Veritas™ Appliance iSCSI 指南

3.1.x

VERITAS™

Veritas Appliance iSCSI 指南

3.1 版

法律声明

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

技术支持

技术支持维护全球的支持中心。所有支持服务将会根据您的支持协议以及当时最新的企业技术支持政策进行交付。有关支持产品和服务以及如何联系技术支持的信息，请访问我们的网站：

https://www.veritas.com/support

您可以在下列 URL 上管理 Veritas 帐户信息：

https://my.veritas.com

如有关于现有支持协议有任何问题，请按如下所示给您所在区域的支持协议管理团队发送电子邮件：

全球（日本除外）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

文档

可以在 Veritas 网站上获取最新文档：

https://sort.veritas.com/documents

文档反馈

您的反馈对我们非常重要。请提出您对本文档的改进建议，或者就本文档中的错误或疏漏进行报告。请注明所报告文本的文档标题、文档版本和章节标题。请将您的反馈发送至：

APPL.docs@veritas.com

您也可以在以下 Veritas 社区站点中查看相关文档信息或进行提问：

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) 是一个网站，提供的信息和工具有助于自动处理及简化某些耗时的管理任务。根据具体产品，SORT 会帮助您准备安装和升级、识别您数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见数据表：

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目录

1

概述

本章节包括下列主题：

关于 iSCSI

iSCSI 是使用 TCP/IP 通过网络来连接存储设备的一种方式。经开发，iSCSI 能够使用 TCP/IP 协议通过现有的 Internet 协议 (IP) 网络传输 SCSI 命令。iSCSI 可以通过 IP 网络同时传递消息流量和基于块的存储，而无需安装单独的光纤通道网络。

该协议允许客户端（称为启动程序）向远程服务器上的 SCSI 存储设备（目标）发送 SCSI 命令。

目标是位于 iSCSI 服务器上的存储资源（通常是该服务器上运行的 iSCSI 存储节点的许多可能实例之一）。要相互通信，iSCSI 启动程序和目标应建立 iSCSI 会话。

以下设备和配置支持 iSCSI。

- NetBackup 5240 配置 H
- NetBackup 5340 配置 A、B、C、D 和 E

关于 iSCSI 启动器和目标

iSCSI 是通过网络共享存储并在块设备级别运行的一种方式。对于 iSCSI 通信，以下组件可相互通信：

- 启动器
- 目标

用于访问 iSCSI 存储的客户端称为启动器。此 iSCSI 启动器可以连接到服务器（iSCSI 目标）。在这种情况下，iSCSI 启动器会将 SCSI 命令发送到 iSCSI 目标。出于此目的，这些 SCSI 命令会在 IP 数据包中打包。

iSCSI 目标设备可接收 iSCSI 命令并共享存储。该存储可以是物理磁盘，也可以是表示多个磁盘的区域或物理磁盘的一部分。存储阵列是典型的 iSCSI 目标。

支持的 iSCSI 功能

查看下面几点，以了解 NetBackup 设备如何支持 iSCSI：

- 5240 Appliance 的配置 H 上以及 5340 计算节点的所有配置中都支持 iSCSI。
- NetBackup 5240 Appliance 的配置 H 始终充当启动程序。
  请参见第 10 页的“NetBackup 5240 Appliance I/O 配置 H”。
- 5340 配置充当启动程序。
  请参见第 11 页的“NetBackup 5340 计算节点 I/O 配置”。
- iSCSI 仅支持 VMware 备份。它支持 NetBackup for VMware 功能。
  请参见第 15 页的“关于 NetBackup for VMware”。
- 对于此版本，iSCSI 功能（命令）在 NetBackup Appliance 命令行操作界面上可用。
- iSCSI 仅支持 IPv4 地址。不支持基于 IPv6 的 iSCSI 连接。
  此外，启动器和目标必须处于相同的第 2 层网络 (L2)。
- iSCSI 支持动态多径处理 (DMP)。可以通过多个路径连接到同一目标。只要其中一个路径可用，就可以继续通过 iSCSI 进行备份或还原。
- 支持使用 iSNS 服务器（Internet 存储名称服务）来发现目标。
  请参见第 25 页的“关于 iSNS”。
- 可在网络接口或 iSCSI 接口上配置 VLAN。如果网络接口和 iSCSI 接口上都配置了 VLAN，则网络接口的 VLAN 在两个接口上均有效。请注意，当不同子网上的网络接口和 iSCSI 接口都配置了 VLAN 时，不支持此配置。

网络接口		iSCSI 接口		描述
IP	**VLAN**	**IP**	**VLAN**	
子网 X	无	子网 X	无	受支持
子网 X	无	子网 Y	VLAN A	受支持

网络接口		iSCSI 接口		描述
子网 X	VLAN B	子网 X	VLAN B	受支持
子网 X	VLAN B	子网 Y	VLAN B	不支持

- 在 10 GB 以太网/iSCSI 卡中只支持 QLogic 小型可插拔 (SFP+) 模块。如果 10 Gb 以太网/iSCSI 卡中检测到不支持的 SFP 模块，则会收到警报（如果已配置警报）。

有关最新的 NetBackup Appliance 兼容性信息，请参考以下网站上的硬件兼容性列表：

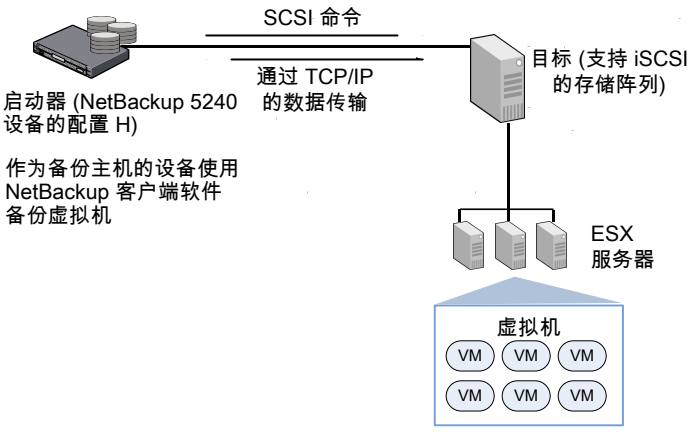
www.netbackup.com/compatibility

iSCSI 拓扑概述

设备可以作为 VMware 备份主机运行并使用 iSCSI 进行 VMware 备份。在此拓扑中，设备会充当启动器并连接到 TCP/IP 网络上的存储阵列（目标）。存储阵列可以通过 FC/LAN 等连接到 ESX 主机。

下图显示了 NetBackup 5240 拓扑作为示例。

图 1-1 iSCSI 拓扑



通过 iSCSI 在设备上备份虚拟机。

关于 iSCSI 限定名称 (IQN)

在 iSCSI 网络中，使用该网络的每个 iSCSI 元素都具有唯一的 iSCSI 名称并分配有一个地址以进行访问。每个 iSCSI 元素（启动器或目标）均由唯一的 iSCSI 限定名称 (IQN) 标识。IQN 是未链接到 IP 地址的逻辑名称。

IQN 具有以下属性：

- 它是唯一的。两个启动器或目标不能具有相同名称。
- 最大长度为 255 个字符。
- 只能包含数字 (0-9)、字母（A-Z 和 a-z）、冒号 (:)、连字符 (-) 和句点 (.)。

IQN 格式示例为 `iqn.yyyy-mm.naming-authority:unique name`，其中：

- `yyyy-mm` 是建立命名机构的年份和月份。
- naming-authority 通常是命名机构的 Internet 域名的反向语法。
- unique name 是您要使用的任何名称，例如，主机的名称。命名机构必须确保冒号后面分配的任何名称都是唯一的。

示例：iqn.1999-06.com.veritas:abc

2

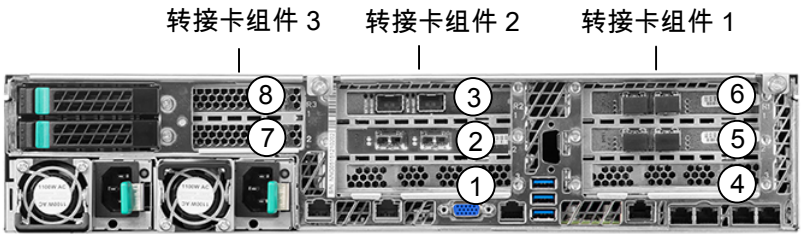
了解设备配置

本章节包括下列主题：

NetBackup 5240 Appliance I/O 配置 H

NetBackup 5240 Appliance 的后面板包含三个 PCIe 转接卡组件。PCIe 转接卡组件 1 和 2 都支持三个标准 PCIe 卡，而 PCIe 转接卡组件 3 支持两个半高 PCIe 卡。这些插槽标记为 1 到 8。下图显示了转接卡组件和插槽号。

图 2-1 后面板转接卡组件位置和 PCIe 插槽分配



NetBackup 5240 Appliance 支持多个基于 PCIe 的 I/O 配置选项。下表显示了插槽 2 中具有 iSCSI 卡的配置 H 选项。

表 2-1 NetBackup 5240 Appliance 配置 H

I/O 配置选项	插槽 1 *	插槽 2	插槽 3	插槽 4	插槽 5	插槽 6	插槽 7 **	插槽 8
H	-	10 GbE NIC [1、2] (iSCSI)	10 GbE NIC [1、2]	-	8 Gb FC HBA [2]	8 Gb FC HBA [2]	-	-

* 插槽 1 中包含一个出厂安装的 PCIe RAID 6 控制器（当随 NetBackup 5240 Appliance 至少购买了一个 NetBackup 5240 存储扩展架时）。否则，插槽 1 未填充。

** 插槽 7 中包含 NetBackup 5240 Appliance 的内部 PCIe RAID 控制器。该 RAID 控制器用于为设备操作系统所在的磁盘驱动器创建 RAID 1 阵列。这些操作系统驱动器位于前面板的插槽 0 和 1 中。

PCIe 卡电缆连接类型：

[1] 直连铜缆（也称为双轴电缆或双股线）

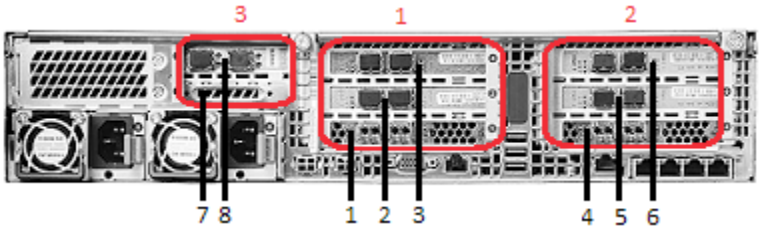
[2] 光缆

有关更多详细信息，请参见 *NetBackup Appliance Product Description Guide*（《NetBackup Appliance 产品说明指南》）。

NetBackup 5340 计算节点 I/O 配置

NetBackup 5340 计算节点的后面板包含三个 PCIe 转接卡组件。PCIe 转接卡组件 1 和 2 都支持三个标准 PCIe 卡，而 PCIe 转接卡组件 3 支持两个半高 PCIe 卡。这些插槽标记为 1 到 8。在下图中，以红色标出了转接卡组件。PCIe 插槽已进行标识。

图 2-2 后面板转接卡组件位置和 PCIe 插槽分配



NetBackup 5340 计算节点支持多个基于 PCIe 的 I/O 配置选项。下表显示了配置 A、B、C、D 和 E。每个配置都支持 iSCSI。

表 2-2 NetBackup 5340 计算节点的基于 PCIe 的标准可用 I/O 配置

I/O 配置选项	插槽 **1 ***	插槽 **2**	插槽 **3**	插槽 **4 ***	插槽 **5**	插槽 **6**	插槽 **7**	插槽 **8**
A	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	已保留	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）
B	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE2562 8 Gb FC HBA [3]	已保留	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）
C	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	已保留	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）
D	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	已保留	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）
E	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2692 16 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	QLogic QLE2562 8 Gb FC HBA [3]	已保留	QLogic QLE8442 10 GbE NIC [1、3]（支持 iSCSI）

I/O 配置选项	插槽 1 *	插槽 2	插槽 3	插槽 4 *	插槽 5	插槽 6	插槽 7	插槽 8

***** 插槽 1 和 4 中的 16Gb 光纤通道 HBA 端口用于将 NetBackup 5340 计算节点与 Veritas 5U84 主存储扩展架连接起来。**因此，插槽 1 和 4 不支持标准网络 I/O 操作**。

PCIe 卡电缆连接类型：

[1] 直连铜缆（也称为双轴电缆或双股线）

[2] 标准铜缆

[3] 光缆

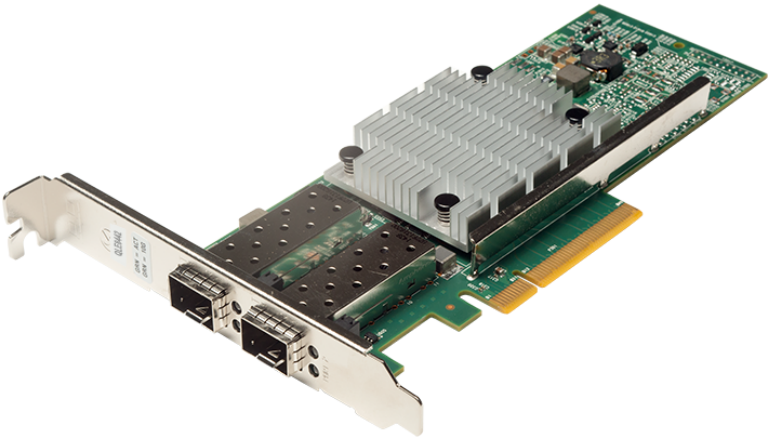


表 2-3 QLE8442 双端口 10 GB 以太网卡规格

项目	规格
支架高度	全高
功耗	9.65 瓦特（标称）
系统接口类型	PCIe v3.0
速度和插槽宽度	8.0 GT/秒，8 通道
LED 指示灯	链接/活动 关 = 无链接（电缆已断开） 常亮 = 线路已连接 闪烁 = 网络活动

项目	规格
认证	FCC A、ICES A、UL、CE、VCCI、CISPR、KCC
工作温度	0 到 55℃（32 到 131°F）
存储温度	-40 到 65℃（-40 到 149°F）
工作湿度	55 C 时 7% 到 93%
存储湿度	65℃ 时最高 93%
气流	55 C 时 100 LFM

要购买适用于您设备的 QLE8442 双端口 10 GB 以太网卡（采用 SFP+ 模块），请与您的 Veritas 销售代表或 Veritas 合作伙伴代表联系。

采用 SFP+ 模块的 QLE8442 双端口 10 GB 以太网卡

SKU 编号	描述
18293	XX40 QLogic QLE8442 10 Gbps 双端口以太网/ISCSI CRU（包括 SFP 模块）

3

了解 NetBackup for VMware

本章节包括下列主题：

关于 NetBackup for VMware

NetBackup for VMware 可备份和还原在 VMware ESX server 上运行的 VMware 虚拟机。NetBackup for VMware 采用 VMware vStorage API for Data Protection。备份过程从 ESX server 转移到了 VMware 备份主机。

NetBackup for VMware 可以执行以下任务：

- 对虚拟机执行脱离主机备份（NetBackup 客户端软件在虚拟机上不是必需的）。脱离主机备份减少了 VMware 主机上的备份处理负载。
- 可提高与标准文件顺序备份方法相当的备份速度（如果虚拟机中充满了大量的小文件）。
- 使用 VSS 自动创建静默快照（仅限 Windows）。如果在 Linux 访客操作系统中启用快照静默，则在 Linux 上创建静默快照。
- 使用快照技术使虚拟机可完全供用户使用。
- 支持 VMware vSphere 和 vCloud Director。
- 执行完全备份和增量式备份，包括块级增量式备份。
- 备份整个虚拟机。
- 在虚拟机关闭的情况下进行备份。

- 可以从备份中还原所选文件。

VMware 备份过程概述

下表介绍了 NetBackup 备份过程中的各个阶段。

表 3-1 NetBackup 备份过程

阶段	描述
第 1 阶段	NetBackup 主服务器启动备份。
第 2 阶段	VMware 备份主机上的 NetBackup 客户端启动虚拟机上的 VMware 快照。
第 3 阶段	Windows：VSS 同步虚拟机上的文件系统。 Linux：如果在 Linux 访客操作系统中启用快照静默，则在虚拟机上同步文件系统。（有关如何启用快照静默的其他信息，请联系您的操作系统供应商和 VMware。）
第 4 阶段	VMware 服务器在虚拟磁盘数据存储上创建快照。
第 5 阶段	NetBackup 客户端从数据存储读取快照，然后将数据写入 NetBackup 存储单元。

“传输模式”选项 (VMware)

传输模式确定快照数据从 VMware DataStore 传送到 VMware 备份主机的方式。适合的模式部分取决于连接 VMware DataStore 与 VMware 备份主机的网络的类型。

默认情况下，选择所有模式。NetBackup 将从上向下按顺序尝试每种传输模式。它将使用可成功用于虚拟机中所有磁盘的第一种模式。

表 3-2 传输模式

模式	描述
SAN	适于通过光纤通道 (SAN) 或 iSCSI 的未加密传输。 **注意：**在 NetBackup 设备上，通过 iSCSI 进行 VMware 备份时使用 **SAN** 传输模式。 **注意：**使用 VMware Virtual Volume (VVol) 的虚拟机不支持此模式。

模式	描述
hotadd	允许您在虚拟机中运行 VMware 备份主机。 **注意：**对于使用 VVol 的虚拟机，虚拟机和备份主机 (hotadd) 虚拟机必须位于同一 VVol 数据存储。 有关此传输模式以及在 VMware 虚拟机中安装备份主机的说明，请参见 VMware 文档。
nbd	适于本地网络上使用网络块设备 (NBD) 驱动程序协议的未加密传输。这种模式的传输通常比光纤通道传输方式要慢。
nbdssl	适于使用网络块设备 (NBD) 驱动程序协议的本地网络上的加密传输 (SSL)。这种模式的传输通常比光纤通道传输方式要慢。

4

配置 iSCSI

本章节包括下列主题：

为 iSCSI 配置设备

在为 iSCSI 配置设备之前，请确保已在您的环境中配置 iSCSI 目标。查看目标供应商提供的文档以获取更多参考。

表 4-1 提供了在设备上配置和设置 iSCSI 的说明。

表 4-1 在设备上配置 iSCSI

步骤编号	描述	参考信息
1.	为启动程序配置 IQN。此步骤为可选步骤。	请参见第 19 页的“为启动器设置 IQN”。
2.	配置 iSCSI 接口。必须配置 IP 地址。可以选择配置其他接口属性，如网络掩码、网关等。	请参见第 20 页的“配置接口属性”。
3.	使用门户地址或 iSNS 服务器发现目标。	请参见第 24 页的“使用门户地址发现目标”。 请参见第 26 页的“使用 iSNS 发现目标”。
4.	连接到目标。	请参见第 28 页的“连接到目标”。

为启动器设置 IQN

本节介绍如何为 NetBackup Appliance（启动器）设置 IQN。

设置 IQN

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Initiator Set IQN** 命令并输入 IQN 作为参数。

关于 IQN，请注意以下几点：

- IQN 的最大长度为 255 个字符。
- IQN 只能包含数字 (0-9)、字母（A-Z 和 a-z）、冒号 (:)、连字符 (-) 和句点 (.)。

示例：iqn.1999-06.com.veritas:abc

4 显示以下消息：

```
iSCSI> Initiator Set IQN iqn.veritas.abc
- [Info] The IQN has been updated to iqn.veritas.abc.
```

查看接口属性

本节列出了查看 iSCSI 接口属性的步骤。

查看接口属性

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface Show** 命令，然后按 **Enter** 以查看 iSCSI 接口。将显示以下属性：

```
appliance.iSCSI > Interface Show
Showing the available interfaces...

+--------------+----------+-----------------+-------------+-------+-------+----+----+
|Interface Name|Network   |   MAC Address   | IP Address  |Netmask Gateway|MTU |VLAN
|              |Interface |                 |             |       |       |    |Tag |
+--------------+----------+-----------------+-------------+-------+-------+----|----+
|     iscsi1   |  eth6    |00:0e:1e:53:55:11|10.181.198.62|       |       |1500|    |
+--------------+----------+-----------|-------------+-------+-------+----+----+

|     iscsi2   |  eth7     |00:0e:1e:53:55:13|             |       |       |1500|    |
+--------------+----------+-----------|-------------+-------+-------+----|----+
```

配置接口属性

本节列出了为 ISCSI 接口配置接口属性（如网关、IPv4 地址、网络掩码、最大传输单元 (MTU) 和 VLAN 标记）的步骤。

MTU 可控制以太网帧的最大传输单元大小。该大小必须为 68 到 65535 之间的数字。当您为 iSCSI 接口配置 MTU 时，将为所映射到的 iSCSI 接口和网络接口配置新的 MTU 值。

VLAN 标记是将 VLAN ID 插入到数据包头中的方法，以便标识数据包所属的 VLAN。具体来说，交换机会使用 VLAN ID 确定要向其发送广播数据包的端口或接口。

可在网络接口或 iSCSI 接口上配置 VLAN。如果网络接口和 iSCSI 接口上都配置了 VLAN，则网络接口的 VLAN 在两个接口上均有效。

配置 IP 地址

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface IPAddress Set** 命令。

4 输入 IP 地址和 iSCSI 接口名称作为参数。按 **Enter**。

示例：

```
iSCSI> Interface IPAddress Set 10.80.156.88iscsi1
[Info] The IP address has been configured for iscsi1.
```

注意：在示例中使用的值是示例占位符值。

配置网络掩码

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface Netmask Set** 命令。

4 输入网络掩码值和 iSCSI 接口名称作为参数。按 **Enter**。

示例：

```
iSCSI> Interface Netmask Set 255.255.255.0iscsi10
[Info] The Netmask has been configured for iscsi10.
```

配置网关

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface Gateway Set** 命令。

4 输入网关值和 iSCSI 接口名称作为参数。按 **Enter**。

示例：

```
iSCSI> Interface Gateway Set 192.168.4.1iscsi10
[Info] The gateway has been configured for iscsi10.
```

配置最大传输单元 (MTU)

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface MTU Set** 命令。

4 输入 MTU 值和 iSCSI 接口名称。

MTU 必须为 68 到 65535 之间的数字。新的 MTU 值将同时应用于所映射到的 iSCSI 接口和网络接口。

示例：

```
iSCSI> Interface MTU Set 3000iscsi10

The new MTU value applies to both iscsi1 and
also network interface eth6.
Do you want to continue?(yes/no)[no]:yes

[Info] The MTU has been configured for iscsi10.
```

配置 VLAN 标记

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface VLAN Set** 命令。

4 输入 VLAN ID 和 iSCSI 接口名称作为参数。按 **Enter**。

VLAN ID 必须为 1 到 4095 之间的数字。

示例：

```
 iSCSI> Interface VLAN Set 75iscsi10

[Info] The VLAN tag has been configured for iscsi10.
```

删除和重置接口属性

本节列出了删除除了 MTU 以外的所有接口属性的步骤。它还包含将 MTU 重置为默认值 (1500) 的步骤。

MTU 无法删除，只能重置为其默认值。

删除接口属性

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 使用以下命令删除特定属性：

- 键入 **Interface Gateway Remove** 命令并输入 iSCSI 接口名称。
  此命令可从指定接口删除网关。

示例：

```
iSCSI> Interface Gateway Remove iscsi1

[Info] The Gateway has been removed from iscsi1.
```

- 键入 **Interface IPAddress Remove** 命令并输入 iSCSI 接口名称。此命令可从指定接口删除 IP 地址。
  示例：

```
iSCSI> Interface IPAddress Remove iscsi1

[Info] The IP address has been removed from iscsi1.
```

- 键入 **Interface Netmask Remove** 命令并输入 iSCSI 接口名称。此命令可从指定接口删除网络掩码。
  示例：

```
iSCSI> Interface Netmask Remove iscsi1

[Info] The Netmask has been removed from iscsi1.
```

- 键入 **Interface VLAN Remove** 命令并输入 iSCSI 接口名称。此命令可从指定接口删除 VLAN 标记。
  示例：

```
iSCSI> Interface VLAN Remove iscsi1

[Info] The VLAN tag has been removed from iscsi1.
```

重置 MTU

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Interface MTU Reset** 命令并输入 iSCSI 接口名称。请注意，此命令可同时在映射到的 iSCSI 接口和网络接口上将 MTU 重置为默认值 (1500)。

示例：

```
iSCSI > Interface MTU Reset iscsi1
The MTU will be reset to 1500 for both iscsi1 and also
the network interface eth6.
Do you want to continue?(yes/no)[no] :yes

[Info] The MTU has been reset to 1500.
```

关于 CHAP 身份验证

设备所使用的身份验证方法称为质询握手身份验证协议（或 CHAP）。CHAP 身份验证可应用于以下命令或操作：

- 发现目标
- 连接到目标

在 iSCSI 会话的初始阶段，设备（启动器）会将登录请求发送到存储系统以开始 iSCSI 会话。然后，存储系统将允许或拒绝登录请求，或确定不需要登录。如果在目标上启用身份验证，则必须对凭据进行身份验证并建立会话，然后服务器才能访问存储资源。服务器会比较客户端中的值，如果信息匹配，则授予会话。如果响应失败，则会话将被拒绝，并且请求阶段将会重新开始。

启动器使用 CHAP 用户名和密码登录。您可以指定 CHAP 密码或生成随机密码。要设置和配置 CHAP 身份验证，请参见目标供应商文档。

使用门户地址发现目标

本节提供了使用目标门户地址发现 iSCSI 目标的说明。目标门户地址是与目标关联的主机名或 IPv4 地址。

目标门户地址的格式为 **<IPv4 地址/主机名>:[<端口>]**。

示例：192.116.116.50 或 abc:3260，其中 3260 是默认端口。

必须先发现目标，然后才能连接到该目标。

使用目标门户地址发现目标

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 Main_Menu > Settings > iSCSI 菜单。

3 键入 **Target Discover Portal** 命令

4 输入已配置为参数的目标门户地址和 iSCSI 接口名称。请注意以下注意事项：

- 目标门户地址必须采用以下格式：**<IPv4 地址/主机名>[:端口]**。主机名可以是短名称或完全限定域名。
  示例：192.116.116.50 或 abc:3260

- iSCSI 接口名称只能包含数字 (0-9)、字母（A-Z 和 a-z）、冒号 (:)、连字符 (-)、下划线 (_) 和句点 (.)。该名称只能以数字 (0-9)、字母（A-Z 和 a-z）和下划线 (_) 开头。

5 运行 **Target Discover Portal <门户地址> <接口名称>** 命令。系统会提示您提供用户名和密码。如果您的目标需要身份验证，则键入 **yes**。按以下方式发现并显示指定门户地址和接口上可用的目标：

```
Does your target require a username and password? (yes,no)[no]:no

Showing the discovered targets...

+-----+-----------------------|--------------------|----------------+
| No. |     Target IQN         |Target Portal Address|
Interfaces   |
+-----+-----------------------|--------------------|----------------|
|  1  |iqn.1996-03.veritas:abc | 10.121.98.22:3260   | iscsi1,
iscsi2 |
+-----+-----------------------|--------------------|----------------|
|  2  |iqn.1996-03.veritas:xyz | 10.121.98.23:3260   | iscsi1,
iscsi2 |
+-----+-----------------------|--------------------|----------------+
|  3  |iqn.1996-03.veritas:host| 10.121.98.24:3260   | iscsi1,
iscsi2 |
------|-----------------------|--------------------|----------------|
```

注意：如果在连接目标后再次运行 `iSCSI > Target Discover Portal` 或 `iSCSI > Target Discover iSNS` 命令，则会覆盖现有连接设置，如目标凭据。如果目标需要身份验证，则将需要在重新连接现有会话后再次输入目标凭据。在设备重新启动、更改设备的 IQN 或重新启动 iSCSI 进程后，必须重新连接现有会话。

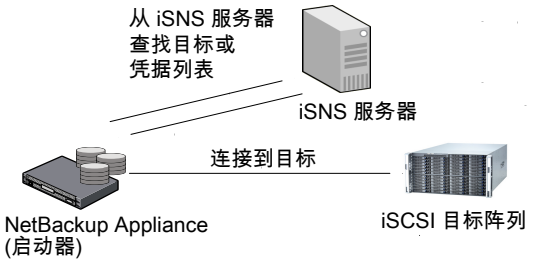
关于 iSNS

iSNS 服务器使用 Internet 存储名称服务协议维护网络上有关活动 iSCSI 设备的信息，包括 IP 地址、iSCSI 节点名称和门户组。使用该 iSNS 协议，可以在 IP 存储网络上自动发现并管理 iSCSI 设备。iSCSI 启动器（如 NetBackup Appliance）可以查询 iSNS 服务器以发现 iSCSI 目标设备。

您可以使用 iSNS（Internet 存储名称服务）服务器发现目标。配置 iSNS 服务器，这样就无需为每个目标配置每个启动器。网络上存在多个主机时，配置 iSNS 服务

器可节省时间。iSNS 服务器通过动态维护有关组卷的 iSCSI 目标名称的最新信息来为组提供中央管理点。

如果您具有 iSNS 服务器，则无需在命令中使用特定目标名称即可发现目标。下图介绍了设备和 iSNS 服务器之间的交互。



使用 iSNS 发现目标

本节提供了使用 Internet 存储名称服务 (iSNS) 方法发现 iSCSI 目标的说明。如果您的网络上至少有一个 iSNS 服务器，则使用此方法。使用此方法，iSCSI 启动器可以发现注册到 iSNS 服务器的目标。对于此方法，您必须提供 iSNS 服务器地址和/或端口。然后，iSCSI 启动器可以查询指定的 iSNS 服务器以发现目标。iSNS 服务器的默认端口为 3205。

仅当发现目标后才能连接到该目标。检查以下注意事项：

- 如果在连接目标后再次运行 `iSCSI > Target Discover Portal` 或 `iSCSI > Target Discover iSNS` 命令，则会覆盖现有连接设置，如目标凭据。如果目标需要身份验证，则在重新连接现有会话后再次输入目标凭据。如果设备重新启动，则需要重新连接现有会话。更改设备的 IQN 或重新启动 iSCSI 进程后，必须重新连接现有会话。
- 在两个 iSCSI 接口上使用 iSNS 发现目标时，先为 *iscsi1* 运行 `Target Discover iSNS` 命令，然后再为 *iscsi2* 运行此命令。`Target Show All` 命令只显示最近的记录。例如，对于某些目标，`Target Show All` 命令中的“**接口**”列可能不会将两个接口（*iscsi1*、*iscsi2*）都显示出来。对于某些目标，实际显示的是最近执行的命令中的接口（此例中为 *iscsi2*）。

使用 iSNS 服务器发现 iSCSI 目标

注意：iSNS 服务器必须已进行设置且在网络上可用，然后才能运行以下步骤。

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 Main_Menu > Settings > iSCSI 菜单。

3 键入 **Target Discover iSNS** 命令。

4 输入已配置为参数的 iSNS 服务器地址和 iSCSI 接口名称。

- iSNS 地址必须采用以下格式：<IPv4 地址或主机名>[:端口]。主机名可以是短名称或完全限定域名。默认端口为 3205。
  示例：192.116.50.50 或 abc:3205
- iSCSI 接口名称只能包含数字 (0-9)、字母（A-Z 和 a-z）、冒号 (:)、连字符 (-)、下划线 (_) 和句点 (.)。该名称只能以数字 (0-9)、字母（A-Z 和 a-z）和下划线 (_) 开头。

5 运行 **Target Discover iSNS <*iSNS 地址*> <*接口名称*>** 命令，以发现在特定接口上注册到 iSNS 服务器的所有 iSCSI 目标。

系统会提示您提供用户名和密码。如果您的目标需要身份验证，则键入 **yes**。

注意：当已在目标设备上启用 CHAP 身份验证并且已通过使用 iSNS 发现目标时，`iSCSI > Target Discover` 命令可能不会提示输入目标凭据。

```
Does your target require a username and password? (yes,no)[no]:no

Showing the discovered targets...

+-----+-------------------------|--------------------|---------------+
| No. |          Target IQN      |Target Portal Address|
Interfaces   |
+-----+-------------------------|--------------------|---------------|
|  1  | iqn.1996-03.veritas:abc  | 10.121.98.22:3260   | iscsi1,
 iscsi2 |
+-----+-------------------------|--------------------|---------------|
|  2  | iqn.1996-03.veritas:xyz  | 10.121.98.23:3260   | iscsi1,
 iscsi2 |
+-----+-------------------------|--------------------|---------------+
|  3  | iqn.1996-03.veritas:host | 10.121.98.24:3260   | iscsi1,
 iscsi2 |
------|-------------------------|--------------------|---------------|
```

连接到目标

发现启动器和目标连接后，iSCSI 启动器必须登录目标才能建立连接并通过 iSCSI 传输数据。如果服务器重新启动，则会保持登录状态，并且会自动还原连接（除非用户从目标注销）。

要将启动器连接到单个目标，请指定门户的 IP 地址和目标 IQN。

连接到目标

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Target Connect** 命令。

4 输入已发现目标的 IQN 和门户地址。如果在目标上启用身份验证，则必须输入用户名。

关于 IQN、门户地址和用户名，请注意以下几点：

- IQN 只能包含数字 (0-9)、字母（A-Z 和 a-z）、冒号 (:)、连字符 (-) 和句点 (.)
  示例：iqn.1999-06.com.veritas:storage.lun1
- 目标门户地址必须采用以下格式：**<IP 地址/主机名>[:端口]**。仅支持 IPv4 地址。主机名可以是短名称或完全限定域名。
  示例：192.116.116.50 或 abc:3260
- 用户名只能包含数字 (0-9)、字母（A-Z 和 a-z）、连字符 (-)、下划线 (_) 和句点 (.)。该名称只能以数字 (0-9)、字母（A-Z 和 a-z）和下划线 (_) 开头。
  示例：john.smith

5 运行命令以连接到目标。一次只能连接到一个已发现的目标。

断开与目标的会话

您可以使用 **iSCSI > Target Disconnect** 命令断开与具有特定 IQN 和门户地址的目标的会话。运行此命令后，将断开连接到此目标的所有会话。

一次只能断开与一个目标的会话。

注意：如果 iSCSI 接口上有工作量正在运行，则此命令需要更长时间才能完成。

断开与目标的会话

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Target Disconnect** 命令。

4 输入要断开连接的目标的 IQN 和门户地址。

关于 IQN 和门户地址，请注意以下几点：

- IQN 只能包含数字 (0-9)、字母（A-Z 和 a-z）、冒号 (:)、连字符 (-) 和句点 (.)
  示例：iqn.1999-06.com.veritas:storage.lun1
- 目标门户地址必须采用以下格式：**<IPv4 地址/主机名>[:端口]**。主机名可以是短名称或完全限定域名。
  示例：192.116.116.50 或 abc:3260

5 运行命令以断开与特定目标的会话。出现以下提示时，键入 **yes**：

```
Do you want to disconnect the target session?[yes, no](no):yes

[Info] The target session has been disconnected.
```

查看目标

本节提供了有关如何查看目标的说明。您可以使用 **iSCSI > Target Show** 命令查看所有已发现的目标或已连接的目标。

查看已连接的目标

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Target Show Connected** 命令，然后按 **Enter**。

4 按以下方式显示已连接目标的列表：

```
Showing the connected targets...

+-----+------------+----------------------+----------------------+--------+
| No. | Session ID |      Target IQN      | Target Portal Address| Status |
+-----+------------+----------------------+----------------------|--------+
|  1  |     5      |iqn.1996-03.veritas:abc|   10.121.37.51:3260  | Online 1     |
+-----+------------+----------------------+----------------------+--------+
```

会话“**状态**”可能是“**联机**”或“**脱机**”。如果拔出电缆或存在网络连接性问题，则“**状态**”可能是“**脱机**”。

查看所有可用的目标

1 打开安全外壳 (SSH) 会话，以管理员身份登录设备。

2 导航到 **Main_Menu > Settings > iSCSI** 菜单。

3 键入 **Target Show All** 命令，然后按 **Enter**。

4 按以下方式显示所有已发现目标的列表：

```
Showing all the targets...

+-----+------------------------|---------------------|-----------+
| No. |      Target IQN        |Target Portal Address|Interfaces |
+-----+------------------------|---------------------|-----------|
|  1  |iqn.1996-03.veritas:abc | 10.121.98.22:3260   | iscsi1    |
+-----+------------------------|---------------------|-----------|
|  2  |iqn.1996-03.veritas:xyz | 10.121.98.23:3260   | iscsi1    |
+-----+------------------------|---------------------|-----------+
|  3  |iqn.1996-03.veritas:host| 10.121.98.24:3260   | iscsi1    |
------|------------------------|---------------------|-----------|
```

注意：在两个 iSCSI 接口上使用 iSNS 发现目标时，`Target Show All` 命令只显示最近的记录。例如，如果先后针对 *iscsi1* 和 *iscsi2* 运行 `Target Discover iSNS` 命令，则对于某些目标，`Target Show All` 命令中的 **Interfaces** 列可能不会将两个接口（*iscsi1*、*iscsi2*）都显示出来。对于某些目标，实际显示的是最近执行的命令中的接口（此例中为 *iscsi2*）。

5

对 iSCSI 问题进行故障排除和一些最佳做法

本章节包括下列主题：

收集 NetBackup Appliance 上的设备日志

可以使用 Main > Support Shell 菜单中的 Datacollect 命令收集设备日志。可以和 Veritas 支持团队共享这些设备日志，以解决设备相关问题。

DataCollect 命令可收集以下日志：

- 版本信息
- 磁盘性能日志
- 命令输出日志
- iSCSI 日志

注意：可以在 /var/log/messages 和 /var/log/iscsiuio.log 中找到 iSCSI 日志。

- CPU 信息
- 内存信息
- 操作系统日志

- 修补程序日志
- 存储日志
- 文件系统日志
- 测试硬件日志
- AutoSupport 日志
- 硬件信息
- Sysinfo 日志

通过 DataCollect 命令收集设备日志

1 登录到 NetBackup Appliance 命令行操作界面。

2 从 `Main > Support` 视图中，键入以下命令以收集设备日志。

```
DataCollect
```

设备会在 `/tmp/DataCollect.zip` 文件中生成设备日志。

3 使用 `Main > Support > Logs > Share Open` 命令将 `DataCollect.zip` 复制到本地文件夹。

4 可以将 `DataCollect.zip` 文件发送到 Veritas 支持团队以解决问题。

关于 syslogd 消息

您可能会在 NetBackup Appliance 命令行操作界面中看到以下消息：

```
Message from syslogd@host at Sep 12 10:09:14 ...
iscsid:

Message from syslogd@host at Sep 12 10:13:27 ...
iscsid:

Message from syslogd@host at Sep 12 10:17:53 ...
iscsid:
```

这些消息可能在不同的时间在 NetBackup Appliance 命令行操作界面中出现。运行 iSCSI 命令时、在命令输出中、甚至在控制台闲置时都可能出现这些消息。这些消息没有不利影响，应将其忽略。

关于 iSCSI 警报

如果为特定设备配置了警报，还可以接收 iSCSI 警报（如适用）。以下情况下将生成 iSCSI 警报：

- 与目标的 iSCSI 会话断开 (V-475-108-1000)
- 与目标存储服务器的 iSCSI 会话脱机 (V-475-108-1001)
- 10 GB 以太网/iSCSI 卡中检测到不支持的小型可插拔 (SFP+) 模块 (V-475-107-1000)

以下为 iSCSI 警报示例：

```
An iSCSI session with the target has been disconnected.
Time of event: 2016-09-09 21:34:13 (-07:00)
UMI Event code: V-475-108-1000
Component Type: Connections
Component: <Target IQN> <Portal address> <Interface name>
Status: Disconnected
State: ERROR
Additional information about this error is available at following
link: V-475-108-1000

An iSCSI session with the target storage server is offline.
Time of event: 2016-10-13 21:34:13 (-07:00)
UMI Event code: V-475-108-1001
Component Type: Connections
Component: <Target IQN> <Portal address> <Interface name>
Status: Offline
State: ERROR
Additional information about this error is available at following
link: V-475-108-1001

The SFP+ module that is currently installed in the 10Gb Ethernet/iSCSI

card is not supported.
Time of event: 2016-10-06 18:31:42 (-07:00)
UMI Event code: V-475-107-1000
Component Type: Ethernet
Component: PCIe slot 6, port 1 SFP
Status: Unsupported
State: ERROR
Additional information about this error is available at following
link: V-475-500-1000
```

最佳做法

以下是针对 iSCSI 的一些建议和最佳做法：

- 配置与默认值不同的 IQN。
  请参见第 19 页的“为启动器设置 IQN”。
- 配置警报，以便可以收到与 iSCSI 相关的警报。
  有关配置警报的信息，请参见《NetBackup Appliance 管理指南》。