



# 管理 **SNMP** (僅限叢集管理員) ONTAP 9

NetApp  
February 12, 2026

# 目錄

管理 SNMP (僅限叢集管理員)	1
瞭解 ONTAP 網路上的 SNMP	1
MIB 總覽	1
SNMP 設陷	1
標準 SNMP 設陷	2
內建 SNMP 設陷	2
為 ONTAP 網路建立 SNMP 社群	2
在 ONTAP 叢集中設定 SNMPv3 使用者	4
v3 安全參數	5
不同安全層級的範例	5
在 ONTAP 網路上設定用於 SNMP 的 traphosts	8
驗證 ONTAP 叢集中的 SNMP 輪詢	9
用於管理 SNMP, 設陷和 traphosts 的 ONTAP 命令	10
設定 SNMP 的命令	10
用於管理 SNMP v1、v2c 和 v3 使用者的命令	10
提供聯絡人和位置資訊的命令	11
管理 SNMP 社群的命令	11
用於顯示 SNMP 選項值的命令	11
用於管理 SNMP 陷阱和 traphosts 的命令	11
用於管理與 SNMP 陷阱相關的事件的命令	12

# 管理 SNMP（僅限叢集管理員）

## 瞭解 ONTAP 網路上的 SNMP

您可以設定SNMP來監控叢集中的SVM、以避免發生問題、並在問題確實發生時予以回應。管理SNMP包括設定SNMP使用者、以及為所有SNMP事件設定SNMP traphost目的地（管理工作站）。依預設、SNMP會在資料生命量上停用。

您可以在資料SVM中建立及管理唯讀SNMP使用者。資料生命期必須設定為在SVM上接收SNMP要求。

SNMP網路管理工作站（或管理程式）可以查詢SVM SNMP代理程式以取得資訊。SNMP代理程式會收集資訊並將其轉送給SNMP管理程式。SNMP代理程式也會在發生特定事件時產生設陷通知。SVM上的SNMP代理程式具有唯讀權限、無法用於任何設定作業或採取修正行動來回應陷阱。提供與SNMP v1、v2c和v3版本相容的SNMP代理程式。ONTAP使用密碼和加密技術、可提供進階的安全性。

如需ONTAP 更多有關支援SNMP的資訊、請參閱 ["TR-4220：Data ONTAP 支援SNMP"](#)。

### MIB 總覽

mib（管理資訊庫）是描述SNMP物件和設陷的文字檔。

MIBs說明儲存系統管理資料的結構、並使用包含物件識別碼（OID）的階層式命名空間。每個oid都會識別可透過SNMP讀取的變數。

由於MIBs不是組態檔、ONTAP 而且無法讀取這些檔案、因此SNMP功能不受MIBs影響。提供下列的mib檔案：  
：ONTAP

- NetApp 自訂 MIB (netapp.mib)

支援IPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）和ICMP（RFC 2466）MIBs（同時顯示IPv6和IPv6資料） ONTAP。

ONTAP 也會在中的物件識別碼（OID）和物件簡短名稱之間提供簡短的交互參照 traps.dat 檔案：



NetApp 支援網站上提供最新版本的 ONTAP MIB 和「traps.dat」檔案。不過、支援網站上的這些檔案版本不一定對應ONTAP 於您的版本的SNMP功能。這些檔案可協助您評估最新ONTAP 版的SNMP功能。

### SNMP設陷

SNMP設陷會擷取系統監控資訊、這些資訊會以非同步通知的形式從SNMP代理程式傳送至SNMP管理程式。

SNMP設陷有三種類型：標準、內建及使用者定義。不支援ONTAP 使用者定義的陷阱。

陷阱可用於定期檢查在MIB中定義的操作臨界值或故障。如果達到臨界值或偵測到故障、SNMP代理程式會傳送訊息（設陷）給警示事件的traphosts。



ONTAP 支援 SNMPv1 和 SNMPv3 設陷。不支援SNMP v2c擷取和通知。ONTAP

## 標準SNMP設陷

這些陷阱定義於RFC 1215。支援的五種標準SNMP設陷ONTAP：冷啟動、暖啟動、連結、LinkUp和驗證失敗。



驗證失敗設陷預設為停用。您必須使用 `system snmp authtrap` 命令來啟用陷阱。如"[指令參考資料ONTAP](#)"需詳細 `system snmp authtrap` 資訊，請參閱。

## 內建SNMP設陷

內建的設陷會預先定義在ONTAP 支援中、並在發生事件時自動傳送至traphost清單上的網路管理站台。這些陷阱（例如diskFailedShutdown, cpuTooBusy和volumeNearlyFull）是在自訂的mib中定義的。

每個內建陷阱都會以獨特的陷阱代碼來識別。

## 為 ONTAP 網路建立 SNMP 社群

使用SNMP v1和SNMP v2c時、您可以建立SNMP社群、做為管理站與儲存虛擬機器（SVM）之間的驗證機制。

透過在資料 SVM 中建立 SNMP 社群、您可以執行命令、例如 `snmpwalk` 和 `snmpget` 資料生命。

關於這項工作

- 在全新安裝ONTAP 的功能中、預設會停用SNMPv1和SNMPv2c。

在建立SNMP社群之後、會啟用SNMP v1和SNMP v2c。

- 支援唯讀社群。ONTAP
- 依預設、指派給資料生命期的「資料」防火牆原則會將 SNMP 服務設為 `deny`。

您必須建立新的防火牆原則、並將 SNMP 服務設為 `allow` 為資料 SVM 建立 SNMP 使用者時。



從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "[設定lifs的防火牆原則](#)"。

- 您可以為管理SVM和資料SVM的SNMP v1和SNMP v2c使用者建立SNMP社群。
- 由於 SVM 不是 SNMP 標準的一部分、因此資料生命體的查詢必須包含 NetApp 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`。

步驟

- 使用建立 SNMP 社群 `system snmp community add` 命令。下列命令顯示如何在管理SVM叢集1中建立SNMP社群：

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

下列命令顯示如何在資料SVM VS1中建立SNMP社群：

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

2. 使用系統SNMP community show命令來驗證是否已建立社群。

下列命令顯示為SNMP v1和SNMP v2c所建立的兩個社群：

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

3. 使用檢查是否允許 SNMP 作為「資料」防火牆原則中的服務 system services firewall policy show 命令。

下列命令顯示預設的「資料」防火牆原則不允許SNMP服務（僅「管理」防火牆原則允許SNMP服務）：

```
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. 建立允許使用存取的新防火牆原則 snmp 使用進行服務 system services firewall policy create

命令。

下列命令會建立一個新的資料防火牆原則「data1」、允許使用 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. 使用命令搭配 `-firewall-policy` 參數，將防火牆原則套用至資料 LIF network interface modify。

下列命令會將新的「data1」防火牆原則指派給LIF「dataif1」：

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

如"[指令參考資料ONTAP](#)"需詳細 `network interface modify` 資訊，請參閱。

## 在 ONTAP 叢集中設定 SNMPv3 使用者

相較於SNMPv1和SNMPv2c、v3是一種安全的傳輸協定。若要使用v3、您必須設定一個v3使用者、以便從SNMP管理程式執行SNMP公用程式。

步驟

使用 `security login create` 指令建立 SNMPv3 使用者。

系統會提示您提供下列資訊：

- 引擎ID：預設值和建議值為本機引擎ID
- 驗證傳輸協定
- 驗證密碼
- 隱私權傳輸協定
- 隱私權傳輸協定密碼

結果

v3使用者可以使用使用者名稱和密碼、從SNMP管理程式登入、然後執行SNMP公用程式命令。

## v3安全參數

v3包含驗證功能、選取時會要求使用者在叫用命令時輸入名稱、驗證傳輸協定、驗證金鑰及其所需的安全層級。

下表列出了v3安全參數：

參數	命令列選項	說明
工程師ID	-e引擎ID	SNMP代理程式的引擎ID。預設值為本機引擎ID（建議使用）。
安全性名稱	-u名稱	使用者名稱不得超過32個字元。
驗證傳輸協定	-A {NONE	md5
SHA	SHA-256}	驗證類型可以是「無」、「MD5」、「SHA」或「SHA-256」。
驗證金鑰	-A通關密碼	至少八個字元的通關密碼。
安全性層級	l {authNoPrimv	authPrimv
noauthNoPrimiv}	安全層級可以是驗證、無隱私權、驗證、隱私權或無驗證、無隱私。	私有傳輸協定
-x {nONE	DE	AES128}
隱私權傳輸協定可以是無、DE或AES128	私有密碼	-X密碼

## 不同安全層級的範例

此範例顯示以不同安全性層級建立的 SNMPv3 使用者如何使用 SNMP 用戶端端指令、例如 `snmpwalk`，查詢叢集物件。

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。



您必須使用 `snmpwalk 5.3.1` 或更新版本、當驗證傳輸協定為 SHA 時。

### 安全性層級：**authPrim**

下列輸出顯示使用驗證權限安全性層級建立的v3使用者。

```
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.測試

下列輸出顯示執行snmpwalk命令的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ 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"
```

### 安全性層級：authNoPrim

下列輸出顯示使用驗證NoPrimiv安全性層級建立的v3使用者。

```
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 不允許您為隱私權傳輸協定選擇 \* 無 \* 。因此、無法在 FIPS 模式中設定驗證 NoPrimv SNMPv3 使用者。

### snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ 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"
```

### 安全性層級：noAuthNoPrimiv

下列輸出顯示使用noAuthNoPrimiv安全性層級建立的v3使用者。

```
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 不允許您為隱私權傳輸協定選擇 \* 無 \* 。

### snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ 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"
```

如"[指令參考資料ONTAP](#)"需詳細 `security login create` 資訊，請參閱。

## 在 ONTAP 網路上設定用於 SNMP 的 traphosts

您可以將traphost（SNMP管理程式）設定為在叢集中產生SNMP設陷時接收通知（SNMP設陷PDU）。您可以指定SNMP traphost的主機名稱或IP位址（IPv4或IPv6）。

開始之前

- 必須在叢集上啟用SNMP和SNMP設陷。



SNMP和SNMP設陷預設為啟用。

- 必須在叢集上設定DNS、才能解析traphost名稱。
- 叢集上必須啟用IPv6、才能使用IPv6位址來設定SNMP traphosts。
- 建立 traphosts 時，您必須指定預先定義的使用者型安全模式（USM）驗證和隱私權認證。

步驟

新增SNMP traphost：

```
system snmp traphost add
```



只有當至少有一個SNMP管理站台指定為traphost時、才能傳送陷阱。

下列命令會以已知的USM使用者新增名為yyy.example.com的v3 traphost：

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

下列命令會使用主機IPv6位址來新增traphost：

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

# 驗證 ONTAP 叢集中的 SNMP 輪詢

設定SNMP之後、您應該確認可以輪詢叢集。

關於這項工作

若要輪詢叢集、您需要使用第三方命令、例如 `snmpwalk`。

步驟

1. 傳送SNMP命令、從不同的叢集輪詢叢集。

對於執行 SNMPv1 的系統、請使用 CLI 命令 `snmpwalk -v version -c community_string ip_address_or_host_name system` 探索 MIB (管理資訊庫) 的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
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
```

對於執行 SNMPv2c 的系統、請使用 CLI 命令 `snmpwalk -v version -c community_string ip_address_or_host_name system` 探索 MIB (管理資訊庫) 的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
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
```

對於執行 SNMPv3 的系統、請使用 CLI 命令 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u`

username -A passwordip\_address\_or\_host\_name system 探索 MIB (管理資訊庫) 的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
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
```

## 用於管理 **SNMP**，設陷和 **traphosts** 的 **ONTAP** 命令

您可以使用 `system snmp` 用於管理 **SNMP**、設陷和 **traphosts** 的命令。您可以使用 `security` 用於管理每個 **SVM** 的 **SNMP** 使用者的命令。您可以使用 `event` 管理與 **SNMP** 設陷相關事件的命令。

### 設定**SNMP**的命令

如果您想要...	使用此命令...
在叢集上啟用 <b>SNMP</b>	<pre>options -option-name snmp.enable -option-value on</pre> <p><b>SNMP</b>服務必須符合管理 (管理) 防火牆原則。您可以使用系統服務防火牆原則<code>show</code>命令來驗證是否允許<b>SNMP</b>。</p>
停用叢集上的 <b>SNMP</b>	<pre>options -option-name snmp.enable -option-value off</pre>

### 用於管理**SNMP v1**、**v2c**和**v3**使用者的命令

如果您想要...	使用此命令...
設定 <b>SNMP</b> 使用者	<pre>security login create</pre>

顯示SNMP使用者	<code>security snmpusers`和 `security login show -application snmp</code>
刪除SNMP使用者	<code>security login delete</code>
修改SNMP使用者登入方法的存取控制角色名稱	<code>security login modify</code>

## 提供聯絡人和位置資訊的命令

如果您想要...	使用此命令...
顯示或修改叢集的聯絡詳細資料	<code>system snmp contact</code>
顯示或修改叢集的位置詳細資料	<code>system snmp location</code>

## 管理SNMP社群的命令

如果您想要...	使用此命令...
為SVM或叢集中的所有SVM新增唯讀（RO）社群	<code>system snmp community add</code>
刪除社群或所有社群	<code>system snmp community delete</code>
顯示所有社群的清單	<code>system snmp community show</code>

由於 SVM 不是 SNMP 標準的一部分、因此資料生命體的查詢必須包含 NetApp 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`。

## 用於顯示SNMP選項值的命令

如果您想要...	使用此命令...
顯示所有SNMP選項的目前值、包括叢集聯絡人、聯絡人位置、叢集是否設定為傳送陷阱、traphosts清單、以及社群和存取控制類型清單	<code>system snmp show</code>

## 用於管理SNMP陷阱和traphosts的命令

如果您想要...	使用此命令...
啟用從叢集傳送的SNMP設陷	<code>system snmp init -init 1</code>
停用從叢集傳送的SNMP設陷	<code>system snmp init -init 0</code>

新增接收叢集中特定事件SNMP通知的traphost	<code>system snmp traphost add</code>
刪除traphost	<code>system snmp traphost delete</code>
顯示traphosts清單	<code>system snmp traphost show</code>

## 用於管理與SNMP陷阱相關的事件的命令

如果您想要...	使用此命令...
顯示產生SNMP陷阱（內建）的事件	<p><code>event route show</code></p> <p>使用 <code>-snmp-support true</code> 僅檢視 SNMP 相關事件的參數。</p> <p>使用 <code>instance -messagename &lt;message&gt;</code> 此參數可檢視事件發生原因的詳細說明、以及任何修正動作。</p> <p>不支援將個別SNMP設陷事件路由傳送至特定的traphost目的地。所有SNMP設陷事件都會傳送至所有的traphost目的地。</p>
顯示SNMP設陷記錄清單、這是已傳送至SNMP設陷的事件通知	<code>event snmhistory show</code>
刪除SNMP設陷歷程記錄	<code>event snmhistory delete</code>

### 相關資訊

- ["系統 SNMP"](#)
- ["安全性"](#)
- ["安全性"](#)
- ["活動"](#)
- ["安全登入"](#)

## 版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。