iSCSI 服务管理

ONTAP 9

NetApp
April 24, 2024

目录

iSCSI 服务管理 1
iSCSI 服务管理 1
iSCSI 身份验证的工作原理 1
iSCSI 启动程序安全管理 2
iSCSI 端点隔离 2
什么是 CHAP 身份验证 2
使用 iSCSI 接口访问列表限制启动程序接口如何提高性能和安全性 3
Internet存储名称服务(iSNS) 3

iSCSI 服务管理

iSCSI 服务管理

您可以使用管理Storage Virtual Machine (SVM)的iSCSI逻辑接口上iSCSI服务的可用性 `vserver iscsi interface enable` 或 `vserver iscsi interface disable` 命令

默认情况下， iSCSI 服务在所有 iSCSI 逻辑接口上都处于启用状态。

如何在主机上实施 iSCSI

iSCSI 可以使用硬件或软件在主机上实施。

您可以通过以下方式之一实施 iSCSI：

- 使用使用使用主机标准以太网接口的启动程序软件。
- 通过 iSCSI 主机总线适配器（ HBA ）： iSCSI HBA 在主机操作系统中显示为带有本地磁盘的 SCSI 磁盘适配器。
- 使用 TCP 卸载引擎（ TOE ）适配器卸载 TCP/IP 处理。

  iSCSI 协议处理仍由主机软件执行。

iSCSI 身份验证的工作原理

在 iSCSI 会话的初始阶段，启动程序会向存储系统发送登录请求，以启动 iSCSI 会话。然后，存储系统会允许或拒绝登录请求，或者确定不需要登录。

iSCSI 身份验证方法包括：

- 质询握手身份验证协议（ CHAP ）—启动程序使用 CHAP 用户名和密码登录。

  您可以指定 CHAP 密码或生成十六进制密码。CHAP 用户名和密码有两种类型：

  - 入站—存储系统对启动程序进行身份验证。

    如果使用 CHAP 身份验证，则需要入站设置。

  - 出站—这是一个可选设置，用于使启动程序能够对存储系统进行身份验证。

    只有在存储系统上定义了入站用户名和密码时，才能使用出站设置。

- deny-- 拒绝启动程序访问存储系统。
- 无—存储系统不需要对启动程序进行身份验证。

您可以定义启动程序及其身份验证方法的列表。您还可以定义不在此列表中的适用场景启动程序的默认身份验证方法。

相关信息

"采用 Data ONTAP 的 Windows 多路径选项：光纤通道和 iSCSI"

iSCSI 启动程序安全管理

ONTAP 提供了许多用于管理 iSCSI 启动程序安全性的功能。您可以定义 iSCSI 启动程序列表以及每个启动程序的身份验证方法，在身份验证列表中显示启动程序及其关联的身份验证方法，在身份验证列表中添加和删除启动程序，以及为不在列表中的启动程序定义默认 iSCSI 启动程序身份验证方法。

iSCSI 端点隔离

从 ONTAP 9.1 开始，现有的 iSCSI 安全命令已得到增强，可接受一个 IP 地址范围或多个 IP 地址。

在与目标建立会话或连接时，所有 iSCSI 启动程序都必须提供源 IP 地址。如果源 IP 地址不受支持或未知，此新功能可防止启动程序登录到集群，从而提供唯一的标识方案。如果任何启动程序的 IP 地址不受支持或未知，则会在 iSCSI 会话层拒绝其登录，从而阻止启动程序访问集群中的任何 LUN 或卷。

使用两个新命令实施此新功能，以帮助管理原有条目。

添加启动程序地址范围

通过使用添加IP地址范围或多个IP地址来改进iSCSI启动程序安全性管理 `vserver iscsi security add-initiator-address-range` 命令：

```
cluster1::> vserver iscsi security add-initiator-address-range
```

删除启动程序地址范围

使用删除一个或多个IP地址范围 `vserver iscsi security remove-initiator-address-range` 命令：

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

什么是 CHAP 身份验证

使用质询握手身份验证协议（ CHAP ）可以在 iSCSI 启动程序和目标之间进行经过身份验证的通信。使用 CHAP 身份验证时，您可以在启动程序和存储系统上定义 CHAP 用户名和密码。

在 iSCSI 会话的初始阶段，启动程序会向存储系统发送登录请求以启动会话。登录请求包括启动程序的 CHAP 用户名和 CHAP 算法。存储系统会响应 CHAP 质询。启动程序提供 CHAP 响应。存储系统会验证响应并对启动程序进行身份验证。CHAP 密码用于计算响应。

使用 CHAP 身份验证的准则

使用 CHAP 身份验证时，应遵循特定准则。

- 如果您在存储系统上定义了入站用户名和密码，则必须对启动程序上的出站 CHAP 设置使用相同的用户名和密码。如果您还在存储系统上定义了出站用户名和密码以启用双向身份验证，则必须对启动程序上的入站 CHAP 设置使用相同的用户名和密码。
- 存储系统上的入站和出站设置不能使用相同的用户名和密码。
- CHAP 用户名可以是 1 到 128 个字节。

  不允许使用空用户名。

- CHAP 密码（密码）可以是 1 到 512 字节。

  密码可以是十六进制值或字符串。对于十六进制值，应输入前缀为 "`0x` " 或 "`0x` " 的值。不允许使用空密码。

> ONTAP 允许对CHAP密码(密码)使用特殊字符、非英语字母、数字和空格。 但是、此操作受主机限制的约束。 如果您的特定主机不允许使用其中任何一种、则无法使用它们。
>
> 例如，如果未使用 IPsec 加密， Microsoft iSCSI 软件启动程序要求启动程序和目标 CHAP 密码至少为 12 字节。无论是否使用 IPsec ，最大密码长度均为 16 字节。
>
> 有关其他限制，请参见启动程序的文档。

使用 iSCSI 接口访问列表限制启动程序接口如何提高性能和安全性

iSCSI 接口访问列表可用于限制 SVM 中启动程序可以访问的 LIF 数量，从而提高性能和安全性。

启动程序使用iSCSI启动发现会话时 `SendTargets` 命令时、它会接收与访问列表中的LIF (网络接口)关联的IP地址。默认情况下，所有启动程序都可以访问 SVM 中的所有 iSCSI LIF 。您可以使用访问列表限制启动程序可以访问的 SVM 中的 LIF 数量。

Internet存储名称服务(iSNS)

Internet 存储名称服务（ iSNS ）是一种协议，可用于自动发现和管理 TCP/IP 存储网络上的 iSCSI 设备。iSNS 服务器会维护有关网络上活动 iSCSI 设备的信息，包括其 IP 地址，iSCSI 节点名称 IQN 和门户组。

您可以从第三方供应商处获取 iSNS 服务器。如果网络上配置了 iSNS 服务器并使其可供启动程序和目标使用，则可以使用 Storage Virtual Machine （ SVM ）的管理 LIF 在 iSNS 服务器上注册该 SVM 的所有 iSCSI LIF 。注册完成后， iSCSI 启动程序可以查询 iSNS 服务器以发现该特定 SVM 的所有 LIF 。

如果决定使用 iSNS 服务，则必须确保已将 Storage Virtual Machine （ SVM ）正确注册到 Internet 存储名称服务（ iSNS ）服务器。

如果网络上没有 iSNS 服务器，则必须手动配置每个目标，使其对主机可见。

iSNS 服务器的功能

iSNS 服务器使用 Internet 存储名称服务（ iSNS ）协议来维护有关网络上活动 iSCSI 设备的信息，包括其 IP 地址， iSCSI 节点名称（ IQN ）和门户组。

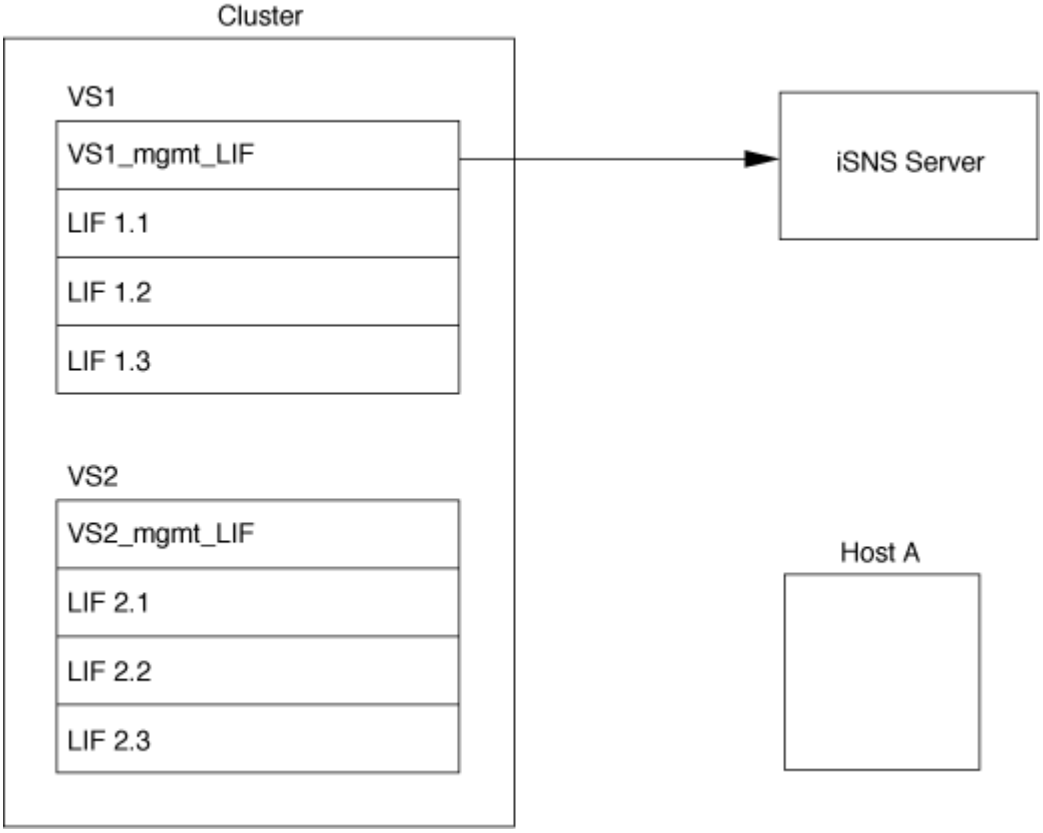
通过 iSNS 协议，可以自动发现和管理 IP 存储网络上的 iSCSI 设备。iSCSI 启动程序可以查询 iSNS 服务器以发现 iSCSI 目标设备。

NetApp 不提供或转售 iSNS 服务器。您可以从 NetApp 支持的供应商处获取这些服务器。

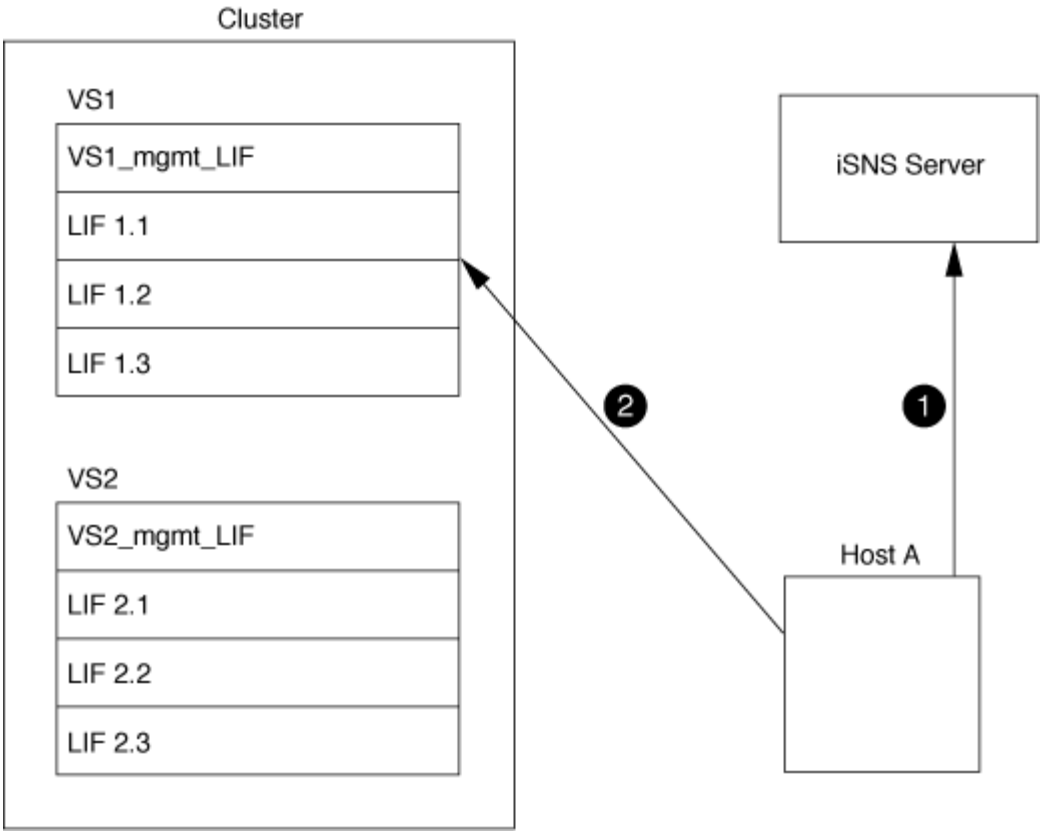
SVM 如何与 iSNS 服务器交互

iSNS 服务器通过 SVM 管理 LIF 与每个 Storage Virtual Machine （ SVM ）进行通信。管理 LIF 会将所有 iSCSI 目标节点名称，别名和门户信息注册到特定 SVM 的 iSNS 服务中。

在以下示例中、SVM"`VS1`"使用SVM管理LIF "`VS1_mgmt_lif`"向iSNS服务器注册。在 iSNS 注册期间， SVM 会通过 SVM 管理 LIF 将所有 iSCSI LIF 发送到 iSNS 服务器。iSNS注册完成后、iSNS服务器会显示一个列表、其中列出了"`VS1`"中为iSCSI提供服务的所有LUN。如果集群包含多个 SVM ，则每个 SVM 都必须分别向 iSNS 服务器注册才能使用 iSNS 服务。



在下一个示例中、iSNS服务器完成目标注册后、主机A可按步骤1中所述、通过iSNS服务器发现"`VS1`"的所有L文件。在主机A完成"`VS1`"的查找后、主机A可以与"`VS1`"中的任何一个L建立连接、如步骤2所示。在将管理LIF "`VS2`"的` VS2_mgmt_LIF`"注册到iSNS服务器之前、主机A无法识别"`VS2`"中的任何LIF。



但是，如果定义了接口访问列表，则主机只能使用接口访问列表中定义的 LIF 来访问目标。

初始配置 iSNS 后，当 SVM 配置设置发生更改时， ONTAP 会自动更新 iSNS 服务器。

从更改配置到ONTAP向iSNS服务器发送更新、可能会有几分钟的延迟。强制立即更新iSNS服务器上的iSNS信息： `vserver iscsi isns update`

用于管理 iSNS 的命令

ONTAP 提供了用于管理 iSNS 服务的命令。

如果您要 …	使用此命令 …
配置 iSNS 服务	`vserver iscsi isns create`
启动 iSNS 服务	`vserver iscsi isns start`
修改 iSNS 服务	`vserver iscsi isns modify`
显示 iSNS 服务配置	`vserver iscsi isns show`
强制更新已注册的 iSNS 信息	`vserver iscsi isns update`
停止 iSNS 服务	`vserver iscsi isns stop`

删除 iSNS 服务	`vserver iscsi isns delete`
查看命令的手册页	`man` *`command name`*

有关详细信息，请参见每个命令的手册页。