



## **EMS 組態**

### **ONTAP 9**

NetApp  
April 24, 2024

# 目錄

EMS 組態 .....	1
EMS 組態概觀 .....	1
使用System Manager設定EMS事件通知和篩選器 .....	1
使用CLI設定EMS事件通知 .....	4
更新過時的EMS事件對應 .....	10

# EMS 組態

## EMS 組態概觀

您可以設定ONTAP 支援功能支援功能、將重要的EMS（事件管理系統）事件通知直接傳送至電子郵件地址、syslog伺服器、簡易管理網路傳輸協定（SNMP）traphost或Webhook應用程式、以便立即通知您需要立即注意的系統問題。

由於重要事件通知預設不會啟用、因此您需要設定EMS、將通知傳送至電子郵件地址、syslog伺服器、SNMP traphost或Webhook應用程式。

檢閱的特定版本 "[《EMS參考資料》（英文ONTAP）](#)"。

如果您的EMS事件對應使用過時ONTAP 的支援功能（例如事件目的地、事件路由）、建議您更新對應。"[瞭解如何從已過時ONTAP 的等字指令更新EMS對應](#)"。

## 使用System Manager設定EMS事件通知和篩選器

您可以使用System Manager來設定事件管理系統（EMS）傳送事件通知的方式、以便在系統問題需要您立即注意時通知您。

版本ONTAP	有了System Manager、您可以...
更新版本ONTAP	將事件傳送至遠端syslog伺服器時、請指定傳輸層安全性（TLS）傳輸協定。
更新版本ONTAP	設定電子郵件地址、syslog伺服器、Webhook應用程式、以及SNMP traphosts。
零點9.7至9.10.0 ONTAP	僅設定SNMP traphosts。您可以使用ONTAP CLI設定其他EMS目的地。請參閱 " <a href="#">EMS 組態概觀</a> "。

您可以執行下列程序：

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)
- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)

相關資訊



- "[《環管系統參考資料》 ONTAP](#)"
- "[使用CLI設定SNMP traphosts以接收事件通知](#)"

## 新增EMS事件通知目的地

您可以使用System Manager來指定要將EMS訊息傳送到何處。

從S廳9.12.1開始ONTAP、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。如需詳細資訊、請參閱 `event notification destination create` 手冊頁。

### 步驟

1. 按一下\*叢集>設定\*。
2. 在\*通知管理\*區段中、按一下 ，然後單擊\*查看事件目的地\*。
3. 在\*通知管理\*頁面上、選取\*事件目的地\*索引標籤。
4. 按一下  `Add`。
5. 指定名稱、EMS目的地類型及篩選條件。



如有需要、您可以新增篩選條件。按一下「新增事件篩選器」。



6. 視您選取的EMS目的地類型而定、請指定下列項目：

若要設定...	指定或選取...
SNMP traphost	<ul style="list-style-type: none"><li>• TrapHost名稱</li></ul>
電子郵件  (從9.10.1開始)	<ul style="list-style-type: none"><li>• 目的地電子郵件地址</li><li>• 郵件伺服器</li><li>• 寄件者電子郵件地址</li></ul>
系統記錄伺服器  (從9.10.1開始)	<ul style="list-style-type: none"><li>• 伺服器的主機名稱或IP位址</li><li>• 系統記錄連接埠（從9.12.1開始）</li><li>• 系統記錄傳輸（從9.12.1開始）</li></ul> <p>選取「* TCP Encrypted （TCP加密*）」可啟用傳輸層安全性（TLS）傳輸協定。如果未輸入* Syslog連接埠*的值、則會根據* Syslog transport*選項使用預設值。</p>
Webhook  (從9.10.1開始)	<ul style="list-style-type: none"><li>• Webhook URL</li><li>• 用戶端驗證（選取此選項以指定用戶端憑證）</li></ul>

## 建立新的EMS事件通知篩選器

從ONTAP 《E59.10.1》開始、您可以使用System Manager定義新的自訂篩選條件、以指定處理EMS通知的規則。

### 步驟



1. 按一下\*叢集>設定\*。
2. 在\*通知管理\*區段中、按一下 ，然後單擊 \* 查看事件目的地 \*。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 按一下  Add。
5. 指定名稱、然後選取是要從現有事件篩選器複製規則、還是要新增規則。
6. 視您的選擇而定、請執行下列步驟：

如果您選擇.....	然後執行下列步驟...
從現有事件篩選器複製規則	<ol style="list-style-type: none"> <li>1. 選取現有的事件篩選器。</li> <li>2. 修改現有規則。</li> <li>3. 如有需要、請按一下以新增其他規則  Add。</li> </ol>
新增規則	指定每個新規則的類型、名稱模式、嚴重性及SNMP設陷類型。

## 編輯EMS事件通知目的地

從ONTAP 版本支援的版本起、您可以使用System Manager來變更事件通知目的地資訊。

### 步驟

1. 按一下\*叢集>設定\*。
2. 在\*通知管理\*區段中、按一下 ，然後單擊\*查看事件目的地\*。
3. 在\*通知管理\*頁面上、選取\*事件目的地\*索引標籤。
4. 在事件目的地名稱旁、按一下 ，然後單擊\*編輯\*。
5. 修改事件目的地資訊、然後按一下「儲存」。



## 編輯EMS事件通知篩選器

從ONTAP 功能更新至功能更新至功能更新、您可以使用System Manager修改自訂的篩選條件、以變更事件通知的處理方式。



您無法修改系統定義的篩選條件。

### 步驟

1. 按一下\*叢集>設定\*。
2. 在\*通知管理\*區段中、按一下 ，然後單擊 \* 查看事件目的地 \*。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 在事件篩選器名稱旁、按一下 ，然後單擊\*編輯\*。
5. 修改事件篩選器資訊、然後按一下「儲存」。



## 刪除EMS事件通知目的地

從ONTAP 《支援範本》（《支援範本》）9.10.1開始、您可以使用System Manager刪除EMS事件通知目的地。



您無法刪除SNMP目的地。

### 步驟

1. 按一下\*叢集>設定\*。
2. 在\*通知管理\*區段中、按一下 ，然後單擊 \* 查看事件目的地 \*。
3. 在\*通知管理\*頁面上、選取\*事件目的地\*索引標籤。
4. 在事件目的地名稱旁、按一下 ，然後單擊 \* 刪除 \*。



## 刪除EMS事件通知篩選器

從《軟件及應用程式》（2019）9.10.1開始ONTAP、您可以使用System Manager刪除自訂的篩選條件。



您無法刪除系統定義的篩選條件。

### 步驟

1. 按一下\*叢集>設定\*。
2. 在\*通知管理\*區段中、按一下 ，然後單擊 \* 查看事件目的地 \*。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 在事件篩選器名稱旁、按一下 ，然後單擊\*刪除\*。

## 使用CLI設定EMS事件通知

### EMS 組態工作流程

您必須將重要的EMS事件通知設定為以電子郵件傳送、轉送至syslog伺服器、轉送至SNMP traphost、或轉送至Webhook應用程式。這有助於您及時採取修正行動、避免系統中斷。

#### 關於這項工作

如果您的環境已包含syslog伺服器、可用來彙總來自其他系統（例如同步器和應用程式）的記錄事件、那麼使用syslog伺服器也能更輕鬆地從儲存系統發出重要的事件通知。

如果您的環境尚未包含syslog伺服器、則使用電子郵件進行重要事件通知會更容易。

如果您已將事件通知轉送到SNMP traphost、則可能需要監控該traphost是否有重要事件。



#### 選擇

- 設定EMS以傳送事件通知。

如果您需要...	請參閱此...
將重要事件通知傳送至電子郵件地址的EMS	<a href="#">設定重要的EMS事件以傳送電子郵件通知</a>
EMS可將重要事件通知轉送至syslog伺服器	<a href="#">設定重要的EMS事件、將通知轉送到syslog伺服器</a>
如果您想要EMS將事件通知轉送到SNMP traphost	<a href="#">設定SNMP traphosts以接收事件通知</a>
如果您想要EMS將事件通知轉送到Webhook應用程式	<a href="#">設定重要的EMS事件、將通知轉送到Webhook應用程式</a>

### 設定重要的**EMS**事件以傳送電子郵件通知

若要接收最重要事件的電子郵件通知、您必須將EMS設定為針對重要活動的事件傳送電子郵件訊息。

您需要的產品

必須在叢集上設定DNS、才能解析電子郵件地址。

關於這項工作

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 設定事件的SMTP郵件伺服器設定：

```
event config modify -mail-server mailhost.your_domain -mail-from  
cluster_admin@your_domain
```

2. 建立事件通知的電子郵件目的地：

```
event notification destination create -name storage-admins -email  
your_email@your_domain
```

3. 設定重要事件以傳送電子郵件通知：

```
event notification create -filter-name important-events -destinations storage-  
admins
```

## 設定重要的EMS事件、將通知轉送到syslog伺服器

若要在syslog伺服器上記錄最嚴重事件的通知、您必須將EMS設定為轉送重要活動訊號的事件通知。

您需要的產品

必須在叢集上設定DNS、才能解析syslog伺服器名稱。

關於這項工作

如果您的環境尚未包含用於事件通知的syslog伺服器、您必須先建立一個。如果您的環境中已包含用於記錄其他系統事件的syslog伺服器、您可能會想要使用該伺服器來處理重要的事件通知。

您可以在ONTAP 叢集執行時、在CLI輸入命令來執行此工作。

從S廳9.12.1開始ONTAP、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。有兩個新參數可供使用：

### **tcp-encrypted**

何時 tcp-encrypted 為指定 syslog-transport、ONTAP 驗證目的地主機的憑證來驗證其身分。預設值為 udp-unencrypted。

### **syslog-port**

預設值 syslog-port 參數取決於的設定 syslog-transport 參數。如果 syslog-transport 設為 tcp-encrypted、syslog-port 預設值為6514。

如需詳細資訊、請參閱 event notification destination create 手冊頁。

步驟

1. 建立重要事件的syslog伺服器目的地：



```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

從ONTAP 功能變數9.12.1開始、可以指定下列值 `syslog-transport`：

- `udp-unencrypted` 無安全性的使用者資料包傳輸協定
- `tcp-unencrypted` 無安全性的傳輸控制傳輸協定
- `tcp-encrypted` -傳輸層安全性 (TLS) 的傳輸控制傳輸協定

預設傳輸協定為 `udp-unencrypted`。

## 2. 設定重要事件以將通知轉送到syslog伺服器：

```
event notification create -filter-name important-events -destinations syslog-ems
```

## 設定SNMP traphosts以接收事件通知

若要在SNMP traphost上接收事件通知、您必須設定traphost。

您需要的產品

- 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。

關於這項工作

如果您尚未設定SNMP traphost來接收事件通知（SNMP設陷）、則必須新增一個。

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 如果您的環境尚未設定SNMP traphost來接收事件通知、請新增一個：

```
system snmp traphost add -peer-address snmp_traphost_name
```

SNMP預設支援的所有事件通知都會轉送到SNMP traphost。

## 設定重要的EMS事件、將通知轉送到Webhook應用程式

您可以設定ONTAP 將重要事件通知轉送至Webhook應用程式。所需的組態步驟取決於您選擇的安全性層級。

準備設定EMS事件轉送

在設定ONTAP 將事件通知轉送到Webhook應用程式之前、您應該考慮幾個概念和要求。

## Webhook應用程式

您需要能夠接收ONTAP 不必要事件通知的Webhook應用程式。Webhook是使用者定義的回撥例行工作、可延伸執行遠端應用程式或伺服器的功能。Webhooks是由用戶端呼叫或啟動（本例ONTAP 為示例）、方法是將HTTP要求傳送至目的地URL。具體而言ONTAP、將HTTP POST要求傳送至裝載Webhook應用程式的伺服器、以及以XML格式設定的事件通知詳細資料。

### 安全選項

視傳輸層安全性（TLS）傳輸協定的使用方式而定、有多種安全選項可供選擇。您選擇的選項會決定所需ONTAP 的功能組態。



TLS是一種在網際網路上廣泛使用的密碼編譯傳輸協定。它使用一或多個公開金鑰憑證來提供隱私、資料完整性和驗證。這些憑證由信任的憑證授權單位核發。

## HTTP

您可以使用HTTP來傳輸事件通知。使用此組態時、連線不安全。不驗證不驗證ONTAP 客戶端和Webhook應用程式的身分。此外、網路流量並未加密或受到保護。請參閱 ["設定Webhook目的地以使用HTTP"](#) 以取得組態詳細資料。

## HTTPS

為了提高安全性、您可以在裝載Webhook例行工作的伺服器上安裝憑證。驗證Webhook應用程式伺服器及雙方身分的HTTPS傳輸協定、ONTAP 以確保網路流量的隱私性和完整性。請參閱 ["設定 Webhook 目的地以使用 HTTPS"](#) 以取得組態詳細資料。

### HTTPS搭配相互驗證

您可以在ONTAP 發出Webhook要求的系統上安裝用戶端憑證、進一步強化HTTPS安全性。除了驗證Webhook應用程式伺服器的身分、並保護網路流量之外、Webhook應用程式還會驗證該客戶端的身分。ONTAP 這種雙向對等驗證稱為「相互TLS」。請參閱 ["設定Webhook目的地使用HTTPS進行相互驗證"](#) 以取得組態詳細資料。

### 相關資訊

- ["傳輸層安全性（TLS）傳輸協定1.3版"](#)

## 設定Webhook目的地以使用HTTP

您可以設定ONTAP 使用HTTP將事件通知轉送至Webhook應用程式。這是最不安全的選項、但設定起來最簡單。

### 步驟

1. 建立新目的地 `restapi-ems` 若要接收事件：

```
event notification destination create -name restapi-ems -rest-api-url  
http://<webhook-application>
```

在上述命令中、您必須使用\* HTTP配置作為目的地。

2. 建立連結的通知 `important-events` 使用篩選 `restapi-ems` 目的地：

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

## 設定 Webhook 目的地以使用 HTTPS

您可以設定 ONTAP、使用 HTTPS 將事件通知轉寄至 Webhook 應用程式。使用伺服器憑證來確認 Webhook 應用程式的身分識別、以及保護網路流量。ONTAP

### 開始之前

- 為 Webhook 應用程式伺服器產生私密金鑰和憑證
- 讓 root 憑證可安裝在 ONTAP 整個過程中

### 步驟

1. 在裝載 Webhook 應用程式的伺服器上安裝適當的伺服器私密金鑰和憑證。具體的組態步驟取決於伺服器。
2. 將伺服器根憑證安裝在 ONTAP

```
security certificate install -type server-ca
```

命令會要求提供憑證。

3. 建立 restapi-ems 接收事件的目的地：

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application>
```

在上述命令中、您必須使用 \* HTTPS \* 配置作為目的地。

4. 建立連結的通知 important-events 使用新的篩選器 restapi-ems 目的地：

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

## 設定 Webhook 目的地使用 HTTPS 進行相互驗證

您可以設定 ONTAP 將事件通知轉送至 Webhook 應用程式、使用 HTTPS 搭配相互驗證。使用此組態有兩個憑證。使用伺服器憑證來確認 Webhook 應用程式的身分、並保護網路流量。ONTAP 此外、裝載 Webhook 的應用程式會使用用戶端憑證來確認 ONTAP 該客戶端的身分。

### 開始之前

您必須先執行下列步驟、才能設定 ONTAP 使用功能：

- 為 Webhook 應用程式伺服器產生私密金鑰和憑證
- 讓 root 憑證可安裝在 ONTAP 整個過程中
- 為 ONTAP 該驗證用戶端產生私密金鑰和憑證

### 步驟

1. 執行工作的前兩個步驟 "設定 Webhook 目的地以使用 HTTPS" 安裝伺服器憑證、ONTAP 以便驗證伺服器的身分。
2. 在 Webhook 應用程式中安裝適當的根和中繼憑證、以驗證用戶端憑證。
3. 將用戶端憑證安裝 ONTAP 在下列項目中：

```
security certificate install -type client
```

命令會要求提供私密金鑰和憑證。

4. 建立 restapi-ems 接收事件的目的地：

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application> -certificate-authority <issuer of the client  
certificate> -certificate-serial <serial of the client certificate>
```

在上述命令中、您必須使用\* HTTPS \*配置作為目的地。

5. 建立連結的通知 important-events 使用新的篩選器 restapi-ems 目的地：

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

## 更新過時的EMS事件對應

### EMS事件對應模型

在版本不含故障碼的9.0之前ONTAP、EMS事件只能根據事件名稱模式的相符結果對應至事件目的地。ONTAP 命令集 (event destination、event route) 使用此模型的ONTAP 最新版本仍然可用，但從 ONTAP 9.0 開始已被淘汰。

從 ONTAP 9.0 開始、ONTAP EMS 事件目的地對應的最佳實務做法是使用更具擴充性的事件篩選器模型、在多個欄位上使用進行模式比對 event filter、event notification`和 `event notification destination 命令集。

如果您的 EMS 對應是使用過時的命令進行設定、您應該更新對應以使用 event filter、event notification`和 `event notification destination 命令集。

事件目的地有兩種類型：

1. 系統產生的目的地：有五個系統產生的事件目的地（預設為建立）

- allevents
- asup
- criticals
- pager
- traphost

某些系統產生的目的地是為了特殊目的而設計。例如、asup目的地會將CallHome.\*事件路由到AutoSupport 位在畫面上的這個動作模組ONTAP、以產生AutoSupport 各種訊息。

2. \* 使用者建立的目的地 \*：這些目的地是使用手動建立的 event destination create 命令。

```
cluster-1::event*> destination show
```

Name	Mail Dest.	SNMP Dest.	Syslog Dest.
Params			

-----	-----	-----	-----
-----			
allevents	-	-	-
false			
asup	-	-	-
false			
criticals	-	-	-
false			
pager	-	-	-
false			
traphost	-	-	-
false			

5 entries were displayed.

+

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

This command is deprecated. Use the "event filter", "event notification destination" and "event notification" commands, instead.

+

```
cluster-1::event*> destination show
```

+

Name	Mail Dest.	SNMP Dest.	Syslog Dest.
Params			

-----	-----	-----	-----
-----			
allevents	-	-	-
false			
asup	-	-	-
false			
criticals	-	-	-
false			
pager	-	-	-
false			
test	test@xyz.com	-	-
false			
traphost	-	-	-
false			

6 entries were displayed.

在過時的模型中、EMS 事件會使用個別對應至目的地 `event route add-destinations` 命令。

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.
```

```
cluster-1::event*> route show -message-name raid.aggr.*
```

Time	Message	Severity	Destinations	Freq	Threshd
-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----
	raid.aggr.autoGrow.abort	NOTICE	test	0	0
	raid.aggr.autoGrow.success	NOTICE	test	0	0
	raid.aggr.lock.conflict	INFORMATIONAL	test	0	0
	raid.aggr.log.CP.count	DEBUG	test	0	0
	4 entries were displayed.				

全新且可擴充的EMS事件通知機制、是以事件篩選器和事件通知目的地為基礎。如需新事件通知機制的詳細資訊、請參閱下列知識庫文章：

- ["事件管理系統概述ONTAP（適用於）9."](#)

Legacy routing based model



Event notification based model



## 更新EMS事件對應、以取代過時ONTAP 的EISO命令

如果您的 EMS 事件對應目前是使用過時的 ONTAP 命令集進行設定 (event destination、event route)、您應該遵循此程序來更新對應以使用 event filter、event notification 和 event notification destination 命令集。

### 步驟

1. 使用列出系統中的所有事件目的地 event destination show 命令。

```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents      -                -                -
false
asup           -                -                -
false
criticals      -                -                -
false
pager          -                -                -
false
test           test@xyz.com     -                -
false
traphost       -                -                -
false
6 entries were displayed.
```

2. 針對每個目的地、使用列出對應至目的地的事件 `event route show -destinations <destination name>` 命令。

```
cluster-1::event*> route show -destinations test
```

```
Time
Message          Severity      Destinations  Freq
Threshd
-----
-----
raid.aggr.autoGrow.abort      NOTICE      test          0          0
raid.aggr.autoGrow.success    NOTICE      test          0          0
raid.aggr.lock.conflict       INFORMATIONAL test          0          0
raid.aggr.log.CP.count        DEBUG        test          0          0
4 entries were displayed.
```

3. 建立對應的 `event filter` 其中包括所有這些事件子集。例如、如果您只想要包含 `raid.aggr.*` 事件、請使用萬用字元 `message-name` 建立篩選器時的參數。您也可以為單一事件建立篩選器。



您最多可以建立50個事件篩選器。



```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule      Rule      Message Name      SNMP Trap Type
Severity
      Position Type
-----
test_events
      1      include  raid.aggr.*      *      *
      2      exclude  *      *      *
2 entries were displayed.
```

4. 建立 event notification destination 針對每個 event destination 端點 (例如 SMTP/SNMP/Syslog )

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name      Type      Destination
-----
dest1      email      test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost  snmp      - (from "system snmp traphost")
2 entries were displayed.
```

5. 將事件篩選器對應至事件通知目的地、以建立事件通知。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID  Filter Name      Destinations
---
1   default-trap-events  snmp-traphost
2   asup_events         dest1
2 entries were displayed.
```

6. 針對每個項目重複步驟 1-5 event destination 那有 event route 對應：



路由至 SNMP 目的地的事件應對應至 snmp-traphost 事件通知目的地。SNMP traphost 目的地使用系統設定的 SNMP traphost。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
      scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>      Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

      Destination Name: snmp-traphost
      Type of Destination: snmp
      Destination: 10.234.166.135 (from "system snmp
traphost")
      Server CA Certificates Present?: -
      Client Certificate Issuing CA: -
      Client Certificate Serial Number: -
      Client Certificate Valid?: -
```

## 版權資訊

Copyright © 2024 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。