问题诊断、系统配置和系统恢复脚本。这些脚本可提供深层次的信息，还可提供比 PowerStore Manager 级别更低的系统控制。*PowerStore Service Scripts Guide* 介绍了这些脚本及其常见应用场景。

设备节点以太网服务端口和 IPMItool

您的设备通过每个节点上的以太网服务端口提供控制台访问权限。这一访问需要使用 IPMItool。IPMItool 是一种类似于 SSH 或 Telnet 的网络工具，使用 IPMI 协议通过以太网与每个节点连接。IPMItool 是一款 Windows 实用程序，会通过安全通信通道访问设备的节点控制台。此实用程序需要实体访问以激活控制台。

节点以太网服务端口接口提供与服务 SSH 接口（服务 LAN 接口）相同的功能和特性，而且还受到相同的限制。但用户是通过以太网端口连接来访问接口的，而不是通过 SSH 客户端。此接口专为现场服务人员设计，他们可连接到设备而不必中断网络。无需专用管理控制台。

此接口提供不可路由的直接点对点连接。服务人员可将服务 LAN 接口用于控制台输出，通过 SSH 访问 PowerStore Service Container 和 PowerStore Manager，包括 ICW（初始配置向导）。始终支持通过服务 LAN 接口对 Service Container 进行 SSH 访问，并且不能禁用；但您可以管理服务帐户凭据。

有关服务脚本的列表，请参阅 *PowerStore Service Scripts Guide*。

NFS 安全

NFS 安全是通过 Kerberos 使用 NFSv3 和 NFSv4 对用户进行身份认证。Kerberos 提供完整性（签名）和隐私（加密）。无需启用完整性和隐私，它们是 NFS 导出选项。

如果没有 Kerberos，服务器会完全依赖于客户端对用户进行身份认证：服务器信任客户端。如果使用 Kerberos，则情况并非如此，服务器将信任密钥发行中心 (KDC)。将由 KDC 处理身份认证并管理帐户（主体）和密码。此外，不会以任何形式在线路中发送密码。

如果没有 Kerberos，将在未加密的线路中发送用户的凭据，因而可以轻松地假冒。如果使用 Kerberos，用户的身份（主体）将包括在加密的 Kerberos 票证中，只能由目标服务器和 KDC 读取。只有它们知道加密密钥。

在与 NFS 安全结合使用时，支持 Kerberos 中的 AES128 和 AES256 加密。与 NFS 安全一起，这还会影响 SMB 和 LDAP。这些加密现在默认受 Windows 和 Linux 支持。这些新加密更安全；但是，是否使用它们由客户端决定。从这一用户主体，服务器将通过查询活动 Unix Directory Service (UDS) 来生成该用户的凭据。由于 NIS 未设安全保护，因此建议不要将其与 NFS 安全结合使用。建议将 Kerberos 与 LDAP 或 LDAPS 结合使用。

可以通过 PowerStore Manager 配置 NFS 安全访问。

文件协议关系

使用 Kerberos 需要以下内容：

- DNS — 您必须使用 DNS 名称，而不是 IP 地址
- NTP — PowerStore 必须配置 NTP 服务器。

注: Kerberos 依赖于 KDC、服务器和网络客户端之间的正确时间同步。

- UDS — 用于构建凭据。
- 主机名 — Kerberos 将使用名称而非 IP 地址。

NFS 安全访问使用一个或两个服务主体名称 (SPN)，具体取决于主机名的值。如果主机名采用 FQDN 格式 host.domain：

- 短 SPN：**nfs/host@REALM**
- 长 SPN：**nfs/host.domainFQDN@REALM**

如果主机名未采用 FQDN 格式，则只会使用短 SPN。

与 SMB（SMB 服务器可以加入到域中）类似，NFS 服务器也可以加入到领域（ “域” 的 Kerberos 等效术语）。对此有两个选项：

- 使用已配置的 Windows 域（如有）
- 完全配置基于 UNIX KDC 的 Kerberos 领域

如果管理员选择使用已配置的 Windows 域，则无需执行其他操作。NFS 服务使用的每个 SPN 在加入/退出 SMB 服务器时，都会自动添加到 KDC 中/从 KDC 中删除。请注意，如果 NFS 安全配置为使用 SMB 配置，则不能销毁 SMB 服务器。

如果管理员选择使用基于 UNIX 的 Kerberos 领域，则需要更多的配置：

- 领域名称：Kerberos 领域的名称，通常全部包含大写字母。
- 完全配置基于 UNIX KDC 的 Kerberos 领域。

为确保客户端装载具有特定安全性的 NFS 导出，系统会提供一个安全参数 sec 来指示所允许的最低安全性。有 4 种安全性：

- `AUTH_SYS`：不使用 Kerberos 的标准旧式安全性。服务器信任客户端提供的凭据
- `KRB5`：使用 Kerberos v5 进行身份验证
- `KRB5i`：Kerberos 身份验证加完整性（签名）
- `KRB5p`：Kerberos 身份验证加完整性，再加隐私（加密）

如果 NFS 客户端尝试装载安全性低于配置的最低安全性的导出，则将拒绝访问。例如，如果最低访问权限是 `KRB5i`，将拒绝任何使用 `AUTH_SYS` 或 `KRB5` 的装载。

构建凭据

当用户连接到系统时，它只会显示其主体 **user@REALM**，这是从 Kerberos 票证中提取的。与 `AUTH_SYS` 安全性不同，凭据不包括在 NFS 请求中。从主体中，提取出（@ 之前的）用户部分并将其用于查找相应 UID 的 UDS。从该 UID，系统使用活动 UDS 构建凭据，类似于启用扩展 NFS 凭据的情况（但有例外情况，在不使用 Kerberos 时，UID 直接由请求提供）。

如果未在 UDS 中映射主体，则会改用已配置的默认 UNIX 用户凭据。如果未设置默认 UNIX 用户，则使用的凭据将为 nobody。

文件系统对象安全性

在多协议环境中，安全策略在文件系统级别设置，每个文件系统具有独立的安全策略。每个文件系统使用其访问策略来确定如何协调 NFS 和 SMB 访问控制语义之间的差异。选择访问策略将决定使用哪一种机制来执行特定文件系统上的文件安全。

注: 如果您的环境需要支持较旧的 SMB1 协议，可以通过使用 `svc_nas_cifssupport` 服务命令来启用它。有关此服务命令的详细信息，请参阅 *PowerStore Service Scripts Guide*。

UNIX 安全模式

选中 UNIX 策略后，任何更改文件级安全（比如从 SMB 协议更改为访问控制列表 (ACL)）的企图都将被忽略。UNIX 访问权限称为文件系统对象的模式位或 NFSv4 ACL。模式位用一个位字符串来表示。每个位代表一个访问模式或权限，这些访问模式或权限被授予拥有与文件系统对象相关联的文件、组的用户以及所有其他用户。对于每个用户类别（用户、组或其他），UNIX 模式位都表示为三组并置 rwx（读、写和执行）三元组。ACL 是用户和用户组的列表，通过该列表，可以控制允许还是拒绝访问服务。

Windows 安全模式

Windows 安全模式主要基于对象的权限，其中涉及使用安全描述符 (SD) 和对象的访问控制列表 (ACL)。选中 SMB 策略后，对来自 NFS 协议的模式位的更改将被忽略。

对文件系统对象的访问基于是否已使用安全描述符将权限设置为“允许”或“拒绝”。SD 描述了对象的所有者和对象的组 SID 及其 ACL。ACL 是每个对象的安全描述符的一部分。每个 ACL 都包含访问控制项 (ACE)。反过来，每个 ACE 都包含标识用户、组或计算机的单个 SID，以及此 SID 拒绝或允许的权限列表。

多协议环境中的文件系统访问

通过 NAS 服务器提供文件访问。NAS 服务器包含一系列用于存储数据的文件系统。NAS 服务器通过 SMB 共享和 NFS 共享来共享文件系统，使得可利用 NFS、SMB 文件协议访问这些数据。通过多协议共享的 NAS 服务器模式，可在 SMB 与 NFS 之间共享相同的数据。由于多协议共享模式可同时提供对文件系统的 SMB 和 NFS 访问，所以必须为多协议共享考虑并正确配置 Windows 用户到 UNIX 用户的映射以及定义要使用的安全规则（模式位、ACL 和用户凭据）。

注: 有关针对多协议共享、用户映射、访问策略和用户凭据来配置和管理 NAS 服务器的信息，请参阅 PowerStore Manager 联机帮助。

用户映射

在多协议环境中，Windows 用户需要匹配到 UNIX 用户。但是，仅当访问策略是 Windows 时，UNIX 用户才必须映射到 Windows 用户。为执行文件系统安全性，这种匹配是必要的，即便并非协议所固有。用户映射中涉及以下组件：

- UNIX 目录服务和/或本地文件
- Windows 解析器
- 安全映射 (secmap) 是一种缓存，其中包含 NAS 服务器所使用的 SID 和 UID 或 GID 之间的所有映射。
- ntxmap

注: 用户映射不影响 SMB 服务器本地的用户或组。

UNIX 目录服务和本地文件

UNIX 目录服务 (UDS) 和本地文件用于执行以下操作：

- 返回特定用户标识符 (UID) 的相应 UNIX 帐户名称。
- 返回特定 UNIX 帐户名称的相应 UID 和主要组标识符 (GID)。

支持的服务包括：

- LDAP
- NIS
- 本地文件
- 无（唯一可能的映射是通过默认用户）

当启用了多协议共享时，应当为 NAS 服务器启用一个 UDS 或本地文件，或本地文件和 UDS 都启用。NAS 服务器的 Unix 目录服务属性确定哪个服务用于用户映射。

Windows 解析器

使用 Windows 解析程序为用户映射执行以下操作：

- 返回特定安全标识符 (SID) 的相应 Windows 帐户名
- 返回特定 Windows 帐户名称的相应 SID

Windows 解析器包括：

- 域的域控制器 (DC)
- SMB 服务器的本地组数据库 (LGDB)

secmap

secmap 的作用是存储所有 SID 到 UID 和主要 GID 以及 UID 到 SID 映射，确保在 NAS 服务器的所有文件系统上的一致性。

ntxmap

ntxmap 用于在 Windows 帐户名和 UNIX 帐户名不同时关联二者。例如，假设用户有一个帐户，在 Windows 上叫 Gerald，在 UNIX 上叫 Gerry，于是 ntxmap 用来在二者间建立关联。

SID 到 UID 和主要 GID 的映射

将按照下列过程顺序解析 SID 到 UID 和主要 GID 的映射：

1. 搜索 secmap 以查找 SID。如果找到 SID，则 UID 和 GID 映射解析。
2. 如果在 secmap 中找不到 SID，必须找到与 SID 相关的 Windows 名称。
   a. 搜索 NAS 的 SMB 服务器的本地组数据库，以查找 SID。如果找到 SID，则相关的 Windows 名称就是本地用户名称加上 SMB 服务器名称。
   b. 如果在本地组数据库中找不到 SID，则搜索域的 DC。如果找到 SID，则相关的 Windows 名称就是用户名称。如果 SID 不可解析，则拒绝访问。
3. Windows 名称被转换为 UNIX 名称。ntxmap 用于以下目的。
   a. 如果在 ntxmap 中找到 Windows 名称，则该条目用作 UNIX 名称。
   b. 如果在 ntxmap 中未找到 Windows 名称，则 Windows 名称用作 UNIX 名称。
4. 使用 UNIX 名称搜索 UDS（NIS 服务器、LDAP 服务器或本地文件）。
   a. 如果在 UDS 中找到 UNIX 用户名称，则 UID 和 GID 映射解析。
   b. 如果找不到 UNIX 名称，但启用了未映射 Windows 帐户功能的自动映射，则会自动分配 UID。
   c. 如果在 UDS 中找不到 UNIX 用户名称，但存在一个默认 UNIX 帐户，则 UID 和 GID 映射解析为该默认 UNIX 帐户的用户名称。
   d. 如果 SID 不可解析，则拒绝访问。

如果找到了该映射，则它被添加到持久性的 secmap 数据库中。如果找不到该映射，则失败的映射被添加到持久性的 secmap 数据库中。

下图阐释了用来解析 SID 到 UID（主要 GID）映射的过程：

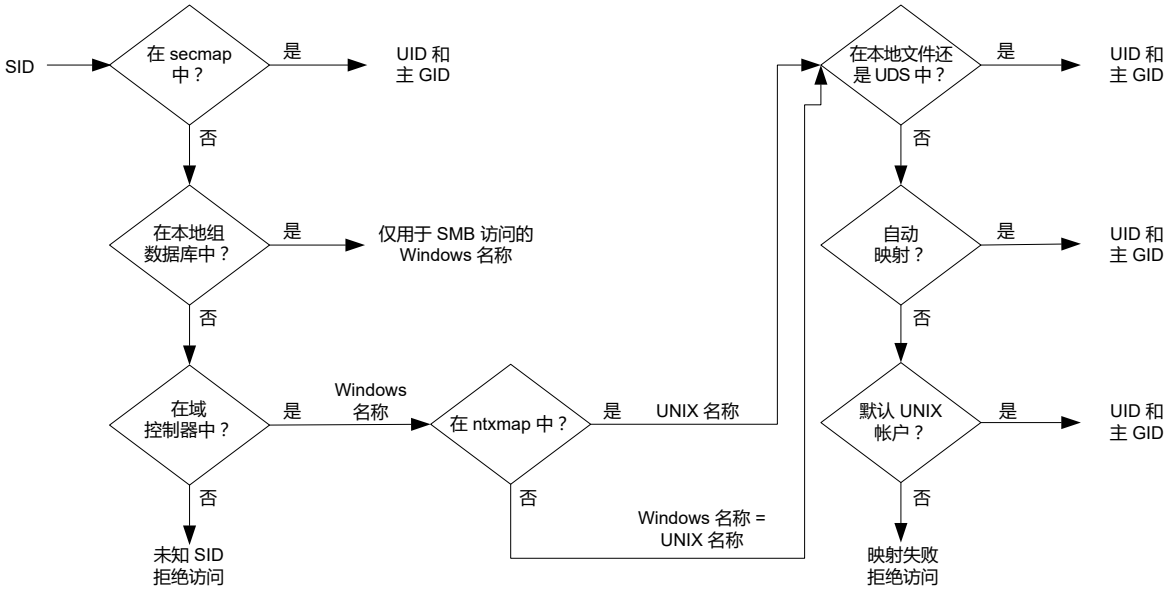

图 1: 用来解析 SID 到 UID（主要 GID）映射的过程

UID 到 SID 映射

将按照下列过程顺序解析 UID 到 SID 映射：

1. 搜索 ecmap 以查找 UID。如果找到 UID，则 SID 映射解析。
2. 如果在 secmap 中找不到 UID，必须找与 UID 相关的 UNIX 名称。
   a. 使用 UID 搜索 UDS（NIS 服务器、LDAP 服务器或本地文件）。如果找到 UID，则相关的 UNIX 名称就是用户名称。
   b. 如果在 UDS 中找不到 UID，但存在一个默认 Windows 帐户，则 UID 将被映射到默认 Windows 帐户的 SID。
3. 如果不使用默认 Windows 帐户信息，则 UNIX 名称转换成 Windows 名称。ntxmap 用于以下目的。
   a. 如果在 ntxmap 中找到 UNIX 名称，则该条目用作 Windows 名称。
   b. 如果在 ntxmap 中找不到 UNIX 名称，则 UNIX 名称用作 Windows 名称。
4. 使用 Windows 名称搜索 Windows DC 或本地组数据库。
   a. 如果找到 Windows 名称，则解析 SID 映射。
   b. 如果 Windows 名称包含一个句点并且最后一个句点 (.) 后跟的名称部分与 SMB 服务器名称匹配，则搜索该 SMB 服务器的本地组数据库来解析 SID 映射。
   c. 如果找不到 Windows 名称，但存在一个默认 Windows 帐户，则 SID 将被映射到默认 Windows 帐户的 SID。
   d. 如果 SID 不可解析，则拒绝访问。

如果找到了该映射，则它被添加到持久性的 secmap 数据库中。如果找不到该映射，则失败的映射被添加到持久性的 secmap 数据库中。

下图阐释了用来解析 UID 到 SID 映射的过程：

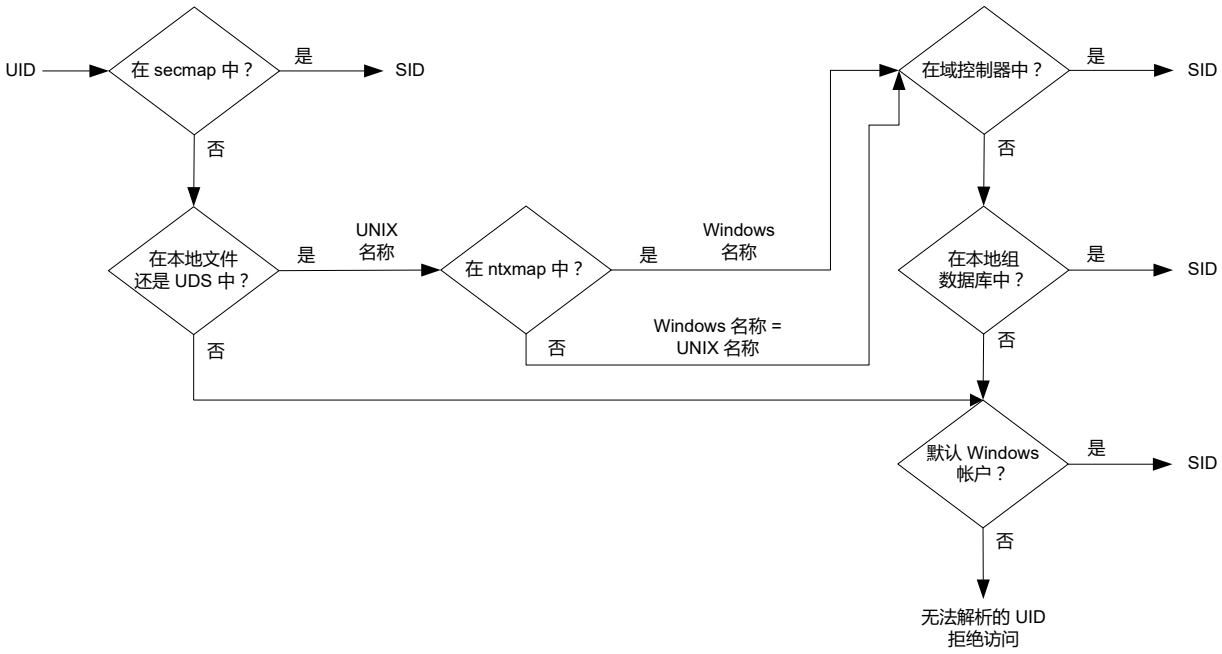

图 2: 用来解析 UID 到 SID 映射的过程

NFS、SMB 和 FTP 的访问策略

在多协议环境中，存储系统使用文件系统访问策略来管理文件系统的用户访问控制。有两种安全保护机制：UNIX 和 Windows。

对于 UNIX 安全身份验证，从 UNIX 目录服务 (UDS) 构建凭据，但非安全 NFS 访问除外，其凭据由主机客户端提供。用户权限根据模式位和 NFSv4 ACL 确定。用户和组标识符（分别为 UID 和 GID）用于标识。没有与 UNIX 安全机制关联的权限。

对于 Windows 安全身份验证，从 SMB 服务器的 Windows 域控制器 (DC) 和本地组数据库 (LGDB) 构建凭据。从 SMB ACL 决定用户权利。安全标识符 (SID) 用于标识。有一些与 Windows 安全性关联的权限，如 TakeOwnership（接管）、Backup（备份）和 Restore（恢复），它们由 SMB 服务器的 LGDB 或组策略对象 (GPO) 授权。

下表介绍了定义哪些协议使用哪种安全机制的访问策略：

访问策略	描述
Native（默认值）	• 每个协议均通过自身的本机安全性来管理访问。 • NFS 共享的安全性使用与检查 NFSv3 UNIX 模式位或 NFSv4 ACL 的请求关联的 UNIX 凭据。然后准予或拒绝访问。 • SMB 共享的安全性使用与检查 SMB ACL 的请求关联的 Windows 凭据。然后准予或拒绝访问。 • NFSv3 UNIX 模式位和 NFSv4 ACL 权限的更改彼此同步。 • Unix 与 Windows 权限之间没有同步。
Windows	• 使用 Windows 安全机制确保 Windows 和 UNIX 文件级访问的安全。 • 使用 Windows 凭据检查 SMB ACL。 • 新建文件的权限由 SMB ACL 转换确定。SMB ACL 权限更改同步到 NFSv3 UNIX 模式位或 NFSv4 ACL。 • NFSv3 模式位和 NFSv4 ACL 权限更改将被拒绝。
UNIX	• 使用 UNIX 安全机制确保 Windows 和 UNIX 文件级访问的安全。 • 根据 SMB 访问请求，使用从本地文件或 UDS 构建的 UNIX 凭据检查 NFSv3 模式位或 NFSv4 ACL 的权限。 • 新建文件的权限由 UMASK 确定。 • NFSv3 UNIX 模式位或 NFSv4 ACL 权限更改同步到 SMB ACL。 • 为避免造成中断，允许更改 SMB ACL 权限，但不会维护这些权限。

对于 FTP，是使用 Windows 还是 UNIX 进行身份验证取决于在对 NAS 服务器进行身份验证时所使用的用户名格式。如果使用 Windows 身份验证，则 FTP 访问控制类似于 SMB；否则，身份验证类似于 NFS。FTP 和 SFTP 客户端在连接到 NAS 服务器时进行身份验证。它可以是 SMB 身份验证（当用户名的格式为 `domain\user` 或 `user@domain` 时）或 UNIX 身份验证（对于单个用户名的其他格式）。由 NAS 服务器中定义的域的 Windows DC 确保进行 SMB 身份验证。UNIX 身份验证通过 NAS 服务器按照在远程 LDAP 服务器、远程 NIS 服务器或 NAS 服务器的本地密码文件中存储的加密密码进行保证。

用于文件级安全的凭据

要强制实施文件级安全，存储系统必须构建一个与所处理的 SMB 或 NFS 请求关联的凭据。有以下两种凭据：Windows 和 UNIX。NAS 服务器为下列使用情形构建 UNIX 和 Windows 凭据：

- 为 NFS 请求构建包含 16 个以上组的 UNIX 凭据。NAS 服务器扩展的凭据属性必须设置为提供这种能力。
- 当文件系统的访问策略是 UNIX 时，为 SMB 请求构建 UNIX 凭据。
- 为 SMB 请求构建 Windows 凭据。
- 当文件系统的访问策略是 Windows 时，为 NFS 请求构建 Windows 凭据。

注: 对于 NFS 请求，如果未设置扩展的凭据属性，则使用来自 NFS 请求的 UNIX 凭据。当 Kerberos 身份认证用于 SMB 请求时，域用户的 Windows 凭据包括在会话建立请求的 Kerberos 票证中。

以下情形将使用永久性凭据缓存：

- 为访问具有 Windows 访问策略的文件系统而构建的 Windows 凭据。
- 在扩展凭据启用的情况下用于通过 NFS 进行访问的 Unix 凭据。

每个 NAS 服务器都有一个缓存实例。

授予未映射用户访问权限

多协议要求满足以下条件：

- 必须将 Windows 用户映射到 UNIX 用户。
- 当 UNIX 用户访问一个有 Windows 访问策略的文件系统时，为构建 Windows 凭据，此用户必须映射到一个 Windows 用户。

对于未映射的用户，有两个属性关联到 NAS 服务器：

- 默认 UNIX 用户。
- 默认 Windows 用户。

当未映射的 Windows 用户试图连接到一个多协议文件系统而为 NAS 服务器配置的是默认 UNIX 用户帐户时，在 Windows 凭据中使用默认 UNIX 用户的用户标识符 (UID) 和主要组标识符 (GID)。同理，当未映射的 UNIX 用户试图连接到一个多协议文件系统而为 NAS 服务器配置的是默认 Windows 用户帐户时，使用默认的 Windows 用户的 Windows 凭据。

注: 如果 UNIX 目录服务 (UDS) 中未设置默认 UNIX 用户，则拒绝未映射的用户进行 SMB 访问。如果在 Windows DC 或 LGDB 中找不到默认 Windows 用户，则拒绝未映射用户对具有 Windows 访问策略的文件系统进行 NFS 访问。

注: 默认 UNIX 用户既可以是有效的现有 UNIX 帐户名称，也可以遵循新的格式 `@uid=xxxx,gid=yyyy@`，其中 *xxxx* 和 *yyyy* 分别是 UID 和主要 GID 的十进制数值，可以通过 PowerStore Manager 在系统上进行配置。

用于 NFS 请求的 UNIX 凭据

若要为仅 NFS 或具有 UNIX 或本机访问策略的多协议文件系统处理 NFS 请求，必须使用 UNIX 凭据。UNIX 凭据始终嵌入在每个请求中；不过，凭据限制为 16 个额外组。通过 NFS 服务器的 `extendedUnixCredEnabled` 属性，可以构建用于超过 16 个组的凭据。如果设置了此属性，系统将使用 UID 对活动 UDS 进行查询以获得主要 GID 及其所属的所有组 GID。如果未在 UDS 中找到 UID，系统将使用嵌入在请求中的 UNIX 凭据。

注: 对于 NFS 安全访问，必须始终使用 UDS 构建凭据。

用于 SMB 请求的 UNIX 凭据

若要为具有 UNIX 访问策略的多协议文件系统处理 SMB 请求，必须在会话建立时，先为 SMB 用户构建 Windows 凭据。Windows 用户的 SID 用于从 AD 查找名称。该名称然后（也可以通过 ntxmap）用于从 UDS 或本地文件（passwd 文件）查找 Unix UID 和 GID。用户的所有者 UID 包括在 Windows 凭据中。当访问一个有 UNIX 访问策略的文件系统时，将使用用户的 UID 查询 UDS 以构建 UNIX 凭据，类似于为 NFS 构建扩展凭据的过程。UID 为配额管理所必需。

用于 SMB 请求的 Windows 凭据

若要为仅 SMB 或具有 Windows 或本机访问策略的多协议文件系统处理 SMB 请求，必须使用 Windows 凭据。只需在用户连接过程中会话建立请求时，构建一次用于 SMB 的 Windows 凭据。

当使用 Kerberos 身份认证时，用户的凭据包括在会话建立请求的 Kerberos 票证中，这与使用 NT LAN Manager (NTLM) 时不同。其他信息从 Windows DC 或 LGDB 中查询得到。对于 Kerberos，从 Kerberos 票证和额外本地组 SID 的列表中获取额外组 SID 的列表。从 LGDB 中获取权限列表。对于 NTLM，从 Windows DC 和额外本地组 SID 的列表中获取额外组 SID 的列表。从 LGDB 中获取权限列表。

此外，还可以从用户映射组件中检索相应的 UID 和主要 GID。由于主要组 SID 未用于访问检查，因此将使用 UNIX 的主要 GID。

注: NTLM 是较早的一个专有安全协议套件，为用户提供身份验证、完整性和机密性。Kerberos 是一种开放的标准协议，通过使用票务系统来提供更快的身份验证。Kerberos 为网络系统添加比 NTLM 更高的安全性。

用于 NFS 请求的 Windows 凭据

仅当用户试图通过 NFS 请求访问具有 Windows 访问策略的文件系统时，才会构建或检索 Windows 凭据。UID 提取自 NFS 请求。有一个全局 Windows 凭据缓存，可帮助避免对具有关联保留时间的每个 NFS 请求构建凭据。如果在此缓存中找到 Windows 凭据，则不需要执行任何其他操作。如果找不到 Windows 凭据，则查询 UDS 或本地文件来查找 UID 的名称。然后，该名称（也可以通过 ntxmap）用于查找 Windows 用户，同时，从 Windows DC 或 LGDB 检索凭据。如果未找到映射，系统将转为使用默认 Windows 用户的 Windows 凭据，或者访问将被拒绝。

了解 Common AntiVirus Agent (CAVA)

Common AntiVirus Agent (CAVA) 使用 NAS 服务器向客户端提供防病毒解决方案。它在 Microsoft Windows Server 环境中使用符合行业标准的 SMB 协议。CAVA 使用第三方防病毒软件在已知的病毒感染存储系统上的文件之前，识别并消除它们。

防病毒为什么很重要？

存储系统可凭借其体系结构抵御病毒入侵。NAS 服务器使用嵌入式操作系统实时运行数据访问。第三方无法在此操作系统上运行包含病毒的程序。尽管操作系统软件可抵御病毒，但是访问存储系统的 Windows 客户端也需要病毒防护。客户端上的病毒防护可减少客户端在服务器上存储受感染文件的机会，并可在客户端打开受感染文件时提供保护。此防病毒解决方案组合了操作系统软件、CAVA 代理和第三方防病毒引擎。CAVA 软件和第三方防病毒引擎必须安装在域中的 Windows 服务器上。

有关 CAVA（属于 Common Event Enabler (CEE) 的一部分）的其他信息，请参阅 *Using the Common Event Enabler on Windows Platforms*，网址为 www.dell.com/powerstoredocs。

代码签名

PowerStore 设计为可接受新版本和修补程序版本的软件升级。主要 GNU 隐私保护 (GPG) 密钥用于签署所有 PowerStore 软件包，并由 Dell EMC 控制此 GPG 密钥。PowerStore 软件升级过程会验证软件包的签名，并拒绝可能被篡改或损坏的无效签名。验证步骤内置于升级过程中，在预安装阶段会自动验证软件包的签名。

2

通信安全设置

本节包括以下主题：

主题：

端口使用情况

以下部分概括介绍了可在设备中找到的网络端口及相应服务的集合。一体机在多种情况下（例如与 vCenter Server 通信）可充当网络客户端。在这些情况下，一体机会启动通信，网络基础架构需要支持这些连接。

注: 有关端口的其他信息，请参阅知识库文章 542240，*PowerStore：客户网络防火墙规则 — TCP/UDP 端口*。转至 https://www.dell.com/support/kbdoc/en-us/542240。客户网络防火墙规则工具可让您筛选和查看与 PowerStore 部署相关的防火墙规则和端口的列表。

设备网络端口

下表概括介绍了可在设备中找到的网络端口及相应服务的集合。

表. 2: 设备网络端口

端口	服务	协议	访问方向	描述
22	SSH 客户端，SupportAssist Connect Home	TCP	双向	• 允许 SSH 访问（如果已启用）。 • SupportAssist Connect Home 需要。 如果关闭，则使用 SSH 的管理连接将不可用。
25	SMTP	TCP	出站	允许设备发送电子邮件。如果关闭，电子邮件通知将不可用。
26	SSH 客户端	TCP	双向	对端口 22 的 SSH 访问将重定向到此端口。如果关闭，则使用 SSH 的管理连接将不可用。
53	DNS	TCP/UDP	出站	用于将 DNS 查询传输到 DNS 服务器。如果关闭，DNS 名称解析将不可用。
80、8080、8128	SupportAssist	TCP	出站	用于 SupportAssist 代理连接。
123	NTP	TCP/UDP	出站	NTP 时间同步。如果关闭，设备之间的时间将不同步。
443	HTTPS	TCP	双向	保护到 PowerStore Manager 的 HTTP 流量。如果关闭，与设备的通信将不可用。
500	IPsec (IKEv2)	UDP	双向	要使 IPSec 能够通过防火墙工作，请打开 UDP 端口 500，并在入站和出站防火墙筛选器上允许 IP 协议编号 50 和 51。应打开 UDP 端口 500，以允许通过防火墙转发 Internet 安全联盟密钥管理协议 (ISAKMP) 流量。IP 协议 ID 50 应该设置为允许转发 IPSec 封装安全协议 (ESP) 流量。IP 协议 ID

表. 2: 设备网络端口（续）

端口	服务	协议	访问方向	描述
				51 应该设置为允许转发验证头 (AH) 流量。如果关闭，则 PowerStore 设备之间的 IPsec 连接将不可用。
587	SMTP	TCP	出站	允许设备发送电子邮件。如果关闭，电子邮件通知将不可用。
3033	导入	TCP/UDP	出站	从传统 EqualLogic 对等存储和 Compellent Storage Center 系统进行存储导入时需要。
3260	iSCSI	TCP	• 入站，用于主机和 ESXi 主机访问 • 双向，用于复制 • 出站，用于存储导入	提供对 iSCSI 服务的以下访问权限时需要： • 外部主机 iSCSI 访问 • 外部或 PowerStore 嵌入式 ESXi 主机 iSCSI 访问 • 群集间的访问，用于复制 • 从传统 EqualLogic 对等存储、Compellent Storage Center、Unity 和 VNX2 系统进行存储导入访问 如果关闭，iSCSI 服务将不可用。由数据移动性用于支持在低延迟连接上实现合理的复制性能。
3261	数据移动性	TCP	双向	由数据移动性用于支持在高延迟连接上实现合理的复制性能。
5353	多播 DNS (mDNS)	UDP	双向	多播 DNS 查询。如果关闭，mDNS 名称解析将不工作。
8443	VASA、SupportAssist	TCP	• 入站，VASA • 出站，SupportAssist	• VASA 3.0 的 VASA 提供程序需要。 • 相关 SupportAssist Connect Home 功能需要。
8443、50443、55443 或 60443	Windows 导入主机代理、Linux 导入主机代理或 VMware 导入主机代理	TCP	出站	从传统存储系统导入数据存储时，必须打开这些端口中的一个。
9443	SupportAssist	TCP	出站	与 Connect Home 相关的 SupportAssist REST API 需要。

与文件相关的设备网络端口

下表概括介绍了可在设备中找到的与文件相关的网络端口及相应服务的集合。

注: 出站端口是瞬时的。

表. 3: 与文件相关的设备网络端口

端口	服务	协议	访问方向	描述
20	FTP	TCP	出站	端口用于 FTP 数据传输。通过启用 FTP 可打开此端口。身份验证可在端口 21 上执行，并按照 FTP 协议进行定义。
21	FTP	TCP	入站	端口 21 是控制端口，FTP 服务可在其上侦听传入的 FTP 请求。
22	SFTP	TCP	入站	允许通过 SFTP (FTP over SSH) 发送警报通知。SFTP 是一种客户端/服务器协议。用户可以使用 SFTP 在本地子网上的设备上执

表. 3: 与文件相关的设备网络端口（续）

端口	服务	协议	访问方向	描述
				行文件传输。还提供传出 FTP 控制连接。如果关闭，FTP 将不可用。
53	DNS	TCP/UDP	出站	用于将 DNS 查询传输到 DNS 服务器。如果关闭，DNS 名称解析将不可用。SMB v1 需要。
88	Kerberos	TCP/UDP	出站	Kerberos 身份验证服务需要。
111	RPC 绑定（对于 SDNAS 命名空间；否则为主机服务）	TCP/UDP	双向	由标准 portmapper 或 rpcbind 服务打开，是一项设备辅助网络服务。不能停止它。按照定义，如果客户端系统与此端口具有网络连接，即可进行查询。不执行任何身份认证。
123	NTP	UDP	出站	NTP 时间同步。如果关闭，设备之间的时间将不同步。
135	Microsoft RPC	TCP	入站	MicroSoft 客户端的多个用途。也用于 NDMP。
137	Microsoft Netbios WINS	UDP；TCP/UDP	入站和出站	NETBIOS 名称服务与设备的 SMB 文件共享服务关联，并且是该功能 (Wins) 的核心组件。如果禁用，则此端口会禁用所有与 SMB 相关的服务。
138	Microsoft Netbios 浏览	UDP	出站	NETBIOS 数据报服务与设备的 SMB 文件共享服务关联，并且是该功能的核心组件。仅使用浏览服务。如果禁用，此端口将禁用浏览功能。
139	Microsoft CIFS	TCP	双向	NETBIOS 会话服务与设备 SMB 文件共享服务相关联，并且是该功能的核心组件。如果启用了 SMB 服务，则此端口开放。SMB v1 特别要求。
389	LDAP	TCP/UDP	出站	非安全 LDAP 查询。如果关闭，非安全 LDAP 身份认证查询将不可用。可将安全 LDAP 配置为替代项。
445	Microsoft SMB	TCP	入站	用于 Windows 2000 和更高版本客户端的 SMB（在域控制器上）和 SMB 连接端口。对设备 SMB 服务具有合法访问权限的客户端必须与端口建立网络连接才能继续操作。禁用此端口将禁用所有与 SMB 相关的服务。如果也禁用端口 139，则将禁用 SMB 文件共享。
464	Kerberos	TCP/UDP	出站	Kerberos 身份验证服务和 SMB 需要。
500	IPsec (IKEv2)	UDP	双向	要使 IPSec 能够通过防火墙工作，请打开 UDP 端口 500，并在入站和出站防火墙筛选器上允许 IP 协议编号 50 和 51。应打开 UDP 端口 500，以允许通过防火墙转发 Internet 安全联盟密钥管理协议 (ISAKMP) 流量。IP 协议 ID 50 应该设置为允许转发 IPSec 封装安全协议 (ESP) 流量。IP 协议 ID 51 应该设置为允许转发验证头 (AH) 流量。如果关闭，则 PowerStore 设备之间的 IPsec 连接将不可用。
636	LDAPS	TCP/UDP	出站	安全 LDAP 查询。如果关闭，安全 LDAP 身份认证将不可用。

表. 3: 与文件相关的设备网络端口（续）

端口	服务	协议	访问方向	描述
1234	NFS mountd	TCP/UDP	双向	用于装载服务，是 NFS 服务（版本 2、3 和 4）的核心组件。
2000	SSHD	TCP	入站	SSHD，用于可服务性（可选）
2049	NFS I/O	TCP/UDP	双向	用于提供 NFS 服务。
3268	LDAP	UDP	出站	非安全 LDAP 查询。如果关闭，非安全 LDAP 身份认证查询将不可用。
4000	STATD for NFSv3	TCP/UDP	双向	用于提供 NFS statd 服务。statd 是 NFS 文件锁定状态监视器，且与 lockd 结合使用，为 NFS 提供崩溃和恢复功能。如果关闭，则 NAS statd 服务将不可用。
4001	NLMD for NFSv3	TCP/UDP	双向	用于提供 NFS lockd 服务。lockd 是 NFS 文件锁定守护程序。它可以处理来自 NFS 客户端的锁定请求，并与 statd 守护程序一起运行。如果关闭，则 NAS lockd 服务将不可用。
4002	RQUOTAD，用于 NFSv3	TCP/UDP；UDP	入站和出站	用于提供 NFS rquotad 服务。rquotad 守护程序向装载了文件系统的 NFS 客户端提供配额信息。如果关闭，则 NAS rquotad 服务将不可用。
4003	XATTRPD（扩展文件属性）	TCP/UDP	入站	在多协议环境中管理文件属性时需要。
4658	PAX（NAS 服务器归档）	TCP	入站	PAX 是一种设备归档协议，与标准 UNIX 磁带格式配合使用。
8888	RCPD（复制数据路径）	TCP	入站	由复制器使用（在次端）。当需要复制某些数据时，Replicator 会将其打开。启动之后，无法停止此服务。
10000	NDMP	TCP	入站	• 使您可通过网络备份应用程序控制网络数据管理协议 (NDMP) 服务器的备份和恢复，无需在服务器上安装第三方软件。在设备中，NAS 服务器充当 NDMP 服务器。 • 如果未使用 NDMP 磁带备份，NDMP 服务可处于禁用状态。 • NDMP 服务使用用户名/密码对进行身份认证。用户名可配置。NDMP 文档介绍了如何针对各种环境配置密码。
[10500,10531]	NDMP 动态端口的 NDMP 保留范围	TCP	入站	对于三向备份/恢复会话，NAS 服务器使用端口 10500 到 10531。
12228	防病毒检查程序服务	TCP	出站	防病毒检查程序服务需要。

与 PowerStore X 型号设备相关的网络端口

下表概括介绍了可在 PowerStore X model 设备上找到的网络端口及相应服务的集合。

表. 4: 与 PowerStore X model 设备相关的网络端口

端口	服务	协议	访问方向	描述
22	SSH 服务器	TCP	入站	允许 SSH 访问（如果已启用）。如果关闭，则使用 SSH 的管理连接将不可用。
80、9000	vSphere Web Access	TCP	入站	vSphere Web Client 的 vSphere Update Manager Web Client 插件的访问权限。
427	CIM 服务定位协议 (SLP)	TCP/UDP	双向	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。
443	vSphere Web Client	TCP	入站	用于客户端连接。
902	网络文件拷贝 (NFC)、VMware vCenter、vSphere Web Client	TCP	• 双向，用于 NFC • 出站，用于 VMware vCenter • 入站，用于 vSphere Web Client	• NFC 为 vSphere 组件提供可识别文件类型的 FTP 服务。默认情况下，ESXi 使用 NFC 执行操作，例如在数据存储之间复制和移动数据。 • VMware vCenter 代理 • 对于 vSphere Web Client，用于客户端连接。
5900、5901、5902、5903、5904	RFB 协议	TCP	入站	对诸如 VNC 等图形用户界面的远程访问。
5988	通用信息模型 (CIM) 服务器	TCP	入站	用于 CIM 的服务器。
5989	CIM 安全服务器	TCP	入站	用于 CIM 的服务器。
6999	NSX 虚拟分布式逻辑路由器，rabbitmqproxy	UDP	• 双向，用于 NSX 虚拟分布式路由器服务 • 出站，用于 Rabbitmqproxy	• 对于 NSX 虚拟分布式路由器服务，如果安装了 NSX VIB 并创建了 VDR 模块，与此服务关联的防火墙端口将打开。如果没有与主机关联的 VDR 实例，则无需打开该端口。 • 对于 rabbitmqproxy，ESXi 主机上运行着一个代理。此代理允许在虚拟机内部运行的应用程序与 vCenter 网络域中运行的 AMQP 代理进行通信。虚拟机不必位于网络中，即不需要 NIC。确保传出连接 IP 地址至少包含正在使用或将来的代理。您可以稍后添加代理，进行纵向扩展。
8000	vMotion	TCP	双向	使用 vMotion 执行虚拟机迁移时必需。ESXi 主机侦听端口 8000 的 TCP 连接，获取远程 ESXi 主机的 vMotion 流量。
8100、8200、8300	容错	TCP/UDP	双向	用于 vSphere Fault Tolerance (FT) 主机之间的流量。
8301、8302	DVSSync	UDP	双向	DVSSync 端口用于同步已启用 VMware FT 记录/重播的主机之间的分布式虚拟端口的状态。只有运行主要或备份虚拟机的主机才必须打开这些端口。在不使用 VMware FT 的主机上，这些端口无需打开。
9080	I/O 筛选器	TCP	出站	由 I/O 筛选器存储功能使用。
31031	vSphere 复制，VMware Site Recovery Manager	TCP	出站	用于 vSphere Replication 和 VMware Site Recovery Manager 的日常复制流量。
44046	vSphere 复制，VMware Site Recovery Manager	TCP	出站	用于 vSphere Replication 和 VMware Site Recovery Manager 的日常复制流量。

3

审核

本章包含以下信息：

主题：

审核

审核提供了系统上用户活动的历史视图。具有管理员、安全管理员或存储管理员角色的用户，可以使用 REST API 在系统中搜索和查看配置更改事件。这些被审核的事件不仅与安全相关，所有设置操作（即 POST/PATCH/DELETE）都会进行审核记录。

其他界面（例如 PowerStore Manager UI 和 CLI）可用于搜索和查看审核事件。

4

数据安全设置

本节包括以下主题：

主题：

静态数据加密

PowerStore 中的静态数据加密 (D@RE) 将经过 FIPS 140-2 验证的自加密驱动器 (SED) 用作主存储（NVMe SSD、NVMe SCM 和 SAS SSD）。NVRAM 高速缓存设备已加密，但目前未经 FIPS 140-2 验证。

加密是在每个驱动器内在数据写入到该介质之前执行的。这样可针对驱动器被盗或丢失 — 以及通过物理解构驱动器来直接读取驱动器的企图 — 来为驱动器上的数据提供保护。加密还提供了一种快速、安全地擦除驱动器上的信息以确保信息无法恢复的方法。除了针对介质实体移除伴有的威胁提供保护之外，通过销毁用于保护介质上之前存储的数据的加密密钥，还可随时重新调整介质的用途。

读取加密数据需要用 SED 的身份验证密钥来解锁驱动器。只有经过身份验证的 SED 才能解锁并访问。驱动器解锁以后，SED 会将加密数据解密回其原始形式。

PowerStore 设备必须全部使用 SED。如果您尝试将非自加密驱动器添加到设备，该设备会出现错误。此外，不支持在加密群集中部署未加密的设备。

加密激活

PowerStore 一体机上的静态数据加密功能是在出厂时设置的。在所有允许进口支持加密的一体机的国家/地区，加密功能是默认启用的。若已启用，将不能禁用加密功能。在所有不允许进口支持加密的一体机的国家/地区，将禁用静态数据加密功能。

注: 不支持静态数据加密的一体机不允许加入由加密一体机组成的群集。

加密状态

将在以下级别报告一体机的加密状态：

- 群集级别
- 一体机级别
- 驱动器级别

群集级别的加密状态只反映一体机是否已启用加密。它与驱动器状态无关。

一体机的加密状态显示为以下之一：

- Encrypted — 该一体机上启用了加密功能。
- Unencrypted — 该一体机不支持加密功能。
- Encrypting — 在加密激活过程中显示。加密过程成功完成后，群集级别的加密状态会显示为“Encrypted”。

提供了一体机中的每个驱动器的驱动器级别加密状态，显示为下列各项之一：

- Encrypted — 驱动器已加密。这是一体机中的驱动器的典型状态，能够执行加密。
- Encrypting — 一体机正在该驱动器上启用加密。在一体机上的初始激活加密或将新驱动器添加到配置的一体机期间，可以看到此状态。
- Disabled — 由于特定于国家/地区的进口限制，驱动器不能启用加密。如果任何驱动器报告此状态，则群集中的所有驱动器也将报告相同的状态。
- Unknown — 一体机尚未尝试在驱动器上启用加密。在一体机上的初始激活加密或将新驱动器添加到配置的一体机期间，可以看到此状态。
- Unsupported — 该驱动器不支持加密。
- Foreign — 该驱动器支持加密，但已经被另一个一体机锁定。它需要先解除锁定，然后才能使用。

密钥管理

在每个 PowerStore 设备的活动节点上运行着一项嵌入式密钥管理器服务 (KMS)。此服务管理着本地密钥库文件密码箱存储，以支持将密钥自动加密备份到系统和引导驱动器。它还控制设备上的自加密驱动器 (SED) 锁定和解锁过程，并负责管理设备的本地密钥库内容。本地密钥库文件使用一个 256 位 AES 密钥加密，密钥库文件密码箱存储利用 RSA 的 BSAFE 技术。

在设备初始化期间，KMS 会自动为 SED 生成随机身份验证密钥。每个驱动器（包括稍后添加到设备的那些）都有一个唯一的身份验证密钥，在 SED 锁定和解锁过程中使用。密钥加密密钥将加密密钥库文件存储中、以及在设备内传输的身份验证和加密密钥。介质加密密钥存储在 SED 专用硬件上，而且无法访问。启用加密时，所有身份验证密钥均存储在设备中。

密钥库备份文件

KMS 支持创建和下载脱离设备的密钥库归档文件备份。脱离设备的备份可减少密钥丢失这种灾难事件的发生可能性，密钥丢失会导致一个设备或整个群集不可用。如果在启动群集密钥库备份时某个特定的设备不可用，总体操作将会成功完成，但会发出一条警告，指出备份并未包含群集中全部设备的密钥库文件，应在离线的设备可用时重试此操作。

注: 群集中的主设备包含群集密钥库归档文件，其中包含在群集中发现的每个设备（包括主设备）的密钥库备份拷贝。

当对群集内一个系统的配置的更改导致更改了密钥库时，建议您生成新的密钥库归档文件供下载。每次只能运行一个密钥库归档文件的备份下载操作。

注: 极力议您将生成的密钥库归档文件下载到外部一个安全的位置。如果一个系统上的密钥库文件损坏并且无法访问，则该系统将进入服务模式。此时，需通过密钥归档文件和一次支持服务来解决问题。

备份密钥库归档文件需要具备管理员或存储管理员用户角色。要备份密钥库归档文件，请单击 **Settings**，并在 **Security** 下选择 **Encryption**。在 **Encryption** 页面上，在 **Lockbox Backup** 之下单击 **Download Keystore Backup**。

注: 要在发生故障时恢复密钥库备份，请联系您的服务提供商。

在启用加密的设备中重新调整驱动器用途

关于此任务

自加密驱动器 (SED) 在设备初始化时或者在插入到一个已经初始化的设备中时将被锁定。在没有先解锁的情况下，无法在另一个系统中使用该驱动器。当锁定的驱动器插入到另一不同的设备中时，其加密状态在新设备中显示为 `Foreign`。可针对新设备重新调整该驱动器的用途，但驱动器上的所有现有数据都将丢失。

要将设备上加密状态显示为 `Foreign` 的驱动器重新调整用途，请执行以下操作：

步骤

1. 记录位于驱动器背面标签上的 PSID（物理安全性 ID）。在重新调整用途过程中必须提供 PSID。
2. 在 PowerStore Manager 中，单击 **Hardware**，选择该设备，然后选择 **Hardware** 卡。
3. 选择要重新调整用途的驱动器。
   该驱动器的 **Encryption Status** 应显示为 `Foreign`。
4. 单击 **Repurpose Drive**。
   Repurpose Drive 滑轨即出现。

5. 键入驱动器的 PSID，然后单击 **Apply**。

结果

该驱动器在设备中重新调整为一个新的驱动器，并且其加密状态会在重新调整用途过程完成后更改为 `Encrypted`。

从启用加密的系统更换基本存储模块和节点

需要一次服务活动，来从启用了加密的设备中更换 base enclosure 和 nodes。

将设备重置为出厂设置

`svc_factory_reset` 这一服务脚本将把单一设备群集恢复到出厂时的状态，删除所有用户数据和持久性配置。

对于多设备群集，`svc_factory_reset` 不能在辅助设备上运行。必须运行 `svc_remove_appliance` 服务脚本。此脚本会将辅助设备恢复到出厂时的状态，删除所有用户数据和持久性配置。当只有主设备保留在群集中时，您可以运行 `svc_factory_reset` 重置该设备。

注: 建议仅由合格的服务提供商运行这些脚本。

有关这些脚本的详细信息，请参阅 *PowerStore Service Scripts Guide*。

5

安全可维护性设置

本章包含以下信息：

主题：

操作说明 SupportAssist™

SupportAssist 功能提供基于 IP 的连接，使 Dell EMC 支持部门可以从您的设备接收错误文件和警报，并执行远程故障排除，从而快速高效地解决问题。

注: 强烈建议启用 SupportAssist 功能以加快问题诊断、执行故障排除和帮助加快问题解决速度。如果不启用 SupportAssist 功能，则可能需要手动收集设备信息，以协助 Dell EMC 支持部门对设备进行故障排除并解决问题。另外，必须在设备上启用 SupportAssist 功能，才能将数据发送到 CloudIQ。有关 CloudIQ 的信息，请访问 www.dell.com/support。登录后，找到 CloudIQ **Product Support** 页面。

SupportAssist 和安全性

SupportAssist 功能在远程连接过程中的每一步都采用多个安全层，以确保您和 Dell EMC 可放心使用该解决方案：

- 所有发送到 Dell EMC 的通知均来自您的站点而从不来自外部来源，并使用高级加密标准 (AES) 256 位加密确保其安全。
- 基于 IP 的体系结构与您现有的基础架构相集成，让您所处的环境保持安全。
- 您的站点与 Dell EMC 之间的通信使用 RSA® 数字证书进行双向身份验证。
- 只有通过双因素身份验证的授权 Dell EMC 客户服务专员可下载数字证书，需要这些数字证书才能查看来自您的站点的通知。
- 通过可选的 SupportAssist v3 策略管理器应用程序，您可以根据您自己独有的准则和要求允许或禁止 Dell EMC 支持人员进行访问，并且该应用程序还包括详细的审核日志。

SupportAssist 管理

您可以使用 PowerStore Manager 或 REST API 管理 SupportAssist 功能。您可以启用或禁用该服务，并提供所选 SupportAssist 选项所需的相关信息。

注: 集中 SupportAssist 的 **Gateway Connect with remote assist** 和 **Gateway Connect without remote assist** 选项不支持高可用性 (HA)。这些选项不提供故障切换到活动的 HA SupportAssist 群集的功能。当 PowerStore 设备部署到单个 HA 网关群集服务器（唯一可用的配置选项）时，将没有向群集中的幸存网关服务器进行故障切换的功能。如果设备连接到的 HA 网关服务器发生故障，则设备将停止向 Dell EMC 支持部门传输任何出站文件（例如 CloudIQ 文件）。用于对设备进行远程访问的 SupportAssist 入站连接仍将使用群集中的幸存 HA 网关服务器继续发挥作用。此外，只应在您的系统中指定的主设备上配置 SupportAssist **Gateway Connect with remote assist** 和 **Gateway Connect without remote assist** 选项。

设备本身并不实施任何策略。如果要对您的设备的远程访问进行更多的控制，您可以使用策略管理器来设置授权权限。Policy Manager 软件组件可以安装在客户提供的服务器上。它控制对设备的远程访问，维护远程连接的审核日志，并支持文件传输操作。

您可以控制哪些用户在何时访问设备的哪些内容。有关策略管理器的详细信息，请访问 www.dell.com/support。登录后，找到适用的 **Support by Product** 页面，然后搜索到特定 SupportAssist 产品技术文档的链接。

SupportAssist 通信

注: 在使用 IPv6 配置管理网络的 PowerStore 型号上无法启用 SupportAssist。SupportAssist 不支持 IPv6。此外，如果在群集上配置了 SupportAssist，则不允许将管理网络从 IPv4 重新配置到 IPv6。

SupportAssist 功能要正常发挥作用，需要拥有对 DNS 服务器的访问权限。

SupportAssist 的 **Connection Status** 提示 PowerStore 与 Dell EMC 后端支持服务之间的连接状态，以及连接的服务质量。连接状态可在五分钟内确定，连接的服务质量可在 24 小时内确定。连接的 **Connection Status** 可显示为以下之一（取决于群集中的任何设备）：

- `Unavailable` — 连接数据不可用。您可能失去了与设备的联系，或由于 SupportAssist 刚刚启用，导致数据不足以确定状态。
- `Disabled` — SupportAssist 尚未启用。
- `Not connected` — 连接已丢失。检测到五个连续的 keepalive 故障。
- `Reconnecting` — 连接中断后 PowerStore 尝试重新连接。需要五个连续的成功 keepalive 请求，才能变回连接状态。

当 PowerStore 连接到 Dell EMC 后端支持服务时，连接的 **Connection Status** 可显示为以下之一（取决于群集中所有设备的平均值）：

- `Evaluating` — 首次初始化 SupportAssist 后的前 24 小时内，无法确定连接的服务质量。
- `Good` — 80% 或更多连续的 keepalive 请求已成功。
- `Fair` — 连续 keepalive 请求的成功率在 50% 至 80% 之间。
- `Poor` — 连续 keepalive 请求的成功率少于 50%。

SupportAssist 选项

SupportAssist 功能提供基于 IP 的连接，使 Dell EMC 支持部门可以从您的系统接收错误文件和警报，并执行远程故障排除，从而快速高效地解决问题。

将设备信息发送至 Dell EMC 支持部门，以便执行远程故障排除的 SupportAssist 选项包括：

- Gateway Connect without remote access — 用于集中 SupportAssist，并在客户提供的支持双向文件传输的网关服务器上运行，其中包括：
  - Call-home
  - CloudIQ 支持
  - 软件通知
  - 从 Dell EMC 支持部门将操作环境/固件下载到群集

  SupportAssist 网关服务器是与该网关关联设备的所有基于 IP 的 SupportAssist 活动的单一出入口。
- Gateway Connect with remote access — 用于集中 SupportAssist，并在客户提供的支持与“Gateway Connect without remote access”相同的双向文件传输的网关服务器上运行，还允许 Dell EMC 支持人员进行远程访问。
- Direct Connect without remote access — 用于在单个设备上运行的分布式 SupportAssist，这些设备具有与 Gateway Connect 相同的双向文件传输，不允许远程访问。
- Direct Connect with remote access — 用于在单个设备上运行的分布式 SupportAssist，这些设备具有与采用“Gateway Connect without remote access”选项的设备一样的双向文件传输，还允许 Dell EMC 支持人员进行远程访问。

另一个选项“已禁用”虽然可用，但不推荐使用。如果您选择该选项，则 Dell EMC 不会收到与该设备的问题有关的通知。可能需要手动收集设备信息以帮助支持代表排除和解决设备的问题。

SupportAssist Gateway Connect 选项

SupportAssist Gateway Connect 运行在网关服务器上。当您选择 **Gateway Connect without remote access** 选项或 **Gateway Connect with remote access** 选项时，您的设备将添加到 SupportAssist 群集中的其他设备。群集驻留在 Dell EMC 支持服务器和一个脱离阵列的网关服务器之间的单个通用（集中式）安全连接背后。网关服务器是与该网关关联的设备的所有基于 IP 的 Dell EMC SupportAssist 活动的单一出入口。

网关服务器是一种远程支持解决方案应用程序，安装在一个或多个客户提供专用服务器上。网关服务器充当关联设备与 Dell EMC 企业之间的通信代理。

有关 SupportAssist 网关的详细信息，请访问戴尔支持网站 (www.dell.com/support) 上的 SupportAssist 产品页面。

要将您的设备配置为使用 SupportAssist 的 **Gateway Connect without remote access** 选项或 **Gateway Connect with remote access** 选项，您需要提供网关服务器的 IP 地址和端口号（默认值为 9443）。此外，请确保网关服务器与设备之间的端口处于打开状态。

注: 网关服务器必须处于正常运行状态，然后才能将设备配置为使用它。只能从 PowerStore Manager 中将设备添加到网关。如果从网关服务器中添加设备，则它看上去已连接，但无法成功发送系统信息。

SupportAssist Direct Connect 选项

SupportAssist Direct Connect 直接在每个设备的主节点上运行。在群集中，每个设备将建立其自己的到 Dell EMC 支持部门的连接。流量不通过群集中的主设备进行路由。但是，SupportAssist 只能在群集级别进行管理，即所有更改都将应用于群集中的每个设备。

在 **Support Assist** 页面上启用并配置 SupportAssist Direct Connect，可通过 PowerStore Manager 中的 **Settings** 访问该页面，它在 **Support** 下列出。这些操作将设置设备，在其自身与 Dell EMC 支持部门之间使用安全连接。可以为 SupportAssist Direct Connect 选择以下远程服务连接选项之一：

- **Direct Connect without remote access**
- **Direct Connect with remote access**

当您选择 **Direct Connect without remote access** 选项并接受最终用户许可协议 (EULA) 时，设备将在其自身与 Dell EMC 支持部门之间建立安全的连接。此选项可实现与 Dell EMC 支持部门之间的双向文件传输连接功能。如适用，您可以配置从设备到关联的代理服务器的连接（可选）。如有必要，您可以以后升级到设置了远程访问配置的 Direct Connect 模式。

当您选择 **Direct Connect with remote access** 选项并接受最终用户许可协议 (EULA) 时，设备将在其自身与 Dell EMC 支持部门之间建立安全的连接。此选项可实现设备与 Dell EMC 支持部门之间的双向远程访问服务连接功能，以及双向文件传输。如果适用，您可以通过 PowerStore Manager 来配置从设备到策略管理器（可选）以及任何关联的代理服务器（可选）的连接。

将新设备添加到现有群集后，新设备将检测群集 SupportAssist 设置，并自动配置新设备以进行匹配。如果当前已启用 SupportAssist Direct Connect，它将在新设备上自动启用，无需执行其他操作。如果无法启用 SupportAssist Direct Connect，也不会使添加设备的过程无法完成。

针对 SupportAssist Gateway Connect 的要求

以下要求同时适用于 **Gateway Connect without remote access** 和 **Gateway Connect with remote access** 这两种 SupportAssist 实现方案：

- 在设备与 SupportAssist 网关服务器之间的端口 9443（或客户指定的另一不同端口）上必须允许网络流量 (HTTPS)。
- SupportAssist 必须为版本 4.0.5 或版本 3.38。

注: 切勿手动向网关服务器添加或从中删除一体机。请仅使用 PowerStore Manager SupportAssist 配置向导向网关服务器添加或从中删除设备。

针对 SupportAssist Direct Connect 的要求

以下要求同时适用于 **Direct Connect without remote access** 和 **Direct Connect with remote access** 这两种 SupportAssist 实现方案：

- 必须在端口 443 和 8443（出站）上允许通向 Dell EMC 支持部门的网络流量 (HTTPS)。未能打开 8443 端口将严重影响性能（30% 至 45%）。未能同时打开这两个端口可能会导致推迟解决终端设备的问题。

以下要求仅适用于 **Direct Connect with Remote Access** SupportAssist 实现方案：

- 如果您的实现方案将包括策略管理器，来对设备的远程访问实现更多控制，则必须在配置 SupportAssist 功能时指明。

配置 SupportAssist

您可以使用以下任一方法为设备配置 SupportAssist：

- 初始配置向导 — 一个用户界面，可引导您完成 PowerStore Manager 初始设置，并准备系统以供使用。

- **Suppoprt Assist** — 一个您可以从 PowerStore Manager 中访问的设置页面（单击 **Settings**，在 **Support** 下选择 **SupportAssist**）。
- REST API 服务器 — 可以接收配置 SupportAssist 设置的 REST API 请求的应用程序接口。有关 REST API 的更多信息，请参阅 PowerStore REST API Reference Guide。

要确定 SupportAssist 功能的状态，请在 PowerStore Manager 中单击 **Settings**，然后在 **Support** 下选择 **SupportAssist**。

配置 SupportAssist

关于此任务

要使用 PowerStore Manager 配置 SupportAssist，请执行以下操作：

注: 将 **Direct Connect with remote access** 选项更改为 **Direct Connect without remote access** 或 **Gateway Connect** 选项要求 Dell EMC 支持人员提供协助。

步骤

1. 单击 **Settings**，然后在 **Support** 下选择 **SupportAssist**。
2. 如果 SupportAssist 的状态显示为已禁用，请单击 **SupportAssist** 控件图标以启用 SupportAssist。
   虽然可以禁用 SupportAssist 功能，但不建议这样做。
   按钮应移至右侧，指示将更改为 `Enabled`。但是，在您输入所需的配置信息并单击 **Apply** 后，**Connection Status** 才会更改。
3. 在 **SupportAssist** 下，**Connect to CloudIQ** 复选框默认处于选中状态；如果您不想将文件发送到 CloudIQ，请清除该复选框；否则，请让它保留选中状态。
4. 从列表中选择要使用的 SupportAssist 选项的 **Type**。
5. 根据您选择的 SupportAssist 选项类型，执行以下操作之一：
   - 对于 **Gateway Connect without remote access** 或 **Gateway Connect with remote access** 选项：
     - 指定网关服务器的 IP 地址。
       注: 网关服务器必须处于正常运行状态，然后才能将设备配置为使用它。
     - 如果将用于连接到网关服务器的端口不是默认的 9443，请使用控件来选择您的网络中将使用的端口号。
   - 对于 **Direct Connect without remote access** 选项：
     - 如果您的网络连接使用代理服务器，请指定代理服务器的 IP 地址。
       注: 代理服务器必须处于正常运行状态，然后才能将系统配置为使用它。
     - 使用控件选择将用于连接到网络中的代理服务器的端口号。
   - 对于 **Direct Connect With Remote Access** 选项：
     - 如果您的网络连接使用代理服务器，请指定代理服务器的 IP 地址。
       注: 代理服务器必须处于正常运行状态，然后才能将设备配置为使用它。
     - 使用控件选择将用于连接到网络中的代理服务器的端口号。
     - 如果要使用策略管理器来控制对系统的远程访问，请指定策略管理器的 IP 地址。
       注: 策略管理器必须处于正常运行状态，然后才能将设备配置为使用它。
     - 如果将用于连接到策略管理器的端口不是默认的 9443，请键入您网络中将使用的端口号。
6. 根据您选择的 SupportAssist 选项类型，执行以下操作之一：
   - 对于 **Direct Connect without remote access** 或 **Direct Connect with Remote Access** 选项，转到下一步。
   - 对于 **Gateway Connect without remote access** 或 **Gateway Connect with Remote Access** 选项，选择 **Test Connection** 检查与网关服务器的连接状态。

   注: 如果“Connectivity Status”仍显示为 `Transitioning`，并且几分钟（测试连接性应花费的时间）后仍无变化，请与在线支持人员联系。
7. 选择 **Send Test alert** 将测试警报发送到 Dell EMC 支持部门以确保端到端连接。
8. 确保显示的联系人信息准确无误。纠正任何显示错误或过时的信息。
   您的 SupportAssist 联系信息对于支持问题的快速响应至关重要，必须准确且最新。
9. 选择 **Apply** 以保留 SupportAssist 配置信息。

A

TLS 加密套件

本附录包含以下信息：

主题：

支持的 TLS 加密套件

加密套件定义了一组用于保护您的 TLS 通信的技术：

- 密钥交换算法（用于加密数据的密钥如何从客户端传递到服务器）。示例：RSA 密钥或 Diffie-Hellman (DH)
- 身份验证方法（主机如何验证远程主机的身份）。示例：RSA 证书、DSS 证书或无身份验证
- 加密方法（如何加密数据）。示例：AES（256 位或 128 位）
- 哈希算法（通过提供确定是否数据已修改的方式来保护数据）。示例：SHA-2 或 SHA-1

支持的加密套件融合了所有这些项。

下表给出了设备 TLS 密码套件的 OpenSSL 名称以及关联的端口。

表. 5: 设备上默认/支持的 TLS 密码套件

加密套件	协议	端口
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443、8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443、8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443、8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443、8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443、8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443、8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443、8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443、8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443、8443