Azure平台映像验证

Cloud Volumes ONTAP

NetApp
June 27, 2024

目录

Azure平台映像验证

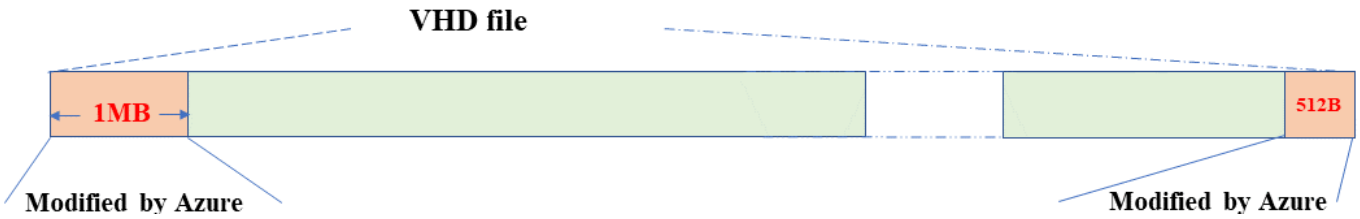
Azure映像验证概述

Azure映像验证符合增强的NetApp安全要求。虽然验证映像文件是一个简单的过程、但Azure映像签名验证确实需要对众所周知的Azure HD映像文件进行特殊处理、因为Azure Marketplace会进行更改。

Cloud Volumes ONTAP软件9.12.09或更高版本支持Azure映像验证。

Azure对已发布的VHD文件的更改

Azure会修改前1 MB (1048576字节)和后512字节的vHD文件。NetApp映像签名会跳过前导1 MB和结尾512字节、并对剩余的HD映像部分进行签名。



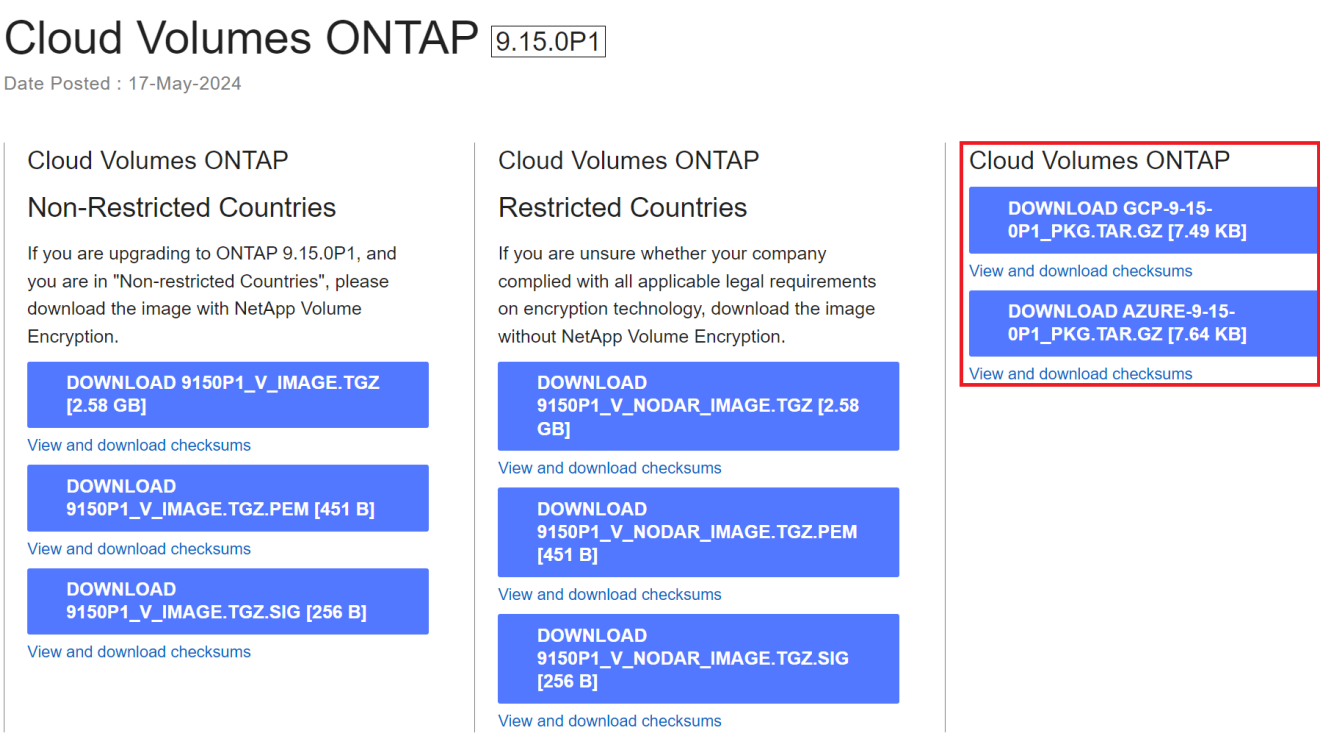
例如、上图显示了一个大小为10 GB的vHD文件。但是、NetApp签名部分会标记为绿色、大小为10 GB - 1 MB - 512 B。

下载Azure映像摘要文件

Azure映像摘要文件可从下载 "NetApp 支持站点"。下载文件为tar.gz格式、其中包含用于图像签名验证的文件。

步骤

1. 转至 "NetApp 支持站点 上的Cloud Volumes ONTAP产品页面" 并在"Downloads"(下载)部分下下载所需的软件版本。
2. 在Cloud Volumes ONTAP下载页面下，单击Azure映像摘要文件的*下载按钮*以下载第三次评估报告。 Gz文件。



3. 对于Linux和MacOS、您必须执行以下操作才能为下载的Azure Image Digest文件获取md5sum和手机256sum。
   a. 对于md5sum、输入 `md5sum` 命令：
   b. 对于"数额 为256SUM"的、输入 `sha256sum` 命令：
4. 验证 `md5sum` 和 `sha256sum` 值与Azure Image Digest File下载匹配。
5. 在Linux和Mac OS上、执行 `tar -xzf` 命令以提取tar.gz文件。

   提取的第三次评估报告。 GZ文件包含摘要文件(.sig)、公共密钥证书文件(.prom)和链证书文件(.prom)。

   列出**untar tar.gz**文件的结果

```
$ 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
```

从Azure Marketplace导出映像

将该vHD映像发布到Azure云后、NetApp将不再管理该映像。而是将发布的映像放置在Azure Marketplace上。在Azure Marketplace上暂存并发布映像时、Azure会更改到VHD的前导1 MB和结尾512 B。要验证该VHD文件的签名、需要首先从Azure Marketplace导出

由Azure修改的VHD映像。

您需要的内容

您必须在系统上安装所需的程序。

- 已安装Azure命令行界面、或者可随时通过Azure门户使用Azure Cloud Shell。

  有关如何安装Azure命令行界面的详细信息、请参见 "Azure文档：如何安装Azure命令行界面"。

步骤

1. 使用version_readme文件的内容将ONTAP版本映射到Azure Marketplace映像版本。

   对于version_readme文件中列出的每个版本映射、ONTAP版本以"budname"表示、Azure Marketplace映像版本以"version"表示。

   例如、在以下version_readme文件中、ONTAP版本"9.15.0P1"映射到Azure Marketplace映像版本"9150.01000024.65090105"。此Azure Marketplace映像版本稍后用于设置映像URN。

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

2. 确定要创建VM的区域名称。

   在设置商城图片的URN时、此区域名称用作"locName"变量的值。

   a. 要接收可用区域的列表、请输入 `az account list-locations -o table` 命令：

      在下表中、区域名称称为"名称"字段。

   ```
   $ 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. 查看下表中相应虚拟机部署类型的SKU名称。

在设置商城图片的URN时、SKU名称将用作"skuName"变量的值。

例如、单节点部署应使用"ONTAP _Cloud BYOL" SKU名称。

虚拟机部署类型	**SKU**名称
单个节点	ONTAP云BYOL
高可用性	ONTAP云BYOL_ha

4. 映射ONTAP版本和Azure Marketplace映像后、通过Azure Cloud Shell或Azure命令行界面从Azure Marketplace导出VHD文件。

通过**Azure**门户上的**Azure Cloud Shell**导出**VHD**文件

1. 从Azure Cloud Shell中、将市场映像导出到vhd (image2、例如9150.01000024.65090105.vhd)、然后下载到本地计算机(例如Linux计算机或Windows PC)。

单击以显示

```
#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 = “fnf1”
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
```

通过**Azure**命令行界面从本地**Linux**计算机导出**VHD**文件

1. 从本地Linux计算机通过Azure命令行界面将市场映像导出到vhd。

单击以显示

```
#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-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
#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="xxxxxxxxxx"
% 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": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "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-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
```

```
    },
....

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
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

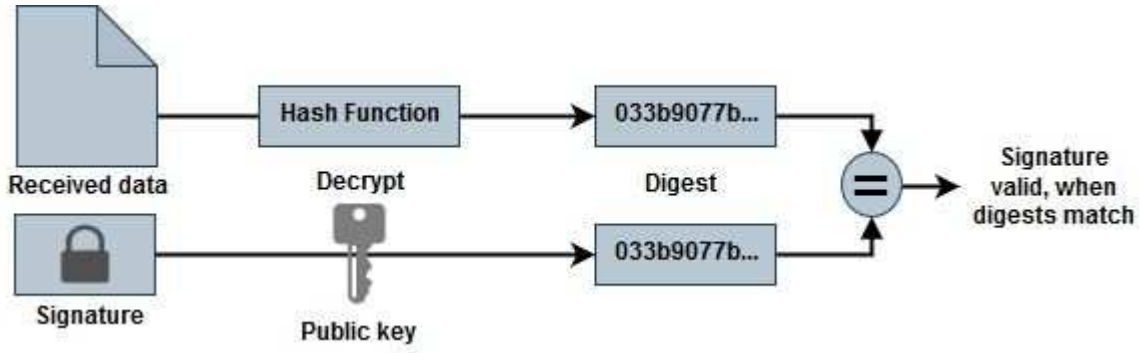
文件签名验证

文件签名验证

Azure映像验证过程将使用哈希函数从具有前导1 MB和末尾512 B条带化的vHD文件生成摘要。为了匹配签名操作步骤、使用SHA256进行哈希。您需要从该视频文件中删除前导1 MB和最终512 B、然后验证视频文件的其余部分。

文件签名验证工作流摘要

下面简要介绍了文件签名验证工作流过程。



- 从下载Azure Image Digest文件 "NetApp 支持站点" 并提取摘要文件(.sig)、公共密钥证书文件(.pem)和链证书文件(.pem)。

  请参见 "下载Azure映像摘要文件" 有关详细信息 …

- 验证信任链。
- 从公共密钥证书(.prom)提取公共密钥(.pub)。
- 提取的公共密钥用于对摘要文件进行解密。然后、将结果与从映像文件创建的临时文件的新未加密摘要进行比较、该文件删除了前导1 MB和结束512字节。

  此步骤可通过以下openssl命令来实现。

  - 常规CLI语句如下所示：

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

  - 如果两个文件都匹配、OpenSSL命令行界面工具会显示"Verified Ok"消息、如果不匹配、则会显示"Verification Failure"消息。

Linux上的文件签名验证

您可以按照以下步骤验证已导出的Linux的VHD文件签名。

步骤

1. 从下载Azure Image Digest文件 "NetApp 支持站点" 并提取摘要文件(.sig)、公共密钥证书文件(.pem)和链证书文件(.pem)。

   请参见 "下载Azure映像摘要文件" 有关详细信息 …

2. 验证信任链。

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

3. 删除前1 MB (1048576字节)和后512字节的vHD文件。

   如果使用"tail"、则选项"-c +K"将输出以指定文件的K有权 字节开头的字节。因此、1048交由"尾部-c"处理。

   ```
   % 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从证书中提取公共密钥、并使用签名文件和公共密钥验证条带化文件(ssign.tmp)。

   如果输入文件通过验证、则会显示命令
   "验证正常"。否则、将显示"Verification Failure"(验证失败)。

```
% 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. 清理工作空间。

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

Mac OS上的文件签名验证

您可以按照以下步骤验证已导出的Mac OS的vHD文件签名。

步骤

1. 从下载Azure Image Digest文件 "NetApp 支持站点" 并提取摘要文件(.sig)、公共密钥证书文件(.pem)和链证书文件(.pem)。

   请参见 "下载Azure映像摘要文件" 有关详细信息 …

2. 验证信任链。

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

3. 删除前1 MB (1048576字节)和后512字节的vHD文件。

   如果使用"tail"、则选项"-c +K"输出以K有权 字节开头的字节
   指定文件的。因此、1048交由"尾部-c"处理。大约需要13米
   以便在Mac OS上完成尾部命令。

```
% 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opensl从证书中提取公共密钥并验证条带化
带有签名文件和公共密钥的file(sign.tmp)。

   如果输入文件通过验证、则该命令将显示"Verification Ok"(验证正常)。
   否则、将显示"Verification Failure"(验证失败)。

```
% 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. 清理工作空间。

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

从何处查找有关Azure映像验证的追加信息

查看以下链接、了解有关Azure映像验证的追加信息。通过以下链接可访问非NetApp站点。

参考资料

- "页面错误博客：如何使用OpenSSL进行签名和验证"
- "使用Azure Marketplace映像为Azure Stack Edge Pro GPU创建VM映像| Microsoft了解"
- "使用Azure命令行界面将受管磁盘导出/复制到存储帐户| Microsoft了解"
- "Azure Cloud Shell快速入门—闪存| Microsoft了解"
- "如何安装Azure命令行界面| Microsoft了解"
- "AZ存储Blob副本| Microsoft了解"
- "使用Azure命令行界面登录—登录和身份验证| Microsoft学习"