



Azure 平台影像驗證

Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

Azure 平台影像驗證	1
Azure 影像驗證總覽	1
下載 Azure Image Digest File	1
映像從 Azure Marketplace 匯出	2
檔案簽章驗證	9
何處可以找到 Azure 影像驗證的其他資訊	12

Azure 平台影像驗證

Azure 影像驗證總覽

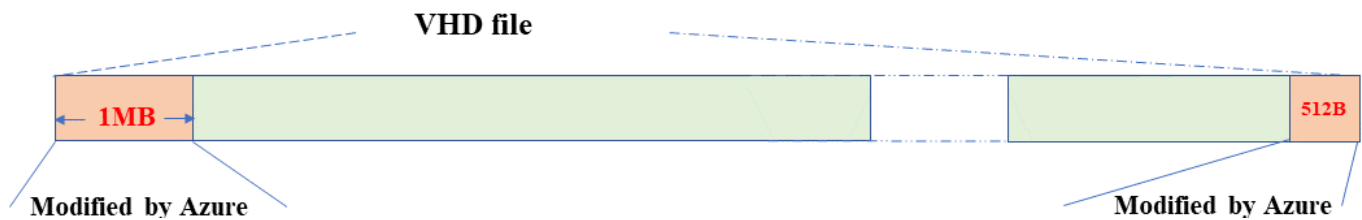
Azure 影像驗證符合增強的 NetApp 安全要求。雖然驗證映像檔案是一項簡單的程序、但 Azure 映像簽章驗證確實需要特別的資料、才能將其傳送至知名的 Azure VHD 映像檔、因為 Azure 市場已進行了一次替代。



Cloud Volumes ONTAP 軟體 9.15.0 版或更新版本支援 Azure 影像驗證。

Azure 對已發佈 VHD 檔案的變更

Azure 修改了領先業界的 1MB (1048576 位元組) 和結束 512 位元組 VHD 檔案。NetApp 映像簽署會略過前導的 1MB 並結束 512 個位元組、然後簽署剩餘的 VHD 映像部分。



例如、上圖顯示大小為 10GB 的 VHD 檔案。但 NetApp 簽署部分會以綠色標示、大小為 10GB - 1MB - 512B。

下載 Azure Image Digest File

Azure Image Digest File 可從下載 "[NetApp 支援網站](#)"。下載檔案為 tar.gz 格式、包含用於影像簽章驗證的檔案。

步驟

1. 前往 "[NetApp 支援網站](#) 上的 [Cloud Volumes ONTAP 產品頁面](#)" 並在「下載」區段下載所需的軟體版本。
2. 在 Cloud Volumes ONTAP 下載頁面下、按一下 Azure 影像摘要檔案的 * 下載按鈕 *、即可下載 TAR . gz 檔案。

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

3. 對於 Linux 和 MacOS 、您必須執行下列步驟、才能取得下載 Azure Image Digest 檔案的 md5sum 和 shav256sum 。

- a. 若為 md5sum 、請輸入 md5sum 命令。
- b. 若為 shaf256sum 、請輸入 sha256sum 命令。

4. 驗證 md5sum 和 sha256sum 值符合 Azure Image Digest File 下載。

5. 在 Linux 和 Mac OS 上、執行 `tar -xzf` 擷取 tar.gz 檔案的命令。

擷取的 TAR 。gz 檔案包含摘要檔案 (.sig) 、公開金鑰憑證檔案 (.pem) 和鏈結憑證檔案 (.pem) 。

- 列出解壓縮 tar.gz 檔案的結果 *

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp 384 May 13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May 13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 version_readme
```

映像從 Azure Marketplace 匯出

一旦 VHD 映像發佈至 Azure 雲端、該映像就不再由 NetApp 管理。而是將發佈的映像放在 Azure 市場上。Azure 對 VHD 的領先 1MB 和結尾 512B 的變更是在 Azure 市場上分段及發佈映像時發生的。若要驗證 VHD 檔案的簽章、Azure 修改的 VHD 映像必須先從 Azure 市場匯出。

您需要的產品

您必須在系統上安裝必要的程式。

- Azure CLI 已安裝、或 Azure Cloud Shell 透過 Azure 入口網站隨時可供使用。



如需如何安裝 Azure CLI 的詳細資訊、請參閱 ["Azure 說明文件：如何安裝 Azure CLI"](#)。

步驟

1. 使用 version_readme.Me 檔案的內容、將 ONTAP 版本對應至 Azure 市場映像版本。

對於版本_讀我檔案中列出的每個版本對應、ONTAP 版本以「buildname」表示、Azure 市場映像版本以「version」表示。

例如、在下列版本_讀我檔案中、ONTAP 版本「9.15.0P1」對應至 Azure 市場映像版本「9150.01000024.05090105」。此 Azure 市場映像版本稍後會用於設定映像 URN。

```
[
  {
    "buildname": "9.15.0P1",
    "publisher": "netapp",
    "version": "9150.01000024.05090105"
  }
]
```

2. 識別您要建立 VM 的區域名稱。

設定市場映像的 URN 時、此區域名稱會用作「locName」變數的值。

- a. 若要接收可用區域的清單、請輸入 `az account list-locations -o table` 命令。

在下表中、區域名稱稱為「名稱」欄位。

```
$ az account list-locations -o table
DisplayName                                Name                                RegionalDisplayName
-----
East US                                    eastus                              (US) East US
East US 2                                  eastus2                             (US) East US 2
South Central US                          southcentralus                      (US) South Central US
...
```

3. 請從下表中檢閱對應 VM 部署類型的 SKU 名稱。

當設定市場映像的 URN 時、SKU 名稱會用作「skuName」變數的值。

例如、單一節點部署應使用「ONTAP 雲端 byol」SKU 名稱。

VM 部署類型	SKU 名稱
單一節點	ONTAP 雲端
高可用度	ONTAP 雲端 _ byol_ha

4. ONTAP 版本和 Azure 市場映像對應完成後、即可透過 Azure Cloud Shell 或 Azure CLI、從 Azure 市場匯出 VHD 檔案。

透過 **Azure** 入口網站上的 **Azure Cloud Shell** 匯出 **VHD** 檔案

1. 從 Azure Cloud Shell 將市場映像匯出至 vhd（image2、例如 9150.01000024.05090105.vhd）、然後下載至您的本機機器（例如 Linux 機器或 Windows PC）。

按一下以顯示

```
#Azure Cloud Shell on Azure portal to get VHD image from Azure
Marketplace
a) Set the URN and other parameters of the marketplace image. URN is
with format "<publisher>:<offer>:<sku>:<version>". Optionally, a
user can list NetApp marketplace images to confirm the proper image
version.
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName
$pubName -Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...

b) Create a new managed disk from the Marketplace image with the
matching image version
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnfl"
PS /home/user1> az disk create -g $diskRG -n $diskName --image
-reference $urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds
3600 --access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-
Json)[0].accessSas

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/'<copy>'.
PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext
```

```
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri
$diskAccessSAS -DestContainer $containerName -DestContext
$destContext -DestBlob $destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container
$containerName -Context $destContext -Blob $destBlobName
```

d) Download the generated image to your server, e.g., a Linux machine.

Use "wget <URL of file examplesaname/Containers/vm-images/9150.01000024.05090105.vhd>".

The URL is organized in a formatted way. For automation tasks, the following example could be used to derive the URL string. Otherwise, Azure CLI 'az' command could be issued to get the URL, which is not covered in this guide. URL Example:

```
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd
```

e) Clean up the managed disk

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG
-DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

從本機 Linux 機器透過 Azure CLI 匯出 VHD 檔案

1. 從本機 Linux 機器透過 Azure CLI 將市場映像匯出至 vhd。

按一下以顯示

```
#Azure CLI on local Linux machine to get VHD image from Azure
Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXX to
authenticate.

% az vm image list --all --publisher netapp --offer netapp-ontap-
cloud --sku ontap_cloud_byol
...
{
  "architecture": "x64",
  "offer": "netapp-ontap-cloud",
  "publisher": "netapp",
  "sku": "ontap_cloud_byol",
  "urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
  "version": "9150.01000024.05090105"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level
Read --name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

c) export vhd from managed disk

Create a container with proper access level. As an example, a container named 'vm-images' with 'Container' access level is used here.

Get storage account access key, on Azure portal, 'Storage Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/'<copy>'. There should be az command that can achieve the same, but this is not included in this guide.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName
```

```
{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

#to check the status of the blob copying

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName
```

```
....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  }
```

```

    },
    ....

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes

```

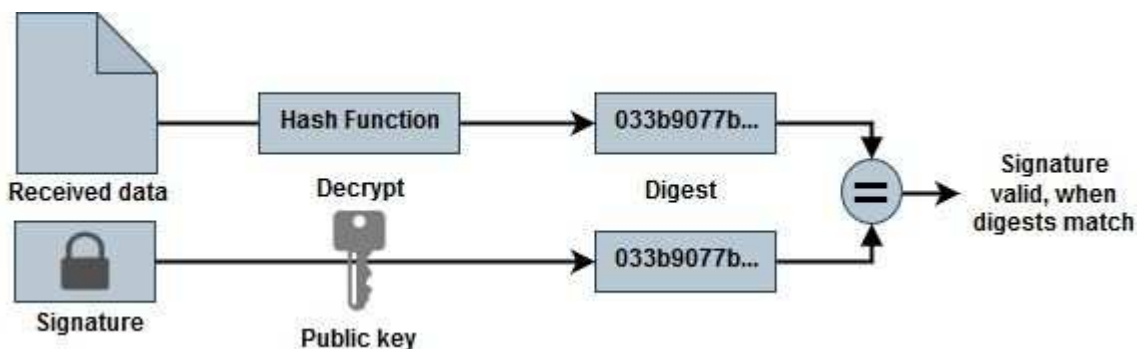
檔案簽章驗證

檔案簽章驗證

Azure 影像驗證程序將使用雜湊功能、從 VHD 檔案產生內含前導式 1MB 等量區塊的摘要、並結束 512B 等量區塊區塊。為了符合簽署程序、使用 SHA256 進行雜湊。您需要從 VHD 檔案移除前導式 1MB 和最終版 512B、然後驗證 VHD 檔案的其餘部分。

檔案簽章驗證工作流程摘要

以下是檔案簽章驗證工作流程程序的概觀。



- 從下載 Azure Image Digest 檔案 "[NetApp 支援網站](#)" 然後擷取摘要檔案 (.SIG)、公開金鑰憑證檔案 (.pem) 和鏈結憑證檔案 (.pem)。

請參閱 "[下載 Azure Image Digest File](#)" 以取得更多資訊。

- 驗證信任鏈結。
- 從公開金鑰憑證（.pem）擷取公開金鑰（.pub）。
- 解壓縮的公開金鑰用於解密摘要檔案。然後將結果與從映像檔案建立的新未加密暫存檔案摘要進行比較、並移除前導式 1MB 與結尾 512 位元組的檔案。

此步驟可透過下列 openssl 命令來達成。

- 一般 CLI 聲明如下所示：

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

- 如果檔案相符、則 Openssl CLI 工具會顯示「驗證成功」訊息、如果檔案不符、則會顯示「驗證失敗」訊息。

Linux 上的檔案簽章驗證

您可以依照下列步驟驗證匯出的 VHD 檔案簽章適用於 Linux。

步驟

1. 從下載 Azure Image Digest 檔案 "[NetApp 支援網站](#)" 然後擷取摘要檔案（.SIG）、公開金鑰憑證檔案（.pem）和鏈結憑證檔案（.pem）。

請參閱 "[下載 Azure Image Digest File](#)" 以取得更多資訊。

2. 驗證信任鏈結。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 移除前導的 1MB（1048576 位元組）、並結束 512 位元組的 VHD 檔案。

如果使用「tail」、選項「-c +K」會以指定檔案的 KTH 位元組開始輸出位元組。因此、1048577 會傳送至 'tail -c」。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 openssl 從憑證擷取公開金鑰、並使用簽章檔案和公開金鑰驗證等量分佈的檔案（sign.tmp）。

如果輸入檔通過驗證、則會顯示命令
"驗證正常"。否則將顯示「驗證失敗」。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Mac OS 上的檔案簽章驗證

您可以依照下列步驟、驗證 Mac OS 匯出的 VHD 檔案簽章。

步驟

1. 從下載 Azure Image Digest 檔案 "[NetApp 支援網站](#)" 然後擷取摘要檔案 (.SIG)、公開金鑰憑證檔案 (.pem) 和鏈結憑證檔案 (.pem)。

請參閱 "[下載 Azure Image Digest File](#)" 以取得更多資訊。

2. 驗證信任鏈結。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 移除前導的 1MB (1048576 位元組)、並結束 512 位元組的 VHD 檔案。

如果使用「tail」、選項「-c +K」會以 KTH 位元組開始輸出位元組指定檔案的。因此、1048577 會傳送至 'tail -c」。大約需要 13 分鐘以在 Mac OS 上完成 tail 命令。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 openssl 從憑證擷取公開金鑰、並驗證等量分割檔案（sign.tmp）、含簽章檔案和公開金鑰。

如果輸入檔案通過驗證、命令會顯示「驗證正常」。
否則將顯示「驗證失敗」。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

何處可以找到 **Azure** 影像驗證的其他資訊

如需 Azure 影像驗證的其他資訊、請參閱下列連結。以下連結將帶您前往非 NetApp 網站。

參考資料

- ["網頁故障部落格：如何使用 OpenSSL 簽署及驗證"](#)
- ["使用 Azure Marketplace 映像為 Azure Stack Edge Pro GPU 建立 VM 映像 | Microsoft Learn"](#)
- ["使用 Azure CLI 將託管磁碟匯出 / 複製到儲存帳戶 | Microsoft Learn"](#)
- ["Azure Cloud Shell Quickstart - Bash | Microsoft Learn"](#)
- ["如何安裝 Azure CLI | Microsoft Learn"](#)
- ["AZ 儲存資源膨脹複本 | Microsoft Learn"](#)
- ["使用 Azure CLI 登入：登入與驗證 | Microsoft Learn"](#)

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。