



iSCSI 设置

E-Series storage systems

NetApp
January 20, 2026

目录

- iSCSI 设置 1
 - 验证E系列(iSCSI)中的Linux配置支持 1
 - 在E系列- Linux (iSCSI)中使用DHCP配置IP地址 1
 - 安装适用于SMCli的SANtricity Storage Manager (11.53或更早版本)- Linux (iSCSI) 2
 - 使用SANtricity系统管理器- Linux (iSCSI)配置存储 3
 - 在E系列- Linux (iSCSI)中配置多路径软件 4
 - 在E系列- Linux (iSCSI)中设置多路径.conf文件 5
 - 在E系列- Linux (iSCSI)中配置交换机 6
 - 在E系列- Linux (iSCSI)中配置网络 6
 - 在E系列- Linux (iSCSI)中配置阵列端网络 6
 - 在E系列- Linux (iSCSI)中配置主机端网络 8
 - 验证E系列- Linux (iSCSI)中的IP网络连接 12
 - 在E系列中创建分区和文件系统- Linux (iSCSI) 13
 - 验证E系列- Linux (iSCSI)主机上的存储访问 15
 - 在E系列- Linux中记录iSCSI配置 15
 - 建议的配置 15
 - 目标 IQN 16
 - 正在映射主机名 16

iSCSI 设置

验证E系列(iSCSI)中的Linux配置支持

为了确保操作可靠，您需要创建一个实施计划，然后使用 NetApp 互操作性表工具（IMT）验证是否支持整个配置。

步骤

1. 转至 "[NetApp 互操作性表工具](#)"。
2. 单击 * 解决方案 Search* 图块。
3. 在菜单：协议 [SAN 主机] 区域中，单击 * E 系列 SAN 主机 * 旁边的 * 添加 * 按钮。
4. 单击 * 查看细化搜索条件 *。

此时将显示细化搜索条件部分。在本节中，您可以选择适用的协议以及其他配置标准，例如操作系统，NetApp 操作系统和主机多路径驱动程序。

5. 选择您知道配置所需的条件，然后查看适用的兼容配置要素。
6. 根据需要，根据工具中的规定更新操作系统和协议。

单击右页面箭头可在查看支持的配置页面上访问选定配置的详细信息。

在E系列- Linux (iSCSI)中使用DHCP配置IP地址

要配置管理工作站与存储阵列之间的通信，请使用动态主机配置协议（DHCP）提供 IP 地址。

开始之前

确保您已具备以下条件：

- 与存储管理端口安装和配置在同一子网上的 DHCP 服务器。

关于此任务

每个存储阵列都有一个控制器（单工）或两个控制器（双工），每个控制器有两个存储管理端口。每个管理端口都将分配一个 IP 地址。

以下说明是指具有两个控制器的存储阵列（双工配置）。

步骤

1. 如果尚未连接以太网缆线，请将其连接到管理工作站以及每个控制器（A 和 B）上的管理端口 1。

DHCP 服务器会为每个控制器的端口 1 分配一个 IP 地址。



请勿在任一控制器上使用管理端口 2。端口 2 保留供 NetApp 技术人员使用。



如果断开并重新连接以太网缆线，或者存储阵列已重新启动，则 DHCP 会重新分配 IP 地址。此过程会一直进行，直到配置了静态 IP 地址为止。建议您避免断开电缆连接或重新启动阵列。

如果存储阵列无法在 30 秒内获取 DHCP 分配的 IP 地址，则会设置以下默认 IP 地址：

- 控制器 A，端口 1：169.254.128.101
- 控制器 B，端口 1：169.254.128.102
- 子网掩码：255.255.0.0

2. 找到每个控制器背面的 MAC 地址标签，然后向网络管理员提供每个控制器端口 1 的 MAC 地址。

网络管理员需要使用 MAC 地址来确定每个控制器的 IP 地址。要通过浏览器连接到存储系统，您需要使用这些 IP 地址。

安装适用于SMcli的SANtricity Storage Manager (11.53或更早版本)- Linux (iSCSI)

如果您使用的是 SANtricity 软件 11.53 或更早版本，则可以在管理工作站上安装 SANtricity 存储管理器软件，以帮助管理阵列。

SANtricity 存储管理器包括用于执行其他管理任务的命令行界面（CLI）以及用于通过 I/O 路径将主机配置信息推送到存储阵列控制器的主机上下文代理。



如果您使用的是 SANtricity 软件 11.60 及更高版本，则无需执行以下步骤。SANtricity 安全命令行界面（SMcli）包含在 SANtricity 操作系统中，可通过 SANtricity 系统管理器下载。有关如何通过 SANtricity 系统管理器下载 SMcli 的详细信息，请参阅 ["下载 SANtricity 系统管理器联机帮助下的命令行界面\(CLI\)主题"](#)



从 SANtricity 软件 11.80.1 版开始，不再支持主机上下文代理。

开始之前

确保您已具备以下条件：

- SANtricity 软件 11.53 或更早版本。
- 正确的管理员或超级用户权限。
- SANtricity 存储管理器客户端的系统，最低要求如下：
 - * RAM *：2 GB 用于 Java Runtime Engine
 - * 磁盘空间 *：5 GB
 - * 操作系统 / 架构 *：有关确定支持的操作系统版本和架构的指导，请访问 ["NetApp 支持"](#)。从 * 下载 * 选项卡中，转到菜单：下载 [E 系列 SANtricity 存储管理器]。

关于此任务

此任务介绍如何在 Windows 和 Linux 操作系统平台上安装 SANtricity 存储管理器，因为在数据主机使用 Linux 时，Windows 和 Linux 都是通用的管理工作站平台。

步骤

1. 从下载 SANtricity 软件版本 "[NetApp 支持](#)". 从 * 下载 * 选项卡中, 转到菜单: 下载 [E 系列 SANtricity 存储管理器]。
2. 运行 SANtricity 安装程序。

Windows	Linux
双击 SMIA* 。 exe 安装包以开始安装。	<ol style="list-style-type: none">a. 转到 SMIA* .bin 安装包所在的目录。b. 如果临时挂载点没有执行权限, 请设置 IATEMPDIR 变量。示例: IATEMPDIR=/root ./AMI-LINUX64-11.25.0A00.0002.binc. 运行 <code>chmod +x SMIA* .bin</code> 命令为文件授予执行权限。d. 运行 <code>./SMIA* .bin</code> 命令启动安装程序。

3. 使用安装向导在管理工作站上安装软件。

使用SANtricity系统管理器- Linux (iSCSI)配置存储

要配置存储阵列, 您可以使用 SANtricity 系统管理器中的设置向导。

SANtricity System Manager 是一个基于 Web 的界面, 嵌入在每个控制器上。要访问用户界面, 请将浏览器指向控制器的 IP 地址。设置向导可帮助您开始进行系统配置。

开始之前

确保您已具备以下条件:

- 带外管理。
- 用于访问 SANtricity 系统管理器的管理工作站, 其中包括以下浏览器之一:

浏览器	最低版本
Google Chrome	81.
Microsoft Edge	90
Mozilla Firefox	80
Safari	14.

关于此任务

如果您是 iSCSI 用户, 则在配置 iSCSI 时关闭了设置向导。

在打开 System Manager 或刷新浏览器且至少满足以下条件之一时, 向导将自动重新启动:

- 未检测到池和卷组。
- 未检测到工作负载。
- 未配置任何通知。

步骤

1. 在浏览器中，输入以下 URL：`https://<DomainNameOrIPAddress>`

IPAddress 是一个存储阵列控制器的地址。

首次在尚未配置的阵列上打开 SANtricity 系统管理器时，将显示设置管理员密码提示符。基于角色的访问管理可配置四个本地角色：管理员，支持，安全性和监控。后三个角色具有无法猜测的随机密码。为管理员角色设置密码后，您可以使用管理员凭据更改所有密码。有关四个本地用户角色的详细信息，请参见 SANtricity System Manager 用户界面中提供的联机帮助。

2. 在设置管理员密码和确认密码字段中输入管理员角色的 System Manager 密码，然后单击 * 设置密码 *。

如果未配置池，卷组，工作负载或通知，则设置向导将启动。

3. 使用设置向导执行以下任务：

- * 验证硬件（控制器和驱动器） * —验证存储阵列中的控制器和驱动器数量。为阵列分配一个名称。
- * 验证主机和操作系统 * - 验证存储阵列可以访问的主机和操作系统类型。
- * 接受池 * - 接受快速安装方法建议的池配置。池是一组逻辑驱动器。
- * 配置警报 * - 允许 System Manager 在存储阵列出现问题时自动接收通知。
- * 启用 AutoSupport * - 自动监控存储阵列的运行状况，并将派单发送给技术支持。

4. 如果尚未创建卷，请转到菜单：Storage[卷 > 创建 > 卷] 创建一个卷。

有关详细信息，请参见 SANtricity System Manager 的联机帮助。

在E系列- Linux (iSCSI)中配置多路径软件

要为存储阵列提供冗余路径，您可以配置多路径软件。

开始之前

您必须在系统上安装所需的软件包。

- 对于 Red Hat（RHEL）主机，运行 `rpm -q device-mapper-multipath` 验证软件包是否已安装。
- 对于 SLES 主机，请运行 `rpm -q multipath-tools` 来验证软件包是否已安装。

如果尚未安装操作系统，请使用操作系统供应商提供的介质。

关于此任务

如果某个物理路径中断，多路径软件可提供指向存储阵列的冗余路径。多路径软件为操作系统提供一个虚拟设备，该虚拟设备表示存储的活动物理路径。多路径软件还可管理更新虚拟设备的故障转移过程。

您可以在 Linux 安装中使用设备映射程序多路径（DM-MP）工具。默认情况下，在 RHEL 和 SLES 中禁用

DM-MP。要在主机上启用 DM-MP 组件，请完成以下步骤。

步骤

1. 如果尚未创建 multipath.conf 文件，请运行 `# touch /etc/multipath.conf` 命令。
2. 使用默认多路径设置，将 multipath.conf 文件留空。
3. 启动多路径服务。

```
# systemctl start multipathd
```

4. 运行 `uname -r` 命令以保存内核版本。

```
# uname -r
3.10.0-327.el7.x86_64
```

在向主机分配卷时，您将使用此信息。

5. 启用 multipathd 启动时执行守护进程。

```
systemctl enable multipathd
```

6. 在 /boot 目录下重建 initramfs 映像或 initrd 映像：

```
dracut --force --add multipath
```

7. 使用 ["手动创建主机"](#) 在联机帮助中使用操作步骤 检查是否已定义主机。验证每个主机类型设置是否基于中收集的内核信息 [第4步](#)。



对于映射到运行内核3.9或更早版本的主机的任何卷、将禁用自动负载平衡。

8. 重新启动主机。

在E系列- Linux (iSCSI)中设置多路径.conf文件

multipath.conf 文件是多路径守护进程 multipathd 的配置文件。

multipath.conf 文件会覆盖 multipathd 的内置配置表。



对于 SANtricity 操作系统 8.30 及更高版本，NetApp 建议使用提供的默认设置。

不需要对/etc/multipath.conf进行任何更改。

在E系列- Linux (iSCSI)中配置交换机

您可以根据供应商针对 iSCSI 的建议配置交换机。这些建议可能包括配置指令以及代码更新。

您必须确保满足以下条件：

- 为了实现高可用性，您有两个单独的网络。确保将 iSCSI 流量隔离到不同的网段。
- 必须启用流量控制 * 端到端 * 。
- 如果适用，您已启用巨型帧。



控制器的交换机端口不支持端口通道 /LACP 。不建议使用主机端 LACP ；多路径具有相同的优势，在某些情况下具有更好的优势。

在E系列- Linux (iSCSI)中配置网络

根据数据存储要求，您可以通过多种方式设置 iSCSI 网络。

有关为您的环境选择最佳配置的提示，请咨询您的网络管理员。

要为 iSCSI 网络配置基本冗余，请将每个主机端口以及每个控制器中的一个端口连接到不同的交换机，并对不同网段或 VLAN 上的每组主机端口和控制器端口进行分区。

您必须启用发送和接收硬件流量控制 * 端到端 * 。您必须禁用优先级流量控制。

如果出于性能原因在 IP SAN 中使用巨型帧，请确保将阵列，交换机和主机配置为使用巨型帧。有关如何在主机和交换机上启用巨型帧的信息，请参见操作系统和交换机文档。要在阵列上启用巨型帧，请完成中的步骤 ["配置阵列端网络"](#)。



许多网络交换机必须配置为超过 9 ， 000 字节，才能实现 IP 开销。有关详细信息，请参见交换机文档。

在E系列- Linux (iSCSI)中配置阵列端网络

您可以使用 SANtricity 系统管理器图形用户界面在阵列端配置 iSCSI 网络。

开始之前

确保您已具备以下条件：

- 一个存储阵列控制器的 IP 地址或域名。
- System Manager GUI ，基于角色的访问控制（ Role-Based Access Control ， RBAC ）或 LDAP 以及为对存储阵列进行适当安全访问而配置的目录服务的密码。有关访问管理的详细信息，请参见 SANtricity System Manager 联机帮助。

关于此任务

此任务介绍如何从 System Manager 的硬件页面访问 iSCSI 端口配置。您也可以从菜单： System[设置 > 配置 iSCSI 端口] 访问配置。

步骤

1. 在浏览器中，输入以下 URL：`https://<DomainNameOrIPAddress>`

IPAddress 是一个存储阵列控制器的地址。

首次在尚未配置的阵列上打开 SANtricity 系统管理器时，将显示设置管理员密码提示符。基于角色的访问管理可配置四个本地角色：管理员，支持，安全性和监控。后三个角色具有无法猜测的随机密码。为管理员角色设置密码后，您可以使用管理员凭据更改所有密码。有关四个本地用户角色的详细信息，请参见 SANtricity System Manager 用户界面中提供的联机帮助。

2. 在设置管理员密码和确认密码字段中输入管理员角色的 System Manager 密码，然后单击 * 设置密码 *。

如果未配置池，卷组，工作负载或通知，则设置向导将启动。

3. 关闭设置向导。

您稍后将使用此向导完成其他设置任务。

4. 选择 * 硬件 *。

5. 如果图形显示了驱动器，请单击 * 显示磁盘架背面 *。

此图将发生变化，以显示控制器，而不是驱动器。

6. 单击包含要配置的 iSCSI 端口的控制器。

此时将显示控制器的上下文菜单。

7. 选择 * 配置 iSCSI 端口 *。

此时将打开配置 iSCSI 端口对话框。

8. 在下拉列表中，选择要配置的端口，然后单击 * 下一步 *。

9. 选择配置端口设置，然后单击 * 下一步 *。

要查看所有端口设置，请单击对话框右侧的 * 显示更多端口设置 * 链接。

端口设置	Description
已配置以太网端口速度	<div>选择所需的速度。下拉列表中显示的选项取决于您的网络可以支持的最大速度（例如 10 Gbps）。</div> <div><div></div><div>控制器上提供的可选 25 Gb iSCSI 主机接口卡不会自动协商速度。您必须将每个端口的速度设置为 10 GB 或 25 GB。所有端口都必须设置为相同的速度。</div></div>
启用 IPv4/Enable IPv6	<div>选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。</div>

端口设置	Description
TCP 侦听端口（可通过单击 * 显示更多端口设置 * 来使用。）	如有必要，请输入新的端口号。 侦听端口是控制器用于侦听主机 iSCSI 启动程序的 iSCSI 登录的 TCP 端口号。默认侦听端口为 3260。您必须输入 3260 或 49152 到 65535 之间的值。
MTU 大小（可通过单击 * 显示更多端口设置 * 来获取。）	如有必要，请为最大传输单元（Maximum Transmission Unit，MTU）输入一个新大小（以字节为单位）。 默认最大传输单元（Maximum Transmission Unit，MTU）大小为每帧 1500 字节。您必须输入一个介于 1500 和 9000 之间的值。
启用 ICMP ping 响应	选择此选项可启用 Internet 控制消息协议（Internet Control Message Protocol，ICMP）。网络计算机的操作系统使用此协议发送消息。这些 ICMP 消息可确定主机是否可访问以及从该主机获取数据包所需的时间。

如果选择了 * 启用 IPv*，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv4 设置。如果选择了 * 启用 IPv6*，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv6 设置。如果同时选择了这两个选项，则 IPv4 设置对话框将首先打开，然后单击 * 下一步 *，IPv6 设置对话框将打开。

10. 自动或手动配置 IPv4 和 / 或 IPv6 设置。要查看所有端口设置，请单击对话框右侧的 * 显示更多设置 * 链接。

端口设置	Description
自动获取配置	选择此选项可自动获取配置。
手动指定静态配置	选择此选项，然后在字段中输入静态地址。对于 IPv4，请包括网络子网掩码和网关。对于 IPv6，请包括可路由的 IP 地址和路由器 IP 地址。

11. 单击 * 完成 *。
12. 关闭 System Manager。

在E系列- Linux (iSCSI)中配置主机端网络

要配置主机端网络，必须执行几个步骤。

关于此任务

您可以通过以下方式在主机端配置 iSCSI 网络：设置每个物理路径的节点会话数，打开相应的 iSCSI 服务，为 iSCSI 端口配置网络，创建 iSCSI 端绑定以及在启动程序和目标之间建立 iSCSI 会话。

大多数情况下，您可以使用适用于 iSCSI CNA/NIC 的收件箱软件启动程序。您无需下载最新的驱动程序，固件和 BIOS。请参见 ["NetApp 互操作性表工具"](#) 以确定代码要求。

步骤

1. 检查 `/etc/iscsi/iscsid.conf` 文件中的 `node.session.nr_sessions` 变量，查看每个物理路径的默认会话数。如有必要，将默认会话数更改为一个会话。

```
node.session.nr_sessions = 1
```

2. 将 `/etc/iscsi/iscsid.conf` 文件中的 `node.session.timeo.replacement_timeout` 变量更改为 20，默认值为 120。

```
node.session.timeo.replacement_timeout = 20
```

3. 您也可以设置 `node.startup = automatic` 在 `/etc/iscsi/iscsid.conf` 中运行任何之前 `iscsiadm` 重新启动后使会话持续存在的命令。

4. 确保 `iscsid` 和 `(open-) iSCSI` 服务已打开并启用，可用于启动。

```
# systemctl start iscsi
# systemctl start iscsid
# systemctl enable iscsi
# systemctl enable iscsid
```

5. 获取主机 IQN 启动程序名称，该名称将用于将主机配置到阵列。

```
# cat /etc/iscsi/initiatorname.iscsi
```

6. 为 iSCSI 端口配置网络。以下是适用于 RHEL 和 SLES 的示例说明：



除了公有网络端口之外，iSCSI 启动程序还应在单独的私有分段或 VLAN 上使用两个或更多 NIC。

- a. 使用 `ifconfig -a` 命令确定 iSCSI 端口名称。
- b. 设置 iSCSI 启动程序端口的 IP 地址。启动程序端口应与 iSCSI 目标端口位于同一子网中。

红帽企业 Linux 8 (RHEL 8)

创建示例文件 `/etc/sysconfig/network-scripts/ifcfg-<NIC port>` 包含以下内容。

```

TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=<NIC port>
UUID=<unique UUID>
DEVICE=<NIC port>
ONBOOT=yes
IPADDR=192.168.xxx.xxx
PREFIX=24
NETMASK=255.255.255.0
NM_CONTROLLED=no
MTU=

```

有关IPv6的可选附加项：

```

IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=fdxx::192:168:xxxx:xxxx/32
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=eui64

```

Red Hat Enterprise Linux 9 和 10 (RHEL 9 和 RHEL 10) 以及 SUSE Linux Enterprise Server 16 (SLES 16)

使用 `nmtui` 用于激活和编辑连接的工具。该工具将生成 `<NIC port>.nmconnection` 文件 `/etc/NetworkManager/system-connections/`。

- SUSE Linux Enterprise Server 12 和 15 （ SLES 12 和 SLES 15 ） *

创建示例文件 `/etc/sysconfig/network/ifcfg-<NIC port>` 包含以下内容。

```

IPADDR='192.168.xxx.xxx/24'
BOOTPROTO='static'
STARTMODE='auto'

```

+ 可选添加IPv6：

```

IPADDR_0='fdxx::192:168:xxxx:xxxx/32'

```

+



请务必为两个 iSCSI 启动程序端口设置地址。

- a. 重新启动网络服务。

```
# systemctl restart network
```

- b. 确保 Linux 服务器可以对 iSCSI 目标端口执行 ping 操作。

7. 通过以下两种方法之一在启动程序和目标之间建立 iSCSI 会话(共四个)。

- a. (可选)使用 ifaces 时、通过创建两个 iSCSI iface 绑定来配置 iSCSI 接口。

```
# iscsiadm -m iface -I iface0 -o new
# iscsiadm -m iface -I iface0 -o update -n iface.net_ifacename -v
<NIC port1>
```

```
# iscsiadm -m iface -I iface1 -o new
# iscsiadm -m iface -I iface1 -o update -n iface.net_ifacename -v
<NIC port2>
```



要列出这些接口，请使用 `iscsiadm -m iface`。

- b. 发现 iSCSI 目标。在工作表中保存 IQN（与每次发现相同），以供下一步使用。

方法1 (使用 ifaces)

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port> -I iface0
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260 -I iface0
```

方法2 (无 ifaces)

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port>
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260
```



IQN 如下所示：

```
iqn.1992-01.com.netapp:2365.60080e50001bf1600000000531d7be3
```

- c. 在iSCSI启动程序和iSCSI目标之间创建连接。

方法1 (使用ifaces)

```
# iscsiadm -m node -T <target_iqn> -p  
<target_ip_address>:<target_tcp_listening_port> -I iface0 -l  
# iscsiadm -m node -T iqn.1992-  
01.com.netapp:2365.60080e50001bf1600000000531d7be3 -p  
192.168.0.1:3260 -I iface0 -l
```

方法2 (无ifaces)

```
# iscsiadm -m node -L all
```

- a. 列出在主机上建立的 iSCSI 会话。

```
# iscsiadm -m session
```

验证E系列- Linux (iSCSI)中的IP网络连接

您可以使用 ping 测试来验证 Internet 协议（IP）网络连接，以确保主机和阵列能够进行通信。

步骤

1. 在主机上，根据是否启用了巨型帧，运行以下命令之一：

- 如果未启用巨型帧，请运行以下命令：

```
ping -I <hostIP\> <targetIP\>
```

- 如果启用了巨型帧，请使用有效负载大小 8,972 字节运行 ping 命令。IP 和 ICMP 合并标头为 28 字节，如果添加到有效负载中，则等于 9,000 字节。s 开关设置 数据包大小 位。d 开关用于设置调试选项。通过这些选项，可以在 iSCSI 启动程序和目标之间成功传输 9,000 字节的巨型帧。

```
ping -I <hostIP\> -s 8972 -d <targetIP\>
```

在此示例中，iSCSI 目标 IP 地址为 192.0.2.8。

```
#ping -I 192.0.2.100 -s 8972 -d 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. 从每个主机的启动程序地址（用于 iSCSI 的主机以太网端口的 IP 地址）到每个控制器 iSCSI 端口执行问题描述 a ping 命令。从配置中的每个主机服务器执行此操作，并根据需要更改 IP 地址。



如果命令失败（例如，returns Packet needs to be fragmented but df set），请验证主机服务器，存储控制器和交换机端口上以太网接口的 MTU 大小（巨型帧支持）。

在E系列中创建分区和文件系统- Linux (iSCSI)

由于新 LUN 在 Linux 主机首次发现时没有分区或文件系统，因此必须先格式化 LUN，然后才能使用它。您也可以选择 LUN 上创建文件系统。

开始之前

确保您已具备以下条件：

- 主机发现的 LUN。
- 可用磁盘的列表。（要查看可用磁盘，请在 /dev/mapper 文件夹中运行 ls 命令。）

关于此任务

您可以使用 GUID 分区表（GPT）或主启动记录（MBR）将磁盘初始化为基本磁盘。

使用 ext4 等文件系统格式化 LUN。某些应用程序不需要执行此步骤。

步骤

1. 发出 sanlun lun show -p 命令，以检索映射磁盘的 SCSI ID。

SCSI ID 是一个 33 个字符的十六进制数字字符串，从数字 3 开始。如果启用了用户友好名称，则设备映射程序会将磁盘报告为 mpath，而不是 SCSI ID。

```
# sanlun lun show -p

E-Series Array: ictml619s01c01-
SRP(60080e50002908b40000000054efb9d2)
Volume Name:
Preferred Owner: Controller in Slot B
Current Owner: Controller in Slot B
Mode: RDAC (Active/Active)
UTM LUN: None
LUN: 116
LUN Size:
Product: E-Series
Host Device:
mpathr(360080e50004300ac000007575568851d)
Multipath Policy: round-robin 0
Multipath Provider: Native
```

host	controller		controller	
path	path	/dev/	host	target
state	type	node	adapter	port
up	secondary	sdcx	host14	A1
up	secondary	sdat	host10	A2
up	secondary	sdbv	host13	B1

2. 根据适用于您的 Linux 操作系统版本的方法创建新分区。

通常，标识磁盘分区的字符会附加到 SCSI ID（例如，数字 1 或 P3）中。

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. 在分区上创建文件系统。

创建文件系统的方法因所选的文件系统而异。

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. 创建一个文件夹以挂载新分区。


```
# mkdir /mnt/ext4
```

5. 挂载分区。

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

验证E系列- Linux (iSCSI)主机上的存储访问

在使用卷之前，您需要验证主机是否可以将数据写入卷并将其读回。

开始之前

确保您已具备以下条件：

- 使用文件系统格式化的初始化卷。

步骤

1. 在主机上，将一个或多个文件复制到磁盘的挂载点。
2. 将文件复制回原始磁盘上的其他文件夹。
3. 运行 `dIFF` 命令将复制的文件与原始文件进行比较。

完成后

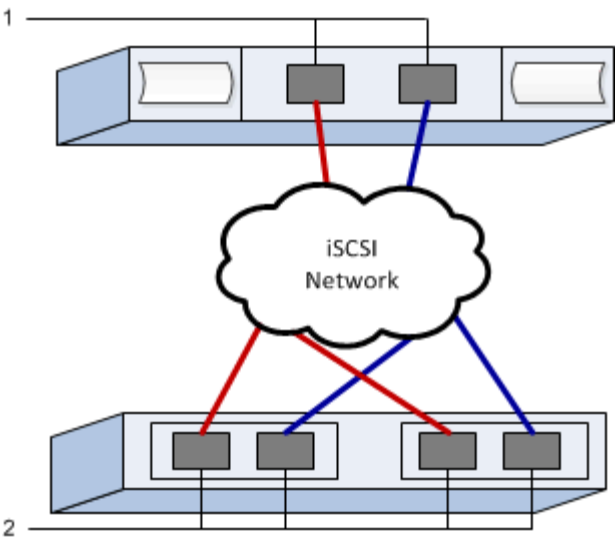
删除复制的文件和文件夹。

在E系列- Linux中记录iSCSI配置

您可以生成并打印此页面的 PDF ，然后使用以下工作表记录 iSCSI 存储配置信息。要执行配置任务，您需要此信息。

建议的配置

建议的配置包括两个启动程序端口和四个目标端口以及一个或多个 VLAN 。



目标 IQN

标注编号	目标端口连接	IQN
2.	目标端口	

正在映射主机名

标注编号	主机信息	名称和类型
1.	正在映射主机名	
	主机操作系统类型	

版权信息

版权所有 © 2026 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。