



管理SNMP (仅限集群管理员)

ONTAP 9

NetApp
February 12, 2026

目录

管理SNMP (仅限集群管理员)	1
了解ONTAP网络上的SNMP	1
MIB概述	1
SNMP 陷阱	1
标准 SNMP 陷阱	2
内置 SNMP 陷阱	2
为ONTAP网络创建SNMP社区	2
在ONTAP集群中配置SNMPv3用户	4
SNMPv3 安全参数	5
不同安全级别的示例	5
在ONTAP网络上为SNMP配置陷阱主机	8
验证ONTAP集群中的SNMP轮询	9
用于管理SNMP、陷阱和陷阱主机的ONTAP命令	10
用于配置 SNMP 的命令	10
用于管理 SNMP v1 , v2c 和 v3 用户的命令	10
用于提供联系人和位置信息的命令	11
用于管理 SNMP 社区的命令	11
用于显示 SNMP 选项值的命令	11
用于管理 SNMP 陷阱和陷阱主机的命令	11
用于管理与 SNMP 陷阱相关的事件的命令	12

管理SNMP (仅限集群管理员)

了解ONTAP网络上的SNMP

您可以将 SNMP 配置为监控集群中的 SVM ，以便在出现问题之前避免出现问题，并在出现问题时对问题做出响应。管理 SNMP 涉及配置 SNMP 用户以及为所有 SNMP 事件配置 SNMP 陷阱主机目标（管理工作站）。默认情况下，SNMP 在数据 LIF 上处于禁用状态。

您可以在数据 SVM 中创建和管理只读 SNMP 用户。必须配置数据 LIF 以接收 SVM 上的 SNMP 请求。

SNMP 网络管理工作站或管理器可以向 SVM SNMP 代理查询相关信息。SNMP 代理会收集信息并将其转发给 SNMP 管理器。SNMP 代理还会在发生特定事件时生成陷阱通知。SVM 上的 SNMP 代理具有只读权限；不能用于任何设置的操作或针对陷阱采取更正操作。ONTAP 提供了一个与 SNMP v1 ， v2c 和 v3 版本兼容的 SNMP 代理。SNMPv3 通过使用密码短语和加密提供高级安全性。

有关 ONTAP 系统中 SNMP 支持的详细信息，请参见 ["TR-4220：Data ONTAP 中的 SNMP 支持"](#)。

MIB概述

MIB（管理信息库）是一个文本文件，用于描述 SNMP 对象和陷阱。

MIB 用于描述存储系统管理数据的结构，它们使用包含对象标识符（OID）的分层命名空间。每个 OID 标识一个可使用 SNMP 读取的变量。

由于 MIB 不是配置文件，并且 ONTAP 不会读取这些文件，因此 SNMP 功能不受 MIB 的影响。ONTAP 提供了以下 MIB 文件：

- NetApp自定义MIB (netapp.mib)

ONTAP 支持 IPv6（RFC 2465），TCP（RFC 4022），UDP（RFC 4113）和 ICMP（RFC 2466）MIB，这些 MIB 可显示 IPv4 和 IPv6 数据。

ONTAP还在中的对象标识符(OID)和对象短名称之间提供了一个简短的交叉引用 traps.dat 文件



ONTAP MIB 和“traps.dat”文件的最新版本可从 NetApp 支持站点获得。但是，支持站点上这些文件的版本不一定与 ONTAP 版本的 SNMP 功能相对应。提供这些文件是为了帮助您评估最新 ONTAP 版本中的 SNMP 功能。

SNMP 陷阱

SNMP 陷阱用于捕获系统监控信息，此信息将作为异步通知从 SNMP 代理发送到 SNMP 管理器。

SNMP 陷阱有三种类型：标准陷阱，内置陷阱和用户定义的陷阱。ONTAP 不支持用户定义的陷阱。

可以使用陷阱定期检查 MIB 中定义的操作阈值或故障。如果达到阈值或检测到故障，SNMP 代理会向陷阱主机发送一条消息（陷阱），提醒其发生此事件。



ONTAP支持SNMPv1和SNMPv3陷阱。ONTAP 不支持 SNMPv2c 陷阱和通知。

标准 SNMP 陷阱

这些陷阱在 RFC 1215 中定义。ONTAP 支持五个标准 SNMP 陷阱：coldstart，warmStart，linkDown，linkUp 和 authenticationFailure。



默认情况下，authenticationFailure 陷阱处于禁用状态。必须使用 `system snmp authtrap` 命令启用陷阱。有关的详细信息 `system snmp authtrap`，请参见["ONTAP 命令参考"](#)。

内置 SNMP 陷阱

内置陷阱在 ONTAP 中预定义，如果发生事件，它们会自动发送到陷阱主机列表上的网络管理工作站。这些陷阱，例如 diskFailedShutdown，cpuTooBusy 和 volumeNearlyFull，均在自定义 MIB 中定义。

每个内置陷阱都由一个唯一的陷阱代码标识。

为ONTAP网络创建SNMP社区

使用 SNMPv1 和 SNMPv2c 时，您可以创建 SNMP 社区，作为管理工作站和 Storage Virtual Machine（SVM）之间的身份验证机制。

通过在数据SVM中创建SNMP社区、您可以执行等命令 `snmpwalk` 和 `snmpget` 在数据生命周期中。

关于此任务

- 在新安装的 ONTAP 中，SNMPv1 和 SNMPv2c 默认处于禁用状态。

创建 SNMP 社区后，SNMPv1 和 SNMPv2c 将处于启用状态。

- ONTAP 支持只读社区。
- 默认情况下、分配给数据"LIF"的"数据"防火墙策略会将SNMP服务设置为 deny。

您必须创建一个新的防火墙策略、并将SNMP服务设置为 allow 为数据SVM创建SNMP用户时。



从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 ["为 LIF 配置防火墙策略"](#)。

- 您可以为管理 SVM 和数据 SVM 的 SNMPv1 和 SNMPv2c 用户创建 SNMP 社区。
- 由于SVM不是SNMP标准的一部分、因此对数据NetApp的查询必须包括SVM根OID (1.3.6.1.4.1.789)、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

步骤

1. 使用创建SNMP社区 `system snmp community add` 命令：以下命令显示如何在管理 SVM cluster-1 中创建 SNMP 社区：

```
system snmp community add -type ro -community-name comty1 -vserver cluster-1
```

以下命令显示如何在数据 SVM vs1 中创建 SNMP 社区：

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. 使用 `system snmp community show` 命令验证是否已创建社区。

以下命令显示了为 SNMPv1 和 SNMPv2c 创建的两个社区：

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. 使用检查"data"防火墙策略中是否允许SNMP作为服务 `system services firewall policy show` 命令：

以下命令显示默认 "data" 防火墙策略中不允许使用 SNMP 服务（仅 "mgmt" 防火墙策略中允许使用 SNMP 服务）：

```
system services firewall policy show
Vserver Policy      Service      Allowed
-----
cluster-1
  data
    dns          0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps       0.0.0.0/0
cluster-1
  intercluster
    https       0.0.0.0/0
    ndmp        0.0.0.0/0
    ndmps       0.0.0.0/0
cluster-1
  mgmt
    dns          0.0.0.0/0
    http         0.0.0.0/0
    https       0.0.0.0/0
    ndmp        0.0.0.0/0
    ndmps       0.0.0.0/0
    ntp         0.0.0.0/0
    snmp        0.0.0.0/0
    ssh         0.0.0.0/0
```

4. 使用创建允许访问的新防火墙策略 snmp 服务 `system services firewall policy create` 命令:

以下命令将创建一个名为data1的新数据防火墙策略、此策略允许使用 snmp

```
system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0
```

```
cluster-1::> system services firewall policy show -service snmp
```

Vserver	Policy	Service	Allowed
cluster-1	mgmt	snmp	0.0.0.0/0
vs1	data1	snmp	0.0.0.0/0

5. 使用命令和-Firewall-policy参数将防火墙策略应用于数据LIF network interface modify。

以下命令会将新的 "data1" 防火墙策略分配给 LIF "datalif1" :

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

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

在ONTAP集群中配置SNMPv3用户

与 SNMPv1 和 SNMPv2c 相比, SNMPv3 是一种安全协议。要使用 SNMPv3 , 必须将 SNMPv3 用户配置为从 SNMP 管理器运行 SNMP 实用程序。

步骤

使用 `security login create` 命令创建 SNMPv3 用户。

系统将提示您提供以下信息:

- 引擎 ID : 默认值和建议值为本地引擎 ID
- 身份验证协议
- 身份验证密码
- 隐私协议
- 隐私协议密码

结果

SNMPv3 用户可以使用用户名和密码从 SNMP 管理器登录并运行 SNMP 实用程序命令。

SNMPv3 安全参数

SNMPv3 包括一项身份验证功能，如果选择此功能，则要求用户在调用命令时输入其名称，身份验证协议，身份验证密钥以及所需的安全级别。

下表列出了 SNMPv3 安全参数：

参数	命令行选项	Description
引擎 ID	-e 引擎 ID	SNMP 代理的引擎 ID。默认值为 local EngineID（建议）。
securityName	-u 名称	用户名不得超过 32 个字符。
authProtocol	-a { none	md5
SHA	SHA-256 }	身份验证类型可以为 none，MD5，SHA 或 SHA-256。
authkey	-A 密码短语	至少包含八个字符的密码短语。
安全性级别	-l { authNoPriv	AuthPriv
noAuthNoPriv }	安全级别可以是 "身份验证"，"无隐私"，"身份验证"，"隐私" 或 "无身份验证"，无隐私。	特权协议
-x { none	des	aes128 }
隐私协议可以是 none，DES 或 aes128	privPassword	-X 密码

不同安全级别的示例

此示例显示了使用不同安全级别创建的 SNMPv3 用户如何使用 SNMP 客户端命令、例如 `snmpwalk`，以查询群集对象。

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。



您必须使用 `snmpwalk 5.3.1` 或更高版本(如果身份验证协议为 SHA)。

安全级别：**AuthPriv**

以下输出显示了使用 `authPriv` 安全级别创建 SNMPv3 用户的过程。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS 模式

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk 测试

以下输出显示了运行 snmpwalk 命令的 SNMPv3 用户：

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全级别：AuthNoPriv

以下输出显示了使用 authNoPriv 安全级别创建 SNMPv3 用户的过程。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS 模式

FIPS不允许您为隐私协议选择*无*。因此、无法在FIPS模式下配置authNo特权SNMPv3用户。

snmpwalk 测试

以下输出显示了运行 snmpwalk 命令的 SNMPv3 用户：

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全级别： noAuthNoPriv

以下输出显示了创建具有 noAuthNoPriv 安全级别的 SNMPv3 用户的过程。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS 模式

FIPS不允许您为隐私协议选择*无*。

snmpwalk 测试

以下输出显示了运行 snmpwalk 命令的 SNMPv3 用户：

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

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

在ONTAP网络上为SNMP配置陷阱主机

您可以将陷阱主机（SNMP 管理器）配置为在集群中生成 SNMP 陷阱时接收通知（SNMP 陷阱 PDU）。您可以指定 SNMP 陷阱主机的主机名或 IP 地址（IPv4 或 IPv6）。

开始之前

- 必须在集群上启用 SNMP 和 SNMP 陷阱。



默认情况下，SNMP 和 SNMP 陷阱处于启用状态。

- 必须在集群上配置 DNS 以解析陷阱主机名称。
- 要使用 IPv6 地址配置 SNMP 陷阱主机，必须在集群上启用 IPv6。
- 创建陷阱主机时、您必须已指定预定义的基于用户的安全模型(User-based Security Model、USM)身份验证和隐私凭据。

步骤

添加 SNMP 陷阱主机：

```
system snmp traphost add
```



只有在至少将一个 SNMP 管理工作站指定为陷阱主机时，才能发送陷阱。

以下命令将使用已知的 USM 用户添加一个名为 `yyy.example.com` 的新 SNMPv3 陷阱主机：

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

以下命令将使用主机的 IPv6 地址添加陷阱主机：

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

验证ONTAP集群中的SNMP轮询

配置 SNMP 后，您应验证是否可以轮询集群。

关于此任务

要轮询集群、您需要使用第三方命令、例如 snmpwalk。

步骤

1. 发送 SNMP 命令以从其他集群轮询集群。

对于运行SNMPv1的系统、请使用命令行界面命令 `snmpwalk -v version -c community_string ip_address_or_host_name system` 发现MIB (管理信息库)的内容。

在此示例中，要轮询的集群管理 LIF 的 IP 地址为 10.11.12.123。命令将显示从 MIB 请求的信息：

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
                        Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

对于运行SNMPv2c的系统、请使用命令行界面命令 `snmpwalk -v version -c community_string ip_address_or_host_name system` 发现MIB (管理信息库)的内容。

在此示例中，要轮询的集群管理 LIF 的 IP 地址为 10.11.12.123。命令将显示从 MIB 请求的信息：

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
                        Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

对于运行SNMPv3的系统、请使用命令行界面命令 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv`

-u username -A passwordip_address_or_host_name system 发现MIB (管理信息库)的内容。

在此示例中，要轮询的集群管理 LIF 的 IP 地址为 10.11.12.123。命令将显示从 MIB 请求的信息：

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
-A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

用于管理SNMP、陷阱和陷阱主机的ONTAP命令

您可以使用 `system snmp` 用于管理SNMP、陷阱和陷阱主机的命令。您可以使用 `security` 用于管理每个SVM的SNMP用户的命令。您可以使用 `event` 用于管理与SNMP陷阱相关的事件的命令。

用于配置 SNMP 的命令

如果您要 ...	使用此命令 ...
在集群上启用 SNMP	<pre>options -option-name snmp.enable -option-value on</pre> <p>管理（mgmt）防火墙策略下必须允许 SNMP 服务。您可以使用 <code>system services firewall policy show</code> 命令验证是否允许使用 SNMP。</p>
在集群上禁用 SNMP	<pre>options -option-name snmp.enable -option-value off</pre>

用于管理 SNMP v1，v2c 和 v3 用户的命令

如果您要 ...	使用此命令 ...
配置 SNMP 用户	<pre>security login create</pre>

显示 SNMP 用户	<code>security snmpusers`和 `security login show -application snmp</code>
删除 SNMP 用户	<code>security login delete</code>
修改 SNMP 用户登录方法的访问控制角色名称	<code>security login modify</code>

用于提供联系人和位置信息的命令

如果您要 ...	使用此命令 ...
显示或修改集群的联系详细信息	<code>system snmp contact</code>
显示或修改集群的位置详细信息	<code>system snmp location</code>

用于管理 **SNMP** 社区的命令

如果您要 ...	使用此命令 ...
为 SVM 或集群中的所有 SVM 添加只读 (ro) 社区	<code>system snmp community add</code>
删除一个社区或所有社区	<code>system snmp community delete</code>
显示所有社区的列表	<code>system snmp community show</code>

由于SVM不是SNMP标准的一部分、因此对数据NetApp的查询必须包括SVM根OID (1.3.6.1.4.1.789)、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

用于显示 **SNMP** 选项值的命令

如果您要 ...	使用此命令 ...
显示所有 SNMP 选项的当前值, 包括集群联系人, 联系人位置, 集群是否配置为发送陷阱, 陷阱主机列表以及社区列表和访问控制类型	<code>system snmp show</code>

用于管理 **SNMP** 陷阱和陷阱主机的命令

如果您要 ...	使用此命令 ...
启用从集群发送的 SNMP 陷阱	<code>system snmp init -init 1</code>
禁用从集群发送的 SNMP 陷阱	<code>system snmp init -init 0</code>

添加一个陷阱主机，用于接收集群中特定事件的 SNMP 通知	<code>system snmp traphost add</code>
删除陷阱主机	<code>system snmp traphost delete</code>
显示陷阱主机的列表	<code>system snmp traphost show</code>

用于管理与 **SNMP** 陷阱相关的事件的命令

如果您要 ...	使用此命令 ...
显示为其生成 SNMP 陷阱（内置）的事件	<p><code>event route show</code></p> <p>使用 <code>-snmp-support true</code> 参数以仅查看与 SNMP 相关的事件。</p> <p>使用 <code>instance -messagename <message></code> 参数、以查看事件可能发生的原因的详细问题描述以及任何更正操作。</p> <p>不支持将单个 SNMP 陷阱事件路由到特定陷阱主机目标。所有 SNMP 陷阱事件都会发送到所有陷阱主机目标。</p>
显示 SNMP 陷阱历史记录列表，这些记录是已发送到 SNMP 陷阱的事件通知	<code>event snmhistory show</code>
删除 SNMP 陷阱历史记录	<code>event snmhistory delete</code>

相关信息

- ["系统SNMP"](#)
- ["安全snmpusers"](#)
- ["安全性"](#)
- ["事件"](#)
- ["安全登录"](#)

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。