



使用命令行界面访问集群（仅限集群管理员） ONTAP 9

NetApp
February 12, 2026

目录

使用命令行界面访问集群（仅限集群管理员）	1
使用节点串行端口访问ONTAP集群	1
使用SSH请求访问ONTAP集群	1
ONTAP SSH登录安全性	4
有关 SSH 登录安全性的限制和其他注意事项	4
SSH 登录安全信息示例	5
启用对ONTAP集群的Telnet或RSH访问	5
使用Telnet请求访问ONTAP集群	7
使用RSH请求访问ONTAP集群	10

使用命令行界面访问集群（仅限集群管理员）

使用节点串行端口访问ONTAP集群

您可以直接从连接到节点串行端口的控制台访问集群。

步骤

1. 在控制台中，按 Enter 键。

系统将响应登录提示。

2. 在登录提示符处，执行以下操作之一：

要使用以下项访问集群 ...	输入以下帐户名称 ...
默认集群帐户	admin
一种备用管理用户帐户	<i>username</i>

系统将提示您输入密码。

3. 输入管理员或管理用户帐户的密码，然后按 Enter 键。

使用SSH请求访问ONTAP集群

您可以通过向ONTAP集群发出问题描述SSH请求来执行管理任务。默认情况下、SSH处于启用状态。

开始之前

- 您必须具有配置为使用的用户帐户 `ssh` 作为访问方法。

```
`-application`命令的参数 `security  
login`用于指定用户帐户的访问方法。有关的详细信息 `security login`  
，请参见link:https://docs.netapp.com/us-en/ontap-cli/security-login-  
create.html#description["ONTAP 命令参考"^]。
```

- 如果您使用Active Directory (AD)域用户帐户访问集群、则必须已通过启用了CIFS的Storage VM为集群设置身份验证通道、并且您的AD域用户帐户也必须已通过添加到集群中 `ssh` 作为一种访问方法、然后 `domain` 作为身份验证方法。

关于此任务

- 您必须使用 OpenSSH 5.7 或更高版本的客户端。
- 仅支持 SSH v2 协议；不支持 SSH v1 。
- ONTAP支持每个节点最多64个并发SSH会话。

如果集群管理 LIF 驻留在节点上，则它与节点管理 LIF 共享此限制。

如果传入连接的速率高于每秒 10 次，则此服务将暂时禁用 60 秒。

- ONTAP 仅支持对 SSH 使用 AES 和 3DES 加密算法（也称为 *ciphers*）。

AES 支持 128，192 和 256 位密钥长度。3DES 的密钥长度为 56 位，与原始 DES 相同，但重复三次。

- 启用 FIPS 模式后，SSH 客户端应与椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA）公有密钥算法协商，以便成功进行连接。
- 如果要从 Windows 主机访问 ONTAP 命令行界面，可以使用 PuTTY 等第三方实用程序。
- 如果使用 Windows AD 用户名登录到 ONTAP，则应使用在 ONTAP 中创建 AD 用户名和域名时使用的相同大小写字母。

AD 用户名和域名不区分大小写。但是，ONTAP 用户名区分大小写。如果在 ONTAP 中创建的用户名与在 AD 中创建的用户名的大小写不匹配，则会导致登录失败。

SSH 身份验证选项

- 从 ONTAP 9.3 开始、您可以执行此操作 ["启用 SSH 多因素身份验证"](#) 本地管理员帐户。

启用 SSH 多因素身份验证后，用户将使用公有密钥和密码进行身份验证。

- 从 ONTAP 9.4 开始、您可以执行此操作 ["启用 SSH 多因素身份验证"](#) LDAP 和 NIS 远程用户。
- 从 ONTAP 9.13.1 开始、您可以选择在 SSH 身份验证过程中添加证书验证、以增强登录安全性。为此、"[将 X.509 证书与公共密钥相关联](#)" 帐户使用的。如果使用 SSH 公共密钥和 X.509 证书登录、则 ONTAP 会在使用 SSH 公共密钥进行身份验证之前检查 X.509 证书的有效性。如果此证书已过期或已撤销、则会拒绝 SSH 登录、并且 SSH 公共密钥会自动禁用。
- 从 ONTAP 9.14.1 开始、ONTAP 管理员可以执行此操作 ["在 SSH 身份验证过程中添加 Cisco Duo 双重身份验证"](#) 以增强登录安全性。启用 Cisco Duo 身份验证后首次登录时、用户需要注册一个设备、以用作 SSH 会话的身份验证程序。
- 从 ONTAP 9.15.1 开始、管理员可以执行此操作 ["配置动态授权"](#) 根据 SSH 用户的信任得分向用户提供额外的自适应身份验证。

步骤

1. 在可访问 ONTAP 集群网络的主机上、输入 `ssh` 命令、格式为以下之一：

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

如果您使用的是 AD 域用户帐户、则必须指定 `username` 格式为 `domainname\AD_accountname` (域名后使用双反斜斜槽) 或 `"domainname\AD_accountname"` (用双引号括起来、域名后加一个反斜杠)。

`hostname_or_IP` 是集群管理 LIF 或节点管理 LIF 的主机名或 IP 地址。建议使用集群管理 LIF。您可以使用 IPv4 或 IPv6 地址。

`command` SSH 交互式会话不需要。

SSH 请求示例

以下示例显示了名为 "Joe" 的用户帐户如何通过问题描述处理 SSH 请求来访问集群管理 LIF 为 10.72.137.28

的集群:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

以下示例显示了名为 DOMAIN1 的域中名为 "John`" 的用户帐户如何通过问题描述发出 SSH 请求来访问集群管理 LIF 为 10.72.137.28 的集群:

```
$ ssh DOMAIN1\\joh@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\joh" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

以下示例显示了名为 "joe`" 的用户帐户如何通过问题描述处理 SSH MFA 请求来访问集群管理 LIF 为 10.72.137.32 的集群:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

相关信息

["管理员身份验证和 RBAC"](#)

ONTAP SSH登录安全性

从 ONTAP 9.5 开始，您可以查看有关先前登录，未成功登录尝试以及自上次成功登录以来权限更改的信息。

以 SSH 管理员用户身份成功登录后，系统将显示与安全相关的信息。系统会就以下情况向您发出警报：

- 您的帐户名称上次登录的时间。
- 自上次成功登录以来失败的登录尝试次数。
- 角色自上次登录以来是否发生了更改（例如，如果管理员帐户的角色从 "admin" 更改为 "backup"。）
- 自上次登录以来是否修改了角色的添加，修改或删除功能。



如果显示的任何信息可疑，您应立即联系安全部门。

要在登录时获取此信息，必须满足以下前提条件：

- 必须在 ONTAP 中配置 SSH 用户帐户。
- 必须创建 SSH 安全登录。
- 您的登录尝试必须成功。

有关 SSH 登录安全性的限制和其他注意事项

以下限制和注意事项适用于 SSH 登录安全信息：

- 此信息仅适用于基于 SSH 的登录。
- 对于基于组的管理员帐户，例如 LDAP/NIS 和 AD 帐户，如果用户所属的组在 ONTAP 中配置为管理员帐户，则用户可以查看 SSH 登录信息。

但是，无法为这些用户显示有关用户帐户角色更改的警报。此外，属于已在 ONTAP 中配置为管理员帐户的 AD 组的用户无法查看自上次登录以来失败登录尝试的次数。

- 从 ONTAP 中删除用户帐户后，为用户维护的信息将被删除。
- 对于与 SSH 以外的应用程序的连接，不会显示此信息。

SSH 登录安全信息示例

以下示例展示了登录后显示的信息类型。

- 每次成功登录后，都会显示此消息：

```
Last Login : 7/19/2018 06:11:32
```

- 如果自上次成功登录以来尝试登录失败，则会显示以下消息：

```
Last Login : 4/12/2018 08:21:26  
Unsuccessful login attempts since last login - 5
```

- 如果自上次成功登录以来尝试登录失败，并且您的权限已被修改，则会显示以下消息：

```
Last Login : 8/22/2018 20:08:21  
Unsuccessful login attempts since last login - 3  
Your privileges have changed since last login
```

启用对ONTAP集群的Telnet或RSH访问

作为一项安全最佳实践、默认情况下会禁用Telnet和RSH。要使集群能够接受Telnet或RSH请求、必须在默认管理服务策略中启用该服务。

Telnet和RSH不是安全协议；您应考虑使用SSH访问集群。SSH 可提供安全的远程 shell 和交互式网络会话。有关详细信息，请参阅 ["使用SSH访问集群"](#)。

关于此任务

- ONTAP最多支持每个节点50个并发Telnet或RSH会话。

如果集群管理 LIF 驻留在节点上，则它与节点管理 LIF 共享此限制。

如果传入连接的速率高于每秒 10 次，则此服务将暂时禁用 60 秒。

- rsh命令需要高级权限。

ONTAP 9. 10.1或更高版本

步骤

1. 确认RSH或Telnet安全协议已启用：

```
security protocol show
```

- a. 如果已启用RSH或Telnet安全协议、请继续执行下一步。
- b. 如果未启用RSH或Telnet安全协议、请使用以下命令启用它：

```
security protocol modify -application <rsh/telnet> -enabled true
```

有关和的 `security protocol modify` 详细信息、`security protocol show`，请参见["ONTAP 命令参考"](#)。

2. 确认 `management-rsh-server` 或 `management-telnet-server` 服务位于管理生命周期管理中：

```
network interface show -services management-rsh-server
```

或

```
network interface show -services management-telnet-server
```

有关的详细信息 `network interface show`，请参见["ONTAP 命令参考"](#)。

- a. 如果 `management-rsh-server` 存在或 `management-telnet-server` 服务、请继续执行下一步。
- b. 如果 `management-rsh-server` 或 `management-telnet-server` 服务不存在、请使用以下命令进行添加：

```
network interface service-policy add-service -vserver cluster1 -policy default-management -service management-rsh-server
```

```
network interface service-policy add-service -vserver cluster1 -policy default-management -service management-telnet-server
```

有关的详细信息 `network interface service-policy add-service`，请参见["ONTAP 命令参考"](#)。

ONTAP 9.9 或更早版本

关于此任务

ONTAP会阻止您更改预定义的防火墙策略、但您可以通过克隆预定义的 `'mgmt'` 管理防火墙策略、然后在此新策略下启用Telnet或RSH来创建新策略。

步骤

1. 进入高级权限模式：

```
set advanced
```

2. 启用安全协议（RSH 或 Telnet）：

```
security protocol modify -application security_protocol -enabled true
```

3. 根据 `mgmt` 管理防火墙策略创建新的管理防火墙策略：

```
system services firewall policy clone -policy mgmt -destination-policy  
policy-name
```

4. 在新的管理防火墙策略中启用 Telnet 或 RSH：

```
system services firewall policy create -policy policy-name -service  
security_protocol -action allow -ip-list ip_address/netmask
```

要允许所有 IP 地址、应指定 `-ip-list 0.0.0.0/0`

5. 将新策略与集群管理 LIF 关联：

```
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt  
-firewall-policy policy-name
```

有关的详细信息 `network interface modify`，请参见["ONTAP 命令参考"](#)。

使用 Telnet 请求访问 ONTAP 集群

您可以通过问题描述向集群发送 Telnet 请求来执行管理任务。默认情况下，Telnet 处于禁用状态。

Telnet 和 RSH 不是安全协议；您应考虑使用 SSH 访问集群。SSH 可提供安全的远程 shell 和交互式网络会话。有关详细信息，请参阅 ["使用 SSH 访问集群"](#)。

开始之前

在使用 Telnet 访问集群之前，必须满足以下条件：

- 您必须拥有一个集群本地用户帐户，该帐户必须配置为使用 Telnet 作为访问方法。

```
`-application` 命令的参数 `security  
login` 用于指定用户帐户的访问方法。有关的详细信息 `security login`  
，请参见 link:https://docs.netapp.com/us-en/ontap-  
cli/search.html?q=security+login ["ONTAP 命令参考"]。
```

关于此任务

- ONTAP 最多支持每个节点 50 个并发 Telnet 会话。

如果集群管理 LIF 驻留在节点上，则它与节点管理 LIF 共享此限制。

如果传入连接的速率高于每秒 10 次，则此服务将暂时禁用 60 秒。

- 如果要从 Windows 主机访问 ONTAP 命令行界面，可以使用 PuTTY 等第三方实用程序。
- rsh命令需要高级权限。

ONTAP 9. 10.1或更高版本

步骤

1. 确认已启用Telnet安全协议:

```
security protocol show
```

- a. 如果已启用Telnet安全协议、请继续执行下一步。
- b. 如果未启用Telnet安全协议、请使用以下命令启用它:

```
security protocol modify -application telnet -enabled true
```

有关和的 `security protocol modify` 详细信息、`security protocol show`, 请参见"ONTAP 命令参考"。

2. 确认此 `management-telnet-server` 服务位于管理生命周期管理中:

```
network interface show -services management-telnet-server
```

有关的详细信息 `network interface show`, 请参见"ONTAP 命令参考"。

- a. 如果存在此 `management-telnet-server` 服务、请继续执行下一步。
- b. 如果此 `management-telnet-server` 服务不存在、请使用以下命令进行添加:

```
network interface service-policy add-service -vserver cluster1 -policy default-management -service management-telnet-server
```

有关的详细信息 `network interface service-policy add-service`, 请参见"ONTAP 命令参考"。

ONTAP 9.9 或更早版本

开始之前

在使用 Telnet 访问集群之前, 必须满足以下条件:

- 必须已在集群或节点管理 LIF 使用的管理防火墙策略中启用 Telnet, 以便 Telnet 请求可以通过防火墙。

默认情况下, Telnet 处于禁用状态。 `system services firewall policy show` 命令和 `-service telnet` 参数用于显示是否已在防火墙策略中启用 Telnet。 有关的详细信息 `system services firewall policy`, 请参见"ONTAP 命令参考"。

- 如果使用 IPv6 连接, 则必须已在集群上配置并启用 IPv6, 并且防火墙策略必须已配置 IPv6 地址。

```
network options ipv6 show 命令用于显示是否已启用 IPv6。 有关的详细信息 network options ipv6 show, 请参见 link:https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html ["ONTAP 命令参考"]。  
system services firewall policy show 命令可显示防火墙策略。
```

步骤

1. 在管理主机中，输入以下命令：

```
telnet hostname_or_IP
```

`hostname_or_IP` 是集群管理 LIF 或节点管理 LIF 的主机名或 IP 地址。建议使用集群管理 LIF。您可以使用 IPv4 或 IPv6 地址。

Telnet 请求示例

以下示例显示了名为“joe”的用户（已设置 Telnet 访问权限）如何发出 Telnet 请求来访问集群管理 LIF 为 10.72.137.28 的集群：

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

使用 RSH 请求访问 ONTAP 集群

您可以通过问题描述向集群发送 RSH 请求来执行管理任务。RSH 不是安全协议，默认情况下处于禁用状态。

Telnet 和 RSH 不是安全协议；您应考虑使用 SSH 访问集群。SSH 可提供安全的远程 shell 和交互式网络会话。有关详细信息，请参阅 ["使用 SSH 访问集群"](#)。

开始之前

在使用 RSH 访问集群之前，必须满足以下条件：

- 您必须拥有一个集群本地用户帐户，该帐户必须配置为使用 RSH 作为访问方法。

```
`-application` 命令的参数 `security
login` 用于指定用户帐户的访问方法。有关的详细信息 `security login`
，请参见 link:https://docs.netapp.com/us-en/ontap-
cli/search.html?q=security+login ["ONTAP 命令参考"^]。
```

关于此任务

- ONTAP 最多支持每个节点 50 个并发 RSH 会话。

如果集群管理 LIF 驻留在节点上，则它与节点管理 LIF 共享此限制。

如果传入连接的速率高于每秒 10 次，则此服务将暂时禁用 60 秒。

- rsh命令需要高级权限。

ONTAP 9. 10.1或更高版本

步骤

1. 确认RSH安全协议已启用:

```
security protocol show
```

- a. 如果已启用RSH安全协议、请继续执行下一步。
- b. 如果未启用RSH安全协议、请使用以下命令启用它:

```
security protocol modify -application rsh -enabled true
```

有关和的 `security protocol modify` 详细信息、`security protocol show`，请参见"[ONTAP 命令参考](#)"。

2. 确认此 `management-rsh-server` 服务位于管理生命周期管理中:

```
network interface show -services management-rsh-server
```

有关的详细信息 `network interface show`，请参见"[ONTAP 命令参考](#)"。

- a. 如果存在此 `management-rsh-server` 服务、请继续执行下一步。
- b. 如果此 `management-rsh-server` 服务不存在、请使用以下命令进行添加:

```
network interface service-policy add-service -vserver cluster1 -policy default-management -service management-rsh-server
```

有关的详细信息 `network interface service-policy add-service`，请参见"[ONTAP 命令参考](#)"。

ONTAP 9.9 或更早版本

开始之前

在使用 RSH 访问集群之前，必须满足以下条件:

- 集群或节点管理 LIF 使用的管理防火墙策略必须已启用 RSH，以便 RSH 请求可以通过防火墙。

默认情况下、RSH处于禁用状态。带有 `-service rsh` 参数的 `system services 防火墙策略 show` 命令用于显示是否已在防火墙策略中启用RSH。有关的详细信息 `system services firewall policy`，请参见"[ONTAP 命令参考](#)"。

- 如果使用 IPv6 连接，则必须已在集群上配置并启用 IPv6，并且防火墙策略必须已配置 IPv6 地址。

```
`network options ipv6 show`命令用于显示是否已启用IPv6。有关的详细信息  
`network options ipv6 show`，请参见link:https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html["ONTAP 命令参考"]。  
`system services firewall policy show`命令可显示防火墙策略。
```

步骤

1. 在管理主机中，输入以下命令：

```
rsh hostname_or_IP -l username:passwordcommand
```

`hostname_or_IP`是集群管理LIF或节点管理LIF的主机名或IP地址。建议使用集群管理 LIF 。您可以使用 IPv4 或 IPv6 地址。

`command`是要通过RSH执行的命令。

RSH请求示例

以下示例显示了已设置RSH访问权限的用户"Joe"如何通过问题描述处理RSH请求来运行 `cluster show` 命令：

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

```
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
admin_host$
```

有关的详细信息 `cluster show`，请参见["ONTAP 命令参考"](#)。

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。