



開始使用 SnapCenter Service

NetApp
July 19, 2022

This PDF was generated from <https://docs.netapp.com/zh-tw/cloud-manager-snapcenter/concept-overview-architecture-limitation-functionalities-snapcenter-service.html> on July 19, 2022. Always check docs.netapp.com for the latest.

目錄

開始使用	1
深入瞭SnapCenter 解支援服務	1
開始使用	3
建立連接器及啟用SnapCenter 「支援服務」的先決條件	3
在Azure中建立連接器SnapCenter 以利服務	7
啟用SnapCenter 支援Azure NetApp Files 功能的支援功能	8
安裝HDBSQL用戶端	11

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

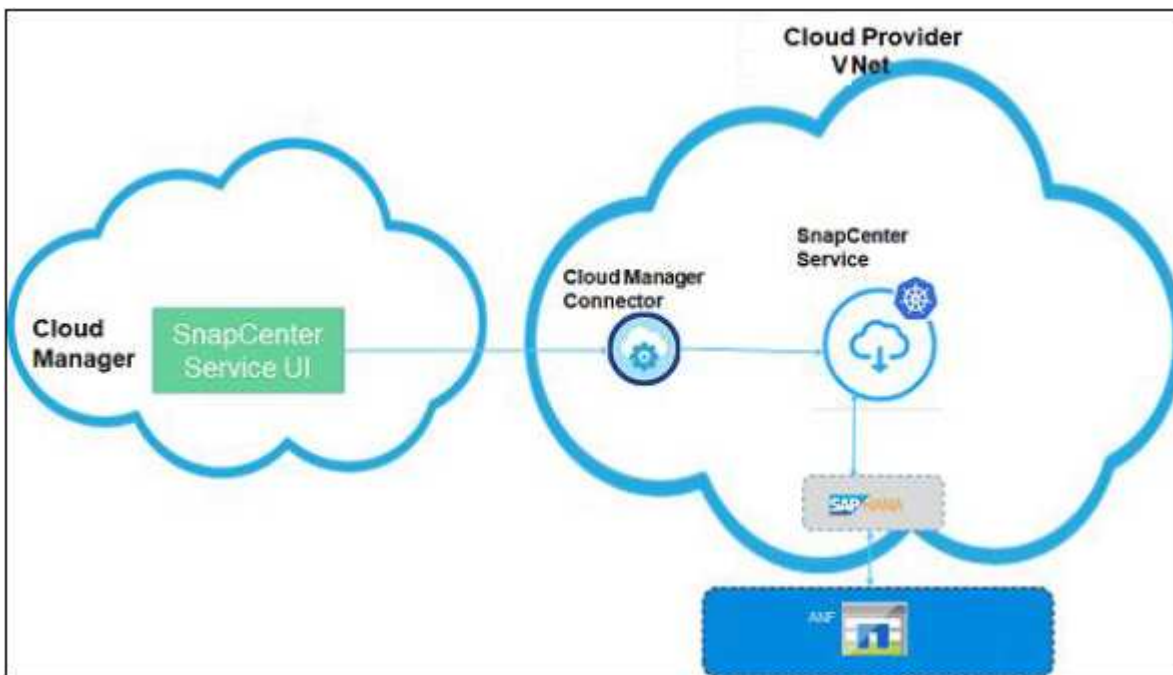
透過NetApp管理的Cloud Manager SaaS架構提供支援、提供多種儲存與資料管理功能。SnapCenter

- 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。

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"](#)

版權資訊

Copyright©2022 NetApp、Inc.版權所有。美國印製本文件中版權所涵蓋的任何部分、不得以任何形式或任何方式（包括影印、錄製、在未事先取得版權擁有者書面許可的情況下、在電子擷取系統中進行錄音或儲存。

衍生自受版權保護之NetApp資料的軟體必須遵守下列授權與免責聲明：

本軟體係由NetApp「依現狀」提供、不含任何明示或暗示的保證、包括但不限於適售性及特定用途適用性的暗示保證、特此聲明。在任何情況下、NetApp均不對任何直接、間接、偶發、特殊、示範、或衍生性損害（包括但不限於採購替代商品或服務；使用損失、資料或利潤損失；或業務中斷）、無論是在合約、嚴格責任或侵權行為（包括疏忽或其他）中、無論是因使用本軟體而產生的任何責任理論（包括疏忽或其他）、即使已被告知可能造成此類損害。

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。除非NetApp以書面明確同意、否則NetApp不承擔因使用本文所述產品而產生的任何責任或責任。使用或購買本產品並不代表NetApp擁有任何專利權利、商標權利或任何其他智慧財產權。

本手冊所述產品可能受到一或多個美國國家/地區的保護專利、國外專利或申請中。

限制權利圖例：政府使用、複製或揭露受DFARS 252.277-7103（1988年10月）和FAR 52-227-19（1987年6月）技術資料與電腦軟體權利條款（c）（1）（ii）分段所述限制。

商標資訊

NetApp、NetApp標誌及所列的標章 <http://www.netapp.com/TM> 為NetApp、Inc.的商標。其他公司和產品名稱可能為其各自所有者的商標。