



# 支援服務文件**SnapCenter**

## SnapCenter Service

NetApp  
May 18, 2022

# 目錄

支援服務文件SnapCenter .....	1
更新功能SnapCenter .....	2
2021年12月21日 .....	2
2021年10月13日 .....	2
開始使用 .....	3
深入瞭SnapCenter 解支援服務 .....	3
開始使用 .....	5
建立連接器及啟用SnapCenter 「支援服務」的先決條件 .....	5
在Azure中建立連接器SnapCenter 以利服務 .....	9
啟用SnapCenter 支援Azure NetApp Files 功能的支援功能 .....	10
安裝HDBSQL用戶端 .....	13
使用支援服務來保護SAP HANA系統SnapCenter .....	15
新增SAP HANA系統 .....	15
備份SAP HANA系統 .....	16
還原SAP HANA系統 .....	17
管理營運 .....	18
疑難排解問題 .....	19
知識與支援 .....	21
註冊以取得支援 .....	21
取得協助 .....	22
法律聲明 .....	24
版權 .....	24
商標 .....	24
專利 .....	24
隱私權政策 .....	24
開放原始碼 .....	24

# 支援服務文件**SnapCenter**

# 更新功能SnapCenter

深入瞭解SnapCenter 解《服務》的新功能。

## 2021年12月21日

### Apache log4j弱點的修正程式

感謝支援服務1.0.1將Apache log4j從2.9.1版升級至2.17版、以解決下列弱點：-2021至44228、-2021至4104及-2021至45105。SnapCenter

支援此功能的叢集應自動更新至最新版本。SnapCenter您應該確定SnapCenter 「支援服務」 UI中的版本顯示叢集為1.0.1.1251或更新版本。

## 2021年10月13日

### 支援SnapCenter S檢修1.0.0

- 支援NetApp®雲端儲存設備上執行的應用程式、可利用此服務提供資料保護功能。SnapCenterNetApp Cloud Manager內啟用的支援功能可為駐留在原地（anf）的SAP HANA®系統、提供高效率、應用程式一致且原則型的備份與還原功能。SnapCenter Azure NetApp Files

["深入瞭解SnapCenter 解支援服務"](#)

- 您應該建立連接器、啟用SnapCenter 「還原服務」、新增SAP HANA系統、然後執行備份與還原作業。

["開始使用"](#)

# 開始使用

## 深入瞭解SnapCenter 解支援服務

支援NetApp®雲端儲存設備上執行的應用程式、可利用此服務提供資料保護功能。SnapCenterNetApp Cloud Manager內啟用的支援功能可為駐留在原地的SAP HANA®系統、提供高效率、應用程式一致、原則型的備份與還原功能。SnapCenter Azure NetApp Files

### 架構

支援下列元件的架構SnapCenter：

- 支援服務UI與Cloud Manager使用者介面整合。SnapCenter

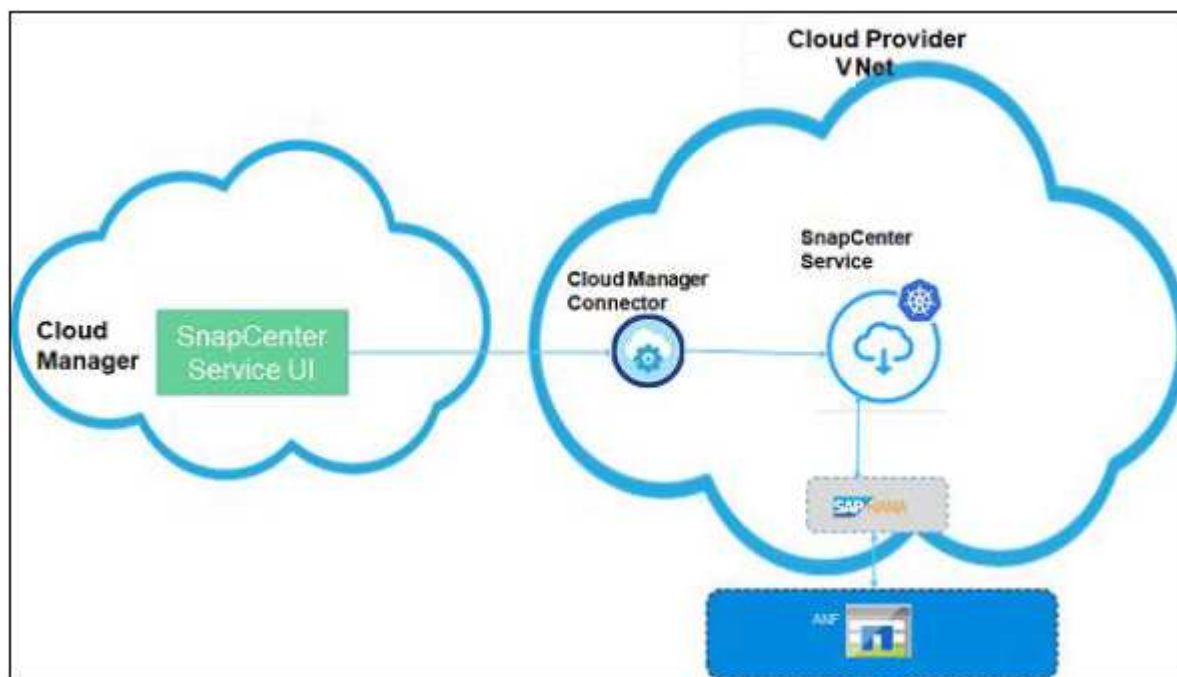
透過NetApp管理的Cloud Manager SaaS架構提供支援、提供多種儲存與資料管理功能。SnapCenter

- Cloud Manager Connector是Cloud Manager的一個元件、可管理SnapCenter 整個過程中的各種功能、包括支援各種服務。
- 支援支援支援Azure Kubernetes Service（以下稱為「支援服務」）的一組資料保護服務、可協調資料保護工作流程。SnapCenter



Cloud Manager Connector與SnapCenter 《支援服務：雲端管理程式》已部署在您的雲端網路中。

下圖顯示SnapCenter 了各個元件之間的關係：



若為任何使用者提出的要求、SnapCenter 則「支援服務」UI會與Cloud Manager SaaS進行通訊、驗證要求後、該SaaS會將通話轉接至Cloud Manager Connector。連接器接著會與SnapCenter IsoreService通

訊、SnapCenter 而IsoreService會叫用Azure NetApp Files Isormangement API和HANA系統命令來執行資料保護作業。

可在HANA系統的相同vnet或不同的vnet中部署支援。SnapCenter如果SnapCenter 使用不同網路的是「支援服務」和HANA系統、您應該在兩者之間建立網路連線。

## 支援的功能

支援下列功能。SnapCenter

- 新增SAP HANA系統
- 備份SAP HANA系統
  - 同時支援快照型和檔案型備份
  - 支援SAP HANA系統的隨需備份
  - 使用系統定義的原則或自訂原則、支援SAP HANA系統的排程備份

您可以在原則中指定不同的排程頻率、例如每小時、每日、每週和每月。

- 支援非資料磁碟區和全域非資料磁碟區的備份
- 根據原則保留備份
- 從使用者指定的備份還原SAP HANA系統
- 監控備份和其他工作
- 在HANA系統上管理資料和記錄備份目錄
- 在儀表板上顯示保護摘要、組態詳細資料和工作狀態
- 透過電子郵件傳送警示

## 限制

支援下列限制：SnapCenter

- 不支援國際化、您應該使用英文瀏覽器。
  - 只有具備「Account Admin」角色的Cloud Manager使用者才能啟用SnapCenter 此功能。
  - Azure Kubernetes Service (KS) 叢集節點故障的相關限制
    - 如果其中一個節點離線、則在使用者叢集中、執行中工作可能會失敗、但後續工作將會執行。
    - 在高效能叢集中、如果其中一個節點停機、您就無法新增SAP HANA系統、但其他作業也能順利執行。
- 您應該叫出節點來新增HANA系統。
- 排程器不支援高可用度組態。

如果排程器使用的MySQL節點當機、您應該叫出節點、讓排程的作業繼續進行。

# 開始使用

立即開始SnapCenter 使用支援服務、只需幾個步驟即可保護您的資料。

您應該 ["註冊NetApp Cloud Central"](#)、["登入Cloud Manager"](#)，然後設定 ["NetApp帳戶"](#)。

只有帳戶管理員才能部署SnapCenter 此功能。不過、帳戶管理員和SnapCenter 支援部門可以執行不同的作業。 ["深入瞭解"](#)

您應該確保一切順利 ["先決條件"](#) 建立連接器並啟用SnapCenter 「支援不支援服務」。

您應該 ["在Azure中建立連接器SnapCenter 以利服務"](#)。

如果您的連接器符合所有先決條件、您可以使用該連接器。

在 Azure NetApp Files Cloud Manager 中建立一個可運作的環境、以建立及管理 NetApp 帳戶、容量資源池、磁碟區和快照。 ["深入瞭解"](#)

您應該 ["啟用SnapCenter 支援服務"](#) 使用Cloud Manager UI。啟用此功能時、會建立Azure Kubernetes Service (aks) 叢集、以裝載此服務。SnapCenter SnapCenter

您應該 ["安裝HDBSQL用戶端"](#) 在SAP HANA資料庫上執行資料保護作業。HDBSQL用戶端用於與SAP HANA系統通訊。

您應該手動進行 ["新增SAP HANA系統"](#)。

您可以這樣做 ["備份SAP HANA系統"](#) 使用系統定義或自訂原則。萬一資料遺失、您可以 ["還原SAP HANA系統"](#) 使用該系統的備份。

## 建立連接器及啟用SnapCenter 「支援服務」的先決條件

在Azure中建立連接器並啟用SnapCenter 「功能性支援」之前、您應該先確定某些事項。

- 請確定為連接器選擇的子網路不應與下列為Azure Kubernetes Service (AKS) 保留的IP位址範圍重疊：  
169.254.0/16、172.30.0/16、172.31.0.0/16和192.0/24。
- 確保所選子網路中沒有執行的問題。
- 確保所選的子網路可存取各連接埠上的SAP HANA系統。
- 如果所選子網路的vnet與SAP HANA系統的vnet不同、請確認VNets可以透過VPN閘道、對等或其他方式彼此通訊。
- 如果您想要在SnapCenter 防火牆後啟用「支援服務」、請執行中所述的動作 [\[Network requirements\]](#)。

您應該事先決定是否要在SnapCenter 防火牆後啟用「支援服務」。啟用SnapCenter 「支援服務」之後、您無法將其設定為在防火牆後執行。這是一個高峰限制。

## 網路需求

設定您的網路、以便Connector管理雲端環境中的資源和程序。

## 防火牆組態

如果您想要在SnapCenter 防火牆後啟用「支援服務」、請執行下列動作。



如果您使用Azure防火牆、可以使用指令碼執行這些步驟。如需相關資訊、請參閱 [\[Azure Firewall configuration\]](#)。

### 步驟

1. 將下列網路規則新增至防火牆。

目的地端點	傳輸協定	連接埠	註解
"服務標籤" - AzureCloud。<地區>:1194	UDP	1194	如果您打算擁有私有連接器和私有SnapCenter 的支援服務叢集、則不需要。
"服務標籤" - AzureCloud。<地區> : 9000	TCP	9000	如果您打算擁有私有連接器和私有SnapCenter 的支援服務叢集、則不需要。
FQDN : ntp.ubuntu.com:123	UDP	123.	Azure虛擬機器的時間同步化所需。
"服務標籤" - AzureCloud。<地區>:443	TCP	443..	如果您打算擁有私有連接器和私有SnapCenter 的支援服務叢集、則不需要。

2. 在防火牆中新增應用程式規則、並附上下列FQDN標記和連接埠詳細資料：
  - FQDN標記- AzureKubernetesService
  - HTTPS : 443
3. 新增以下端點作為目標FQDN的應用程式規則、其傳輸協定和連接埠為HTTPS : 443。

端點	目的
https://management.azure.com https://login.microsoftonline.com	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP 大多數 Azure 地區部署及管理功能。
https://management.microsoftazure.de https://login.microsoftonline.de	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure Germany 地區部署及管理功能。
https://management.usgovcloudapi.net https://login.microsoftonline.com	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure US Gov 地區部署及管理功能。
https://api.services.cloud.netpp.com	允許API要求至NetApp Cloud Central。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。



端點	目的
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	讓 Connector 能夠存取及下載資訊清單、範本及 Cloud Volumes ONTAP 升級影像。
https://cloudmanagerinfraproduct.azurecr.io	存取執行 Docker 之基礎架構的容器元件軟體映像、並提供與 Cloud Manager 整合服務的解決方案。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 NetApp 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://support.netapp.com	與 NetApp AutoSupport 通訊
https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	與 NetApp 溝通以取得系統授權與支援登錄。
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com	讓 NetApp 能夠收集疑難排解支援問題所需的資訊。
* .blob.core.windows.net	使用 Proxy 時 HA 配對必須具備此功能。
https://auth0.com	驗證驗證所需的項目。
https://registry-1.docker.io https://auth.docker.io https://production.cloudflare.docker.com	擷取 SnapCenter 相依於「支援服務」工作流程引擎的項目。
https://exteranl-log.cloudmanager.netapp.com	允許通訊將記錄傳輸至 Cloud Manager 記錄儲存庫。

4. 選擇您要安裝 SnapCenter 的子網路。
5. 使用路由建立路由表：
  - 將流量從子網路轉送到防火牆內部 IP 位址
  - 將流量從防火牆的公用 IP 位址轉送到網際網路。
6. 將路由表附加至子網路。

如需 Cloud Manager Connector 網路需求的相關資訊、請參閱 ["連接器的網路需求"](#)。

## Azure 防火牆組態

如果您想要在 SnapCenter Azure 防火牆後啟用「支援服務」、請執行下列動作。

您需要的是什麼


- 您應該已經建立防火牆（傳統模式）。
- 您應該已經建立 Vnet 和子網路以供 SnapCenter 使用。

- 如果您的防火牆資源和vnet SnapCenter of the不同時租戶、您應該登入Azure Shell中的兩個租戶。
- 如果您的防火牆vnet和SnapCenter 物件不一樣、您應該在VNets之間建立對等關係。

## 步驟

1. 下載 "[scs\\_azure\\_firewall\\_config.sh](#)" 指令碼至您的本機系統。

2. 登入 "[Microsoft Azure入口網站](#)"。

3.  按一下 若要開啟雲端Shell並選取Bash主控台。

a. 將指令碼上傳至Azure雲端Shell。

b. 指派執行指令碼的權限。

```
"chmod+x ./sSC_azure_firewall_config.sh"
```

c. 執行指令碼。

```
/scs_azure_firewall_config.sh -fwsubid <Firewall_SubscriptionID>-fwname <Firewall_name>-fwrg  
<Firewall_Resource_Group>-scssubid <SnapCenter_Service_SubscriptionID>-scsvnet  
<SnapCenter_Service_net_name>-Snapscra_Resource <Snapscr_Center_Service_net_name>
```



如果您尚未建立資源群組、指令碼會建立資源群組。建立Connector時、您可以使用相同的資源群組、讓SnapCenter 所有的相關資源都位於相同的資源群組中。

## 結果

- 已設定防火牆規則。
- 系統會建立資源群組以供SnapCenter 支援服務使用。
- 路由表會在SnapCenter 「支援服務」資源群組中建立。
- 已設定路由表規則。
- 路由表會附加至子網路。

## 連線至HANA系統

支援服務叢集需要使用HDBSQL命令、與使用者網路中的HANA系統進行通訊。SnapCenter需要使用各種網路架構來允許使用叢集與HANA系統之間的通訊通道SnapCenter 、例如：

- 連接器和SnapCenter S檢修 叢集部署在HANA系統的相同vnet上
- 連接器和SnapCenter 物件服務叢集部署在不同於HANA系統的Vnet中、並使用2個VNets之間的vnet對等機制來建立通訊。
- 連接器和SnapCenter 物件服務叢集部署在不同於HANA系統的Vnet中、並使用兩個VNets之間的VPN閘道來建立通訊。

## 安全性群組組態

如果在HANA系統中設定了網路安全群組（NSG）、則應允許傳入通訊、從SnapCenter 支援服務的連接埠、到

使用者存放區金鑰中指定的HANA系統連接埠。

- 傳輸協定：All TCP
- 子網路：SnapCenter 叢集子網路的功能
- 目的：執行HDBSQL命令

執行於支援SSL的HANA系統SnapCenter、可在支援SSL的情況下、與執行此功能的HANA叢集進行SSL通訊。

## 在Azure中建立連接器SnapCenter 以利服務

客戶管理員應先部署Connector、然後才能使用Cloud Manager功能。Connector 可讓Cloud Manager 管理公有雲環境中的資源與程序。

根據預設、您可以從Azure Marketplace在Azure中建立連接器。執行的步驟 "[從Azure Marketplace建立連接器](#)" 請記住下列事項：

- 只要Cloud Volumes ONTAP 指定Cloud Manager for Sfor Sfor、SnapCenter 就能運用相同的功能來執行支援服務。
- 針對Cloud Manager名稱、請指定您的Connector VM名稱、以利識別。這會在Cloud Manager UI中顯示為連接器名稱。
- 如果您已設定連接器而沒有公用IP或設定防火牆、則應該有跳接主機來連線至連接器機器。

如果您有 "[使用者同意](#)" 您可以在Azure Active Directory中啟用、或是如果租戶管理員可以提供同意、您可以從Cloud Manager UI建立Connector。

### 已啟用使用者同意

如果您的Azure Active Directory已啟用使用者同意、"[從Cloud Manager建立Connector](#)"。

### 使用者同意已停用

#### 1. 執行下列其中一項：

- 如果系統管理員同意工作流程已設定在您的Active Directory中、您應該 "[要求管理員同意](#)"。
- 如果未設定管理員同意工作流程、您應該：
  - i. "[建構URL以授予全租戶管理員同意](#)"。



將clientID指定為\_989efff4-9a9e-46fa-9f17-de39e15714f9\_。這是Cloud Manager精靈中所命名的Cloud Manager Azure應用程式ID。

- ii. 請租戶管理員在瀏覽器中執行URL、並取得他的同意。

您的管理員可以忽略顯示的錯誤

#### 2. "[從Cloud Manager建立Connector](#)"。



建立連接器時所提供的使用者名稱和密碼、或金鑰、都是連線至機器所需的

# 啟用SnapCenter 支援Azure NetApp Files 功能的支援功能

您可以SnapCenter 使用Cloud Manager UI啟用此功能。啟用此功能時、會建立Azure Kubernetes Service (aks) 叢集、以裝載此服務。SnapCenter SnapCenter

您需要的是什麼

- 您應在Azure訂閱中註冊「Microsoft.ContainerService」資源供應商。如需相關資訊、請參閱 ["如何註冊資源提供者"](#)。
- 您應該確保一切順利 ["先決條件"](#) 達成。

關於此工作

在建立Connector時、會在相同的資源群組和所選的相同子網路中建立高效能叢集。如果您建立的Connector沒有公有IP位址、則會以私有模式建立使用者叢集。

使用者必須指派具有必要權限的託管身分識別、才能建立及管理高效能叢集。系統會建立指派給使用者的託管身分識別、並將其指派給Connector VM。

步驟

1. 登入Cloud Manager。
2. 選取在Cloud Manager中建立的Connector。

確保連接器的網路連線能力可保護至SAP HANA系統。

3. 按一下\*所有服務\*>\* SnapCenter 《》《啟用》。
4. 執行下列其中一項：
  - 如果您已從Cloud Manager UI建立Connector、而且您有權限建立和指派角色、則SnapCenter 使用者指派的託管身分識別將會透過安裝此功能自動建立。
    - i. 選取\*使用Azure登入\*。
    - ii. 在「Get Ready (準備就緒)」頁面上、按一下\*繼續\*。
    - iii. 指定Azure認證資料。




您應確保Azure登入帳戶擁有足夠的權限。如需權限及如何指派權限的相關資訊、請參閱 [\[Permissions required for Azure login account\]](#)。

- 如果您是從Azure市場建立Connector、或是沒有權限建立及指派角色、請依照下列步驟建立使用者指派的託管身分識別。
  - i. 選取\*使用Azure CLI指令碼\*。
  - ii. 如果您對Azure帳戶沒有足夠的權限、請聯絡您的管理員。

如需權限及如何指派權限的相關資訊、請參閱 [\[Permissions required for Azure login account\]](#)。

- iii. 下載 ["prerequisite\\_azure.sh"](#) 指令碼至您的本機系統。
- iv. 登入 ["Microsoft Azure入口網站"](#)。

v. 按一下  若要開啟雲端Shell並選取Bash主控台。

vi. 將指令碼上傳至Azure雲端Shell。

vii. 指派執行指令碼的權限。

```
"chmod+x ./prerite_azure.sh"
```

viii. 執行指令碼。

```
prerequisite_azure.sh -s <dentition_ID>-g <connector資源組名稱>-c <connector VM名稱>'
```

5. 在「Cluster Configuration」（叢集組態）頁面上、執行下列步驟：

a. 選取叢集組態。

- 如果您選取\*高可用度\*、則會在可用區域之間建立一個Azure Kubernetes服務（KS）叢集、其中包含3個工作節點。
- 如果選擇\*單一節點\*、將會建立具有單一節點的高效能叢集。

b. 指定Kubernetes Pod位址範圍。

確保Kubernetes Pod位址範圍不會與虛擬網路、連接的虛擬網路、連接的內部部署網路的IP範圍重疊。此外、範圍不應與服務位址範圍和Docker橋接器位址重疊。

c. 指定Kubernetes服務位址。

確保Kubernetes服務位址範圍不會與虛擬網路、連接的虛擬網路、連接的虛擬網路和內部部署網路的IP範圍重疊。此外、範圍不應與Pod位址範圍和Docker橋接器位址重疊。

d. 指定Docker橋接器網路。

請確保Docker Bridge位址不會與虛擬網路的IP範圍、連接的虛擬網路、連接的虛擬網路和內部部署網路重疊。此外、範圍不應與Pod位址範圍和服務位址範圍重疊。

e. 如果建立的Connector沒有公用IP、而且您在vnet上使用自訂DNS伺服器、請選取\*支援自訂DNS伺服器\*。




您應該在專屬DNS區域中為裝載自訂DNS伺服器的VNETs建立虛擬網路連結。私有DNS區域名稱和資源群組名稱會顯示在UI上。

6. 在「檢閱」頁面上、檢閱詳細資料、然後按一下「啟用」。

7. 成功啟用SnapCenter 此功能後、按一下\*「Finish」（完成）\*。

結果

- 成功啟用SnapCenter 「支援不支援服務」之後、就會建立「高效能叢集」。您可以按一下以檢視「高」叢集詳細資料 。



如果您無法啟用SnapCenter 此功能、可以修正問題、然後按一下\*重試\*。

- 建立使用者指派的託管身分識別之後、系統會將其指派給自訂角色。
  - 指派給使用者的託管身分識別、將指派給具有下列Connector資源群組範圍權限的自訂角色：

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.ContainerService/managedClusters/read",
"Microsoft.ContainerService/managedClusters/write",
"Microsoft.ContainerService/managedClusters/delete",
"Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Network/networkInterfaces/read"
```

- 指派給使用者的託管身分識別、將指派給具有下列Connector vnet權限的自訂角色：

```
"Microsoft.Authorization/roleAssignments/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/join/action"
```

- 如果在子網路上設定路由表來路由傳送至防火牆、則指派給使用者的受管理身分識別將會指派給具有下列路由表範圍權限的自訂角色。

```
"Microsoft.Network/routeTables/*",
"Microsoft.Network/networkInterfaces/effectiveRouteTable/action",
"Microsoft.Network/networkWatchers/nextHop/action"
```

- 如果連接器安裝時沒有公用IP、則指派給使用者的託管身分識別將會指派給自訂角色、並在私有DNS區域的範圍內具有下列權限。

```
"Microsoft.Network/privateDnsZones/*"
```

## Azure登入帳戶所需的權限

Azure登入帳戶可用來建立使用者指派的託管身分識別、必要角色、以及將身分識別指派給Connector VM。



登入帳戶的認證資料不會儲存在SnapCenter 任何地方、也不會用來呼叫API。認證資料僅用於UI 中。

### 步驟

1. 使用建立自訂角色 "[SnapCenter\\_Deployment角色、json](#)" 檔案：

您應該使用Azure訂閱ID來取代SnapCenter\_Deployment角色1.json檔案中的<Subscription\_ID>。

2. 將角色指派給Connector資源群組範圍內的登入帳戶。
3. 使用建立自訂角色 "[SnapCenter\\_Deployment\\_ROI2.json](#)" 檔案：

您應該使用Azure訂閱ID來取代SnapCenter\_Deployment角色2.json檔案中的<Subscription\_ID>。

4. 將角色指派給Connector vnet或更高版本範圍內的登入帳戶。
5. 如果您有 "[已設定防火牆](#)"、使用建立自訂角色 "[SnapCenter-Deployment：角色3.json](#)" 檔案：

您應將SnapCenter\_Deployment角色3.json檔案中的<Subscription\_ID>替換為Azure訂閱ID。

6. 將角色指派給位於路由表範圍內的登入帳戶、該表會附加到SnapCenter 該子網路。

## 安裝HDBSQL用戶端

啟用SnapCenter 完「支援服務」之後、請安裝HDBSQL用戶端、以便在SAP HANA資料庫上執行資料保護作業。HDBSQL用戶端用於與SAP HANA系統通訊。

### 步驟

1. 從SAP帳戶下載HDB用戶端軟體。

這是副檔名為（.SAR）的歸檔檔案。範例：IMDB\_CLIENT20\_008\_20-80002082.SAR



HDB用戶端軟體版本應為2.4.202.1590784230或更新版本。

2. 從SAP帳戶下載最新的SAPCAR公用程式。範例：[SAPCAR\\_1010-70006178.Ex](#)
3. 在Cloud Manager UI上、按一下\* Connector\*以取得連接器名稱。
4. 登入 "[Microsoft Azure入口網站](#)"。
5. 按一下\*虛擬機器\*。
6. 搜尋Cloud Manager Connector、然後複製指派給Connector的公有IP位址。

如果連接器未啟用公用IP、您應該使用跨接主機。

7. 將SAPCAR公用程式和HDB用戶端歸檔（.SAR）檔案複製到Connector機器。

若要將檔案複製到Connector路徑、您需要認證資料或建立Connector時提供的金鑰。

- 「CP <SAPCAR\_service><username>@<ip\_address>:/home/<username>'
- 「CP <HDB\_Client\_archive ><username>@<ip\_address>:/home/<username>'

檔案會複製到\_/home/<使用者名稱>\_。

8. 使用ssh認證或金鑰登入Connector VM。

9. 在Connector VM中執行下列命令、以在下列系統中安裝HDBSQL用戶端。
- a. 「Udo CP /home/<使用者名稱>/<SAPCAR\_UTIT>/var/lib/dred/voles/cloudmanager\_snapcenter\_volVolume /資料/」
  - b. 「Udo CP /home/<使用者名稱>/< HDB\_Client\_archive>/var/lib/ded泊 塢/磁碟區/cloudmanager\_snapcenter\_volume /\_data/」
  - c. 「Udo Docker執行- IT cloudmanager\_snapcenter /bin/bash /opt/netapp/hdbclient/hdbclient.sh - archivefile <HDB\_Client\_archive>- archiveutil<SAPCar\_utile>」

瞭解更多資訊

["如何使用scp移動檔案"](#)



# 使用支援服務來保護SAP HANA系統SnapCenter

## 新增SAP HANA系統

手動新增SAP HANA系統。不支援自動探索SAP HANA系統。

新增SAP HANA系統時、您應該新增HDB使用者儲存金鑰。HDB安全使用者存放區金鑰可用來將SAP HANA系統的連線資訊安全地儲存在用戶端上、而HDBSQL用戶端則使用安全的使用者存放區金鑰來連線至SAP HANA系統。



如果使用SAP HANA叢集中的節點當機、您就無法新增或修改SAP HANA系統。

### 步驟

1. 在「支援服務」頁面上、按一下SnapCenter 「\* SAP HANA Systems\*>\* Add\*」。
2. 在「系統詳細資料」頁面上、執行下列動作：
  - a. 選取系統類型。
  - b. 指定SAP HANA系統的SID。
  - c. 指定SAP HANA系統名稱。
  - d. 按一下HDB Secure User Store Keys (HDB安全使用者儲存金鑰) 文字方塊以新增使用者儲存金鑰詳細資料

指定金鑰名稱、系統詳細資料、使用者名稱和密碼。

- e. 按一下「\* 新增 \*」。



如果您要新增多主機SAP HANA系統、則應該為每個主機新增使用者儲存金鑰。

3. 按一下 \* 繼續 \* 。
4. 在Storage Footprint頁面上、執行下列步驟：
  - a. 選取工作環境並指定NetApp帳戶。
  - b. 選取所需的磁碟區。
  - c. 按一下「新增儲存設備」。
5. 按一下 \* 繼續 \* 。
6. 檢閱所有詳細資料、然後按一下\*「Add\* (新增\*)」。

您也可以編輯或移除SnapCenter 已新增至「支援服務」的SAP HANA系統。當您移除SAP HANA系統時、所有相關的備份和目錄項目都會刪除、不再受到保護。


## 新增非資料磁碟區

新增多租戶資料庫容器或單一容器類型的SAP HANA系統之後、即可新增HANA系統的非資料磁碟區。

## 步驟

1. 在「支援服務」頁面上、按一下SnapCenter SAP HANA Systems。

畫面會顯示所有新增至SnapCenter 該服務的系統。

2. 按一下  對應到您要新增非資料磁碟區的多租戶資料庫容器或單一容器類型系統。
3. 按一下「新增非資料磁碟區」。
4. 按一下「新增儲存設備」。

## 備份SAP HANA系統

您可以使用系統定義或自訂原則、執行隨需備份或排程SAP HANA系統備份。支援Snapshot型和檔案型備份。SnapCenter

### 建立備份原則

原則指定備份類型、備份頻率、排程、保留類型、保留計數、以及資料保護作業的其他特性。您可以使用Cloud Manager UI來建立原則。

根據預設、有兩個系統定義的原則可供使用、每個原則分別用於快照型和檔案型備份作業。

## 步驟

1. 在「支援服務」頁面上、按一下SnapCenter 「原則」 > 「新增」。
2. 在「Create Backup Policy（建立備份原則）」頁面上、執行下列動作：
  - a. 指定原則名稱。
  - b. 選取您要使用此原則建立的備份類型。
  - c. 指定備份名稱。

預設會新增後置時間戳記。您可以選取備份名稱中應包含的其他尾碼、並定義尾碼的顯示順序。

- d. 指定排程備份的排程頻率、以及排程備份的開始和結束時間。
  - e. 指定要保留的快照複本數目、或指定保留快照複本的天數。
3. 按一下「\* 新增 \*」。

按一下即可檢視、編輯或刪除原則  與原則對應。

### 建立隨需備份

建立原則關聯或不關聯任何原則、即可建立SAP HANA系統的隨需備份。

## 步驟

1. 在「支援服務」頁面上、按一下SnapCenter 「\* SAP HANA Systems\*」。

畫面會顯示所有新增至SnapCenter 該服務的系統。

2. 按一下 ... 與您要保護的系統相對應。
3. 按一下\*隨需備份\*。
4. 在「隨需備份」頁面上、執行下列其中一項動作：
  - 如果要將備份與原則關聯、請選取原則、然後按一下「建立備份」。
  - 如果您不想將備份與原則建立關聯、請執行下列動作：
    - i. 在Policy（策略）字段中，選擇\* None"（無）\*。
    - ii. 選取備份類型。

如果您要備份非資料磁碟區、則只能選取\* Snapshot Based \*作為備份類型。

- iii. 指定保留期間。
- iv. 按一下「建立備份」。

## 建立排程備份

將原則與SAP HANA系統建立關聯、以建立排程備份。

### 步驟

1. 在「支援服務」頁面上、按一下SnapCenter 「\* SAP HANA Systems\*」。
- 畫面會顯示所有新增至SnapCenter 該服務的系統。
2. 按一下 ... 與您要保護的系統相對應。
3. 按一下\*保護\*。
4. 選取您要用來保護SAP HANA系統的原則。
5. 按一下\*保護\*。

\*瞭解更多資訊\*<https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-backup-anf-overview.html>["SAP HANA利用Azure NetApp Files NetApp服務在支援功能的基礎上進行備份與還原SnapCenter"^]

## 還原SAP HANA系統

萬一資料遺失、請從該系統的備份之一還原SAP HANA系統。

僅支援儲存還原。因為不支援還原HANA系統、所以您應該先使用SAP HANA Studio或SAP HANA Cockpit將HANA系統置於還原模式。

### 步驟

1. 在「支援服務」頁面上、按一下SnapCenter 「\* SAP HANA Systems\*」。
- 畫面會顯示加入SnapCenter 到「畫面服務」的系統。
2. 按一下 ... 與您要還原的系統相對應。

3. 按一下「檢視備份」。
4. 在備份區段中、按一下 ... 與您要用來還原系統的備份相對應。
5. 按一下 \* 還原 \*。
6. 檢閱訊息並選擇\*是、還原\*進行確認。



還原資料庫之後、如果您使用HANA Studio對SAP HANA系統進行時間點還原、SnapCenter 則可能會還原根據保留設定由還原服務刪除的資料備份目錄項目。如果刪除的資料備份目錄項目因為恢復作業而還原、SnapCenter 則無法偵測並刪除這些項目。這可能導致SnapCenter 無法正確清理記錄目錄。您可以驗證SnapCenter 支援服務中的備份項目、找出哪些資料備份目錄項目是新還原的項目、然後手動刪除這些項目。

\*瞭解更多資訊<https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-backup-anf-overview.html>["SAP HANA利用Azure NetApp Files NetApp服務在支援功能的基礎上進行備份與還原SnapCenter"]

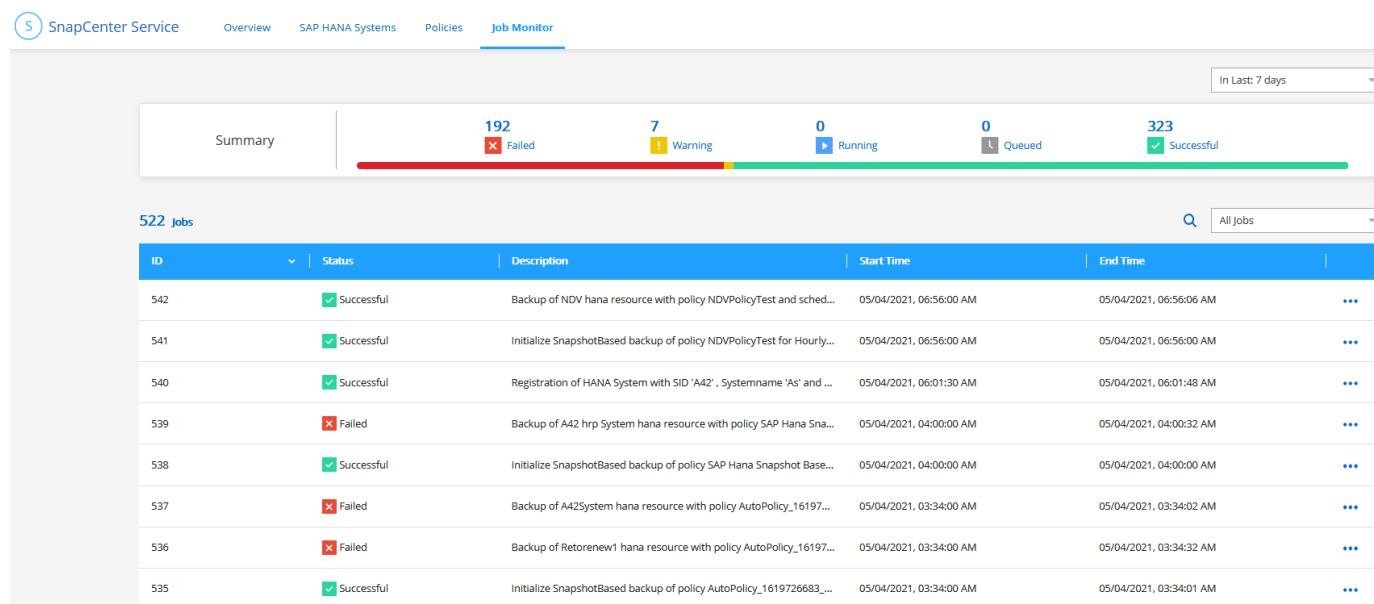
## 管理營運

您可以監控已執行工作的狀態、接收電子郵件通知、以及檢視儀表板。

### 監控工作

按SnapCenter 一下「支援服務」頁面上的\*工作監控\*、即可檢視工作狀態。「工作監控」頁面會顯示整體摘要、並列出所有工作。

然後按一下 ... 以檢視詳細資料。

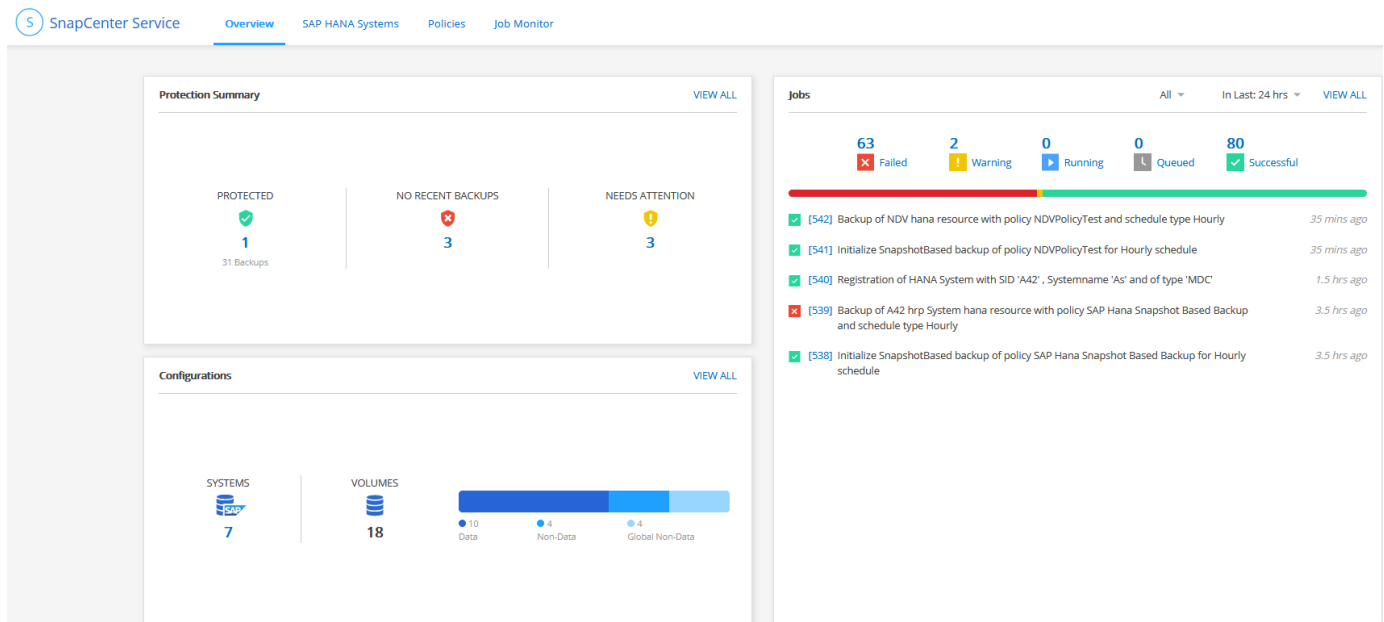


### 電子郵件通知

根據預設、系統會針對隨需備份、排程備份和還原作業失敗、傳送電子郵件通知。只有具備「帳戶管理員」角色的Cloud Manager使用者才會收到電子郵件。

## 檢視儀表板

按SnapCenter 一下「支援服務」頁面上的「總覽」、即可檢視保護摘要、組態詳細資料及工作狀態。



## 疑難排解問題

### 問題：Redis Pod陷入CrashLoopBackOff狀態

\*說明\*在高可用度組態中、如果叢集的所有節點都當機、則會使高可用度叢集恢復正常運作狀態。當您重新啟動所有節點時、可能會發現所有的Redis Pod都處於CrashLoopBackOff狀態。

\*解決方案\*您應該執行下列命令來還原系統。

1. 登入Connector。
2. 刪除所有Redis Pod。
  - 「Docker執行-it cloudmanager\_snapcenter --sh」
  - 「kubectl scale -複本= 0 STS-dasions- redis節點- n SnapCenter 」
3. 確認是否已刪除所有Redis Pod。「kubectl Get pod -n SnapCenter 架次」
4. 如果Redis Pod未刪除、請執行下列命令：
  - 「kubectl刪除pod sc-das依賴 關係-redis節點-0 -n SnapCenter sce」
  - 「kubectl刪除pod sc-dresase-redis節點1 -n SnapCenter sce」
  - 「kubectl刪除pod sc-dresase-redis節點2 -n SnapCenter sce」
5. 刪除所有Redis Pod之後、請執行：「kubectl scale -複本=3 STs sc-dasions- redis節點- n SnapCenter fes」
6. 確認所有刪除的Pod是否都已啟動且正在執行。「Kubectl Get pod -n SnapCenter 架次」

## 問題：重新啟動叢集節點後、工作發生故障

**\*說明\***在高可用度組態中、如果叢集的所有節點都當機、則會使高可用度叢集恢復正常運作狀態。當您重新啟動所有節點時、可能會看到工作發生故障、而精細的工作會變成灰色或逾時。

**\*解決方案\***您應該執行下列命令：

1. 登入Connector。
2. 儲存RabbitMQ statefulset (STS-) 部署。
  - 「Docker執行-it cloudmanager\_snapcenter --sh」
  - 「kubectl Get STS RabbitMQ -o yaml -n SnapCenter flexec> RabbitMQ\_STs.yaml」
3. 識別連接至RabbitMQ Pod的持續磁碟區 (PV) 。 「kubectl Get PV | grep RabbitMQ」
4. 刪除附加至RabbitMQ Pod的持續磁碟區宣告 (PVCS) 。 「kubectl Get PVC -n SnapCenter feze| grep RabbitMQ | awk {'print \$1'} | xargs kubectl DELETE PVC -n SnapCenter fas」
5. 刪除您先前在步驟3中識別的每個PV 。 「kubectl DELETE PV 'PVname」
6. 建立RabbitMQ狀態 。 「kubectl create -f RabbitMQ\_STs.yaml -n SnapCenter sety

## 問題：在租戶資料庫建立期間、備份作業失敗

**\*說明\***如果啟動隨需或排程備份、則在建立租戶資料庫時、備份作業會失敗。

**\*解決方案\***建立租戶資料庫是SAP HANA系統的維護作業。

建立租戶資料庫之前、您應該先使用SnapCenter 還原服務將SAP HANA系統置於維護模式。將SAP HANA系統置於維護模式之後、便無法啟動任何作業。

建立租戶資料庫之後、您應該將SAP HANA系統恢復為正式作業模式。

# 知識與支援

## 註冊以取得支援

在您透過NetApp技術支援開啟支援案例之前、您必須先將NetApp支援網站帳戶新增至Cloud Manager、然後註冊以取得支援。

### 新增一個NSS帳戶

「支援儀表板」可讓您從單一位置新增及管理所有NetApp支援網站帳戶。

#### 步驟

1. 如果您還沒有 NetApp 支援網站帳戶、"註冊一項"。
2. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取\*「支援」\*。



3. 按一下「」 「nss管理」 > 「新增nssAccount」。
4. 出現提示時、按一下\*繼續\*以重新導向至Microsoft登入頁面。

NetApp使用Microsoft Azure Active Directory做為身分識別供應商、提供專為支援與授權所設計的驗證服務。

5. 在登入頁面上、提供您的NetApp支援網站註冊電子郵件地址和密碼、以執行驗證程序。

此動作可讓Cloud Manager使用您的NSS帳戶。

附註：帳戶必須是客戶層級的帳戶（非來賓帳戶或臨時帳戶）。

### 註冊您的帳戶以取得支援

支援註冊可從支援儀表板的Cloud Manager取得。

#### 步驟

1. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取\*「支援」\*。



2. 在\* Resources（資源）選項卡中，單擊 Register for Support\*（註冊以獲得支持\*）。
3. 選取您要登錄的NSS認證、然後按一下「登錄」。

## 取得協助

NetApp以多種方式支援Cloud Manager及其雲端服務。我們全年無休提供豐富的免費自助支援選項、例如知識庫（KB）文章和社群論壇。您的支援註冊包括透過網路票證提供遠端技術支援。

### 自我支援

這些選項可供免費使用、一天24小時、一週7天：

- "知識庫"

請搜尋Cloud Manager知識庫、找出有助於疑難排解問題的文章。

- "社群"

加入Cloud Manager社群、追蹤後續討論或建立新討論。

- 文件

您目前正在檢視的Cloud Manager文件。

- <mailto:ng-cloudmanager-feedback@netapp.com> [意見反應電子郵件]

我們非常重視您的意見。提交意見反應、協助我們改善Cloud Manager。

### NetApp支援

除了上述的自我支援選項、您也可以與NetApp支援工程師合作、在您啟動支援之後解決任何問題。



## 步驟

1. 在Cloud Manager中、按一下\*「說明」>「支援」\*。
2. 在「Technical Support（技術支援）」下選擇可用的選項之一：
  - a. 按一下\*致電我們\*以尋找NetApp技術支援的電話號碼。
  - b. 按一下「開啟問題」、選取其中一個選項、然後按一下「傳送」。

NetApp代表將審查您的案例、並盡快回覆您。

# 法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

## 版權

<http://www.netapp.com/us/legal/copyright.aspx>

## 商標

NetApp、NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp、Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 專利

如需最新的 NetApp 擁有專利清單、請參閱：

<https://www.netapp.com/us/media/patents-page.pdf>

## 隱私權政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

- ["Cloud Manager 3.9 注意事項"](#)

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.