



Introduction to Windows Server 2016 Shielded VMs

Introduces the new Shield Virtual Machines feature of Windows Server 2016

Provides instructions on how to deploy Guarded Hosts and Shielded VMs

Explains how to create a new Shielded VM on-premises and move it to a Guarded Fabric

Helps IT Specialists understand the new features of Windows Server 2016

Boyong Li



Abstract

This document provides step-by-step instructions on how to deploy Shielded Virtual Machines (VMs) and Guarded Fabric on Lenovo® servers running Windows Server 2016 Datacenter Edition. This document is intended for IT specialists and IT managers needing to understand more about the new features of Windows Server 2016. This paper is based on Windows Server 2016 Technical Preview 5 (TP5).

This paper is part of a series of technical papers on the new features of Windows Server 2016. For other papers in the series, see the following link:

<https://lenovopress.com/?term=ws2016>

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

<http://lenovopress.com>

Do you have the latest version? We update our papers from time to time, so check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you're there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction	3
Deploying a guarded fabric	4
Creating a new Shielded VM on-premises and moving it to a guarded fabric	21
Summary	32
Change history	32
Authors	32
Notices	33
Trademarks	34

Introduction

Virtualization security is a major investment area in Windows Server 2016 Hyper-V. In addition to protecting hosts or other VMs from a VM running malicious software, VMs also need to be protected from a compromised host. In a public cloud environment, this also means protection from a rogue administrator. Because a VM is effectively just a file stored on disk, it needs to be protected from unauthorized access via the storage system, the network, and while it is being backed up.

Data protection is a fundamental need for every virtualization platform today, whether it's Hyper-V, ESXi, or any other virtualization engine. If a VM file can be copied or moved offsite (either maliciously or accidentally) that VM can be run on any other system. Protecting high value assets in your organization, such as domain controllers, sensitive file servers, and HR systems is a top priority.

To help protect against compromised fabric, Windows Server 2016 Hyper-V introduces Shielded VMs. A *Shielded VM* is a Generation 2 feature (supported on Windows Server 2012 and later) that comes with a virtual Trusted Platform Module (TPM), is encrypted using BitLocker, and can only run on healthy and approved hosts in the fabric.

Shielded VMs and guarded fabric enables cloud service providers or enterprise private cloud administrators to provide a more secure environment for tenant VMs.

A guarded fabric is composed of

- ▶ Host Guardian Service (HGS), typically running on a cluster of 3 nodes
- ▶ One or more guarded hosts
- ▶ A set of Shielded VMs.

Figure 1 shows how the Host Guardian Service uses *attestation* to ensure that only known, valid hosts can start the Shielded VMs, and the Key Protection Service to securely release the keys for Shielded VMs.

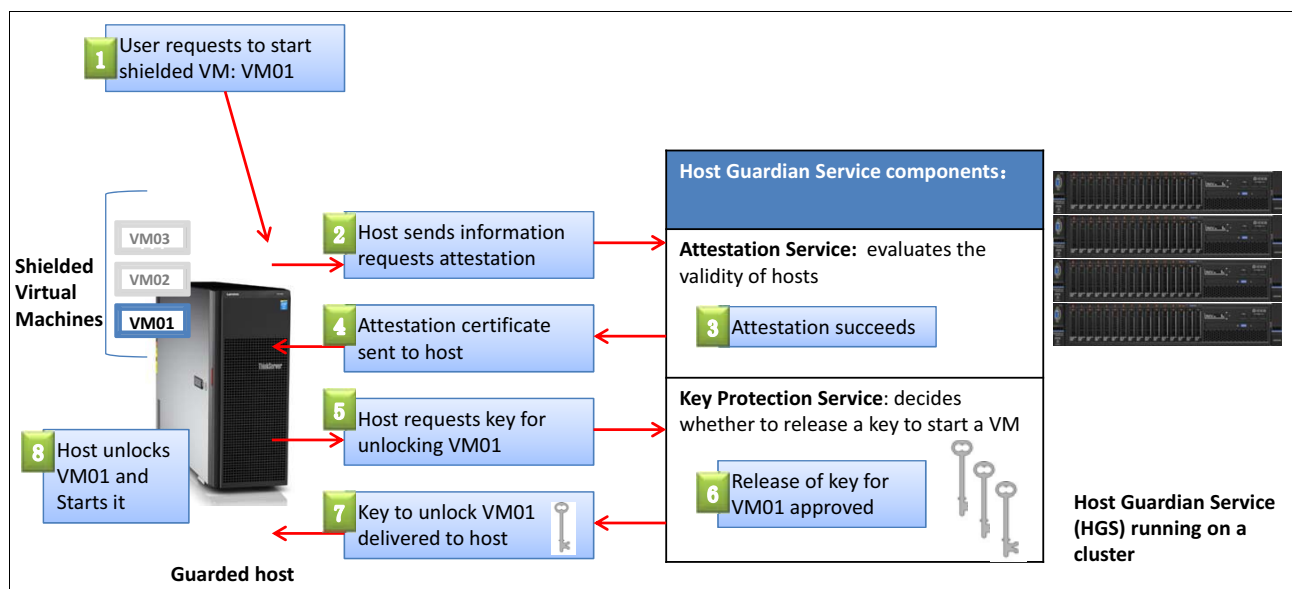


Figure 1 Verification process of Shielded VM

There are many possible attack vectors that Shielded VMs can protect against. Table 1 on page 4 shows a few examples, along with how Shielded VMs protect against each attack:

Table 1 Examples of attacks that Shielded VMs can defend against

Attack vector	Shielded VM defense
A malicious admin stealing VHDs	Shielded VMs' VHDs are encrypted.
Attaching a debugger to the Hyper-V host	HGS will not release keys to hosts with debuggers attached—this is something we measure in HGS.
Injecting malware on a Hyper-V host	All software (kernel mode, user mode and drivers) running on a host is measured.
Injecting malware into a VM template disk	Shielded VMs are only deployed from template disks that match known healthy ones.
A malicious admin attempting to move a Shielded VM to an untrusted host	Trusted hosts are added to HGS using an identifier unique to their TPM; the new host will not be recognized because it is not added.

This document provides guidance for deploying a guarded fabric, that is, the Host Guardian Service (HGS) plus guarded hosts, on which Shielded VMs can run. Additionally, this document introduces how to create a new Shielded VM on-premises and move it to a guarded fabric.

Deploying a guarded fabric

When you first deploy a guarded fabric, you must decide which type of attestation to use. Hyper-V hosts that want to run Shielded VMs must attest with their HGS before they can start a Shielded VM.

There are two methods of attestation that you can use for a guarded fabric:

- ▶ **Admin-trusted attestation mode:** Easier to deploy, but provides lesser assurances
- ▶ **TPM-trusted attestation mode:** Has hardware and firmware requirements (TPM 2.0 and UEFI 2.3.1, with secure boot enabled) and involves more configuration steps, but provides substantially stronger assurances.

Table 2 describes the level of assurance offered by the two modes of attestation.

Table 2 Attestation modes

Attestation mode you choose for hosts	Host assurances
Admin-trusted attestation <ul style="list-style-type: none"> ▶ Requires relatively few configuration steps ▶ Compatible with commonplace server hardware 	Only hosts that you have designated as guarded hosts can decrypt and start Shielded VMs. You designate hosts as guarded by placing them in a security group that you create in Active Directory Domain Services (AD DS). A trust relationship must be established between the fabric AD and the Host Guardian Service's forest.
TPM-trusted attestation <ul style="list-style-type: none"> ▶ Requires more configuration steps ▶ Host hardware and firmware must include TPM 2.0 and UEFI 2.3.1 with secure boot enabled ▶ Offers the strongest possible protections 	Only hosts that you have designated as guarded hosts, and that are running code that you have identified as trusted, can start Shielded VMs. The technologies that ensure that the hosts are running trusted code are built into the Windows Server operating system, and include secure measured boot and Code Integrity policies.

In this document, we provide configuration instructions with TPM-trusted attestation mode used as an example. Overall steps are as follows:

1. "Requirements"
2. "Configuring the first HGS node"
3. "Configuring the Fabric DNS" on page 8
4. "Configuring the Guarded Host" on page 14
5. "Verifying that HGS is configured properly" on page 17
6. "Configuring secondary HGS nodes" on page 18
7. "Confirming that hosts can attest successfully" on page 20

Requirements

The Host Guardian Service (HGS) node and Guarded Hyper-V host must be configured as below:

- ▶ Secure Boot: Enabled
- ▶ Secure Boot mode: User Mode
- ▶ TPM 2.0 support: Enabled
- ▶ VT-D: Enabled

Operating system checkup:

- ▶ Windows Server 2016 Technical Preview 5 Datacenter edition
- ▶ Run **TPM.msc** and you should see The TPM is ready for use shown in the Status section of the displayed window and the version should be 2.0, as shown in Figure 2.

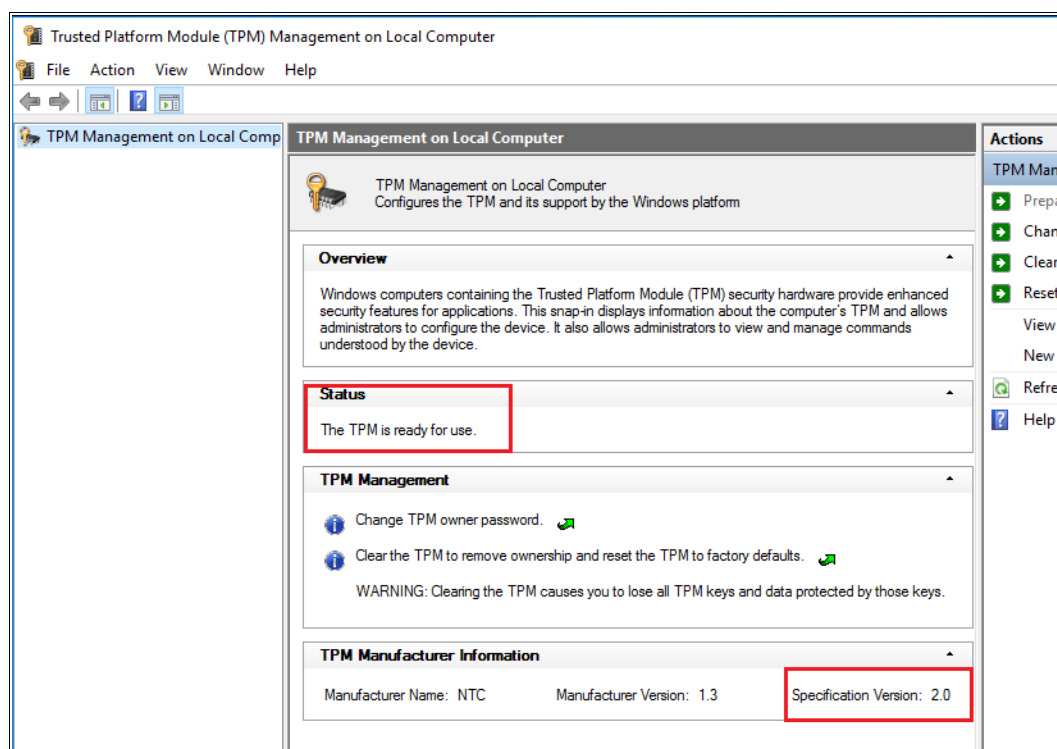


Figure 2 Checking the status of the Trusted Platform Module (TPM)

Configuring the first HGS node

This section describes configuring the first Host Guardian Service node. The steps are:

1. “Adding the HGS Role”
2. “Installing the Host Guardian Service” on page 6
3. “Creating self-signed certificates for HGS” on page 7
4. “Initializing the HGS server for TPM-trusted attestation” on page 8

Adding the HGS Role

Follows these steps:

1. Add the Host Guardian Service role to the machine in Server Manager or by running the following command in an elevated Windows PowerShell console:

```
Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
```

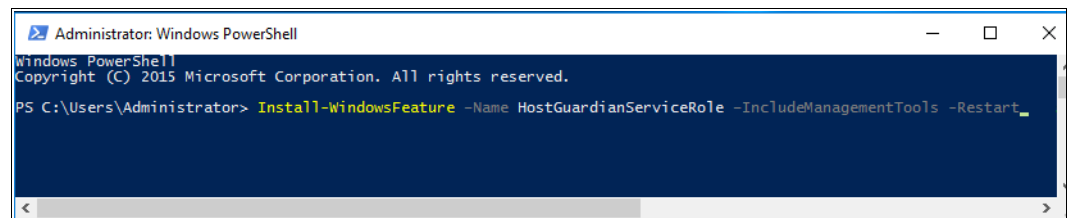


Figure 3 *Install-WindowsFeature command*

2. You will see the following progress window.

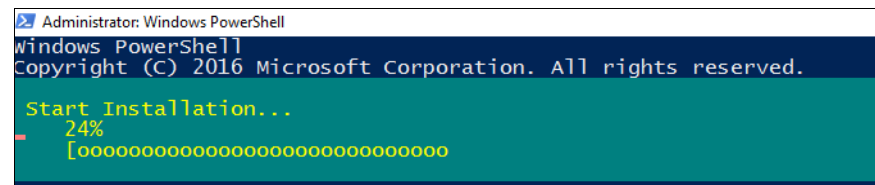


Figure 4 *Output*

3. When the installation finishes the system will restart.

Installing the Host Guardian Service

Follows these steps:

1. In an elevated Windows PowerShell console, run the following command (Figure 5) to install the Host Guardian Service and configure its domain:

```
$adminPassword = ConvertTo-SecureString -AsPlainText '<password>' -Force
```

```
Install-HgsServer -HgsDomainName 'relecloud.com' -SafeModeAdministratorPassword $adminPassword -Restart
```

Substitute relecloud.com for the name of your HGS domain if necessary.

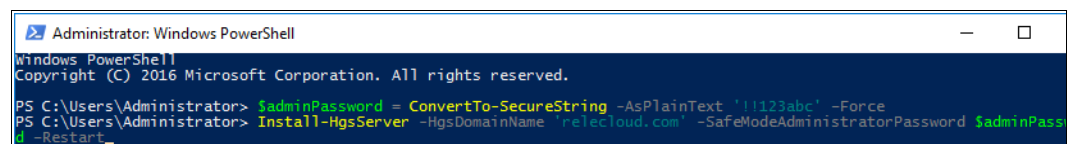


Figure 5 *Install-HgsServer command*

2. You will see the following progress window, Figure 6. The server will restart automatically upon completion.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

Installing Host Guardian Service
Installing Active Directory domain controller.
[ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
Install-ADDSForest

Validating environment and user input
All tests completed successfully
[ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
Installing new forest
Starting
  
```

Figure 6 *Install-HgsServer output*

3. After the computer restarts, log in as the domain administrator using the same password you previously used as the local administrator (regardless of the password you specified in the previous step).

Creating self-signed certificates for HGS

Follows these steps:

1. Open an elevated Windows PowerShell console and run the following command to specify the password to use when exporting the self-signed certificate:
`$certificatePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force`
 For <password>, replace it with the real password.
2. Create and export the signing certificate by running the following commands:
`$signingCert = New-SelfSignedCertificate -DnsName "signing.relecloud.com"`
`Export-PfxCertificate -Cert $signingCert -Password $certificatePassword -FilePath 'C:\signingCert.pfx'`

For signing (after -DnsName) and for C:\signingCert, you can leave the names as shown or replace them with your preferred names. The commands and output are shown in Figure 7 on page 7.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $certificatePassword = ConvertTo-SecureString -AsPlainText '11123abc' -Force
PS C:\Users\Administrator> $signingCert = New-SelfSignedCertificate -DnsName "signing.relecloud.com"
PS C:\Users\Administrator> Export-PfxCertificate -Cert $signingCert -Password $certificatePassword -FilePath 'C:\signingCert.pfx'

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
-a----          5/16/2016   5:17 PM           2647 signingCert.pfx

PS C:\Users\Administrator>
  
```

Figure 7 *Export-PfxCertificate command*

3. Create and export the encryption certificate by running the following commands:
`$encryptionCert = New-SelfSignedCertificate -DnsName "encryption.relecloud.com"`
`Export-PfxCertificate -Cert $encryptionCert -Password $certificatePassword -FilePath 'C:\encryptionCert.pfx'`

For encryption (after -DnsName) and for C:\encryptionCert, you can leave the names as shown or replace them with your preferred names. The commands and output are shown in Figure 8.

```

Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $certificatePassword = ConvertTo-SecureString -AsPlainText '11123abc' -Force
PS C:\Users\Administrator> $signingCert = New-SelfSignedCertificate -DnsName 'signing.relecloud.com'
PS C:\Users\Administrator> Export-PfxCertificate -Cert $signingCert -Password $certificatePassword -FilePath 'C:\signingCert.pfx'

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
-a-----         5/16/2016   5:17 PM           2647 signingCert.pfx

PS C:\Users\Administrator> $encryptionCert = New-SelfSignedCertificate -DnsName 'encryption.relecloud.com'
PS C:\Users\Administrator> Export-PfxCertificate -Cert $encryptionCert -Password $certificatePassword -FilePath 'C:\encryptionCert.pfx'

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
-a-----         5/16/2016   5:31 PM           2656 encryptionCert.pfx

PS C:\Users\Administrator>

```

Figure 8 Export-PfxCertificate command

4. Restart the HGS server.

Initializing the HGS server for TPM-trusted attestation

Follows these steps:

1. Open an elevated Windows PowerShell console and run the following command to initialize the HGS server in TPM-trusted mode with the encryption and signing certificates created previously:

```
$certificatePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force
```

```
Initialize-HGSServer -HgsServiceName '<HgsServiceName>' -SigningCertificatePath
'C:\signingCert.pfx' -SigningCertificatePassword $certificatePassword
-EncryptionCertificatePath 'C:\encryptionCert.pfx'
-EncryptionCertificatePassword $certificatePassword -TrustTPM -Confirm:$false
```

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $certificatePassword = ConvertTo-SecureString -AsPlainText '11123abc' -Force
PS C:\Users\Administrator> Initialize-HGSServer -HgsServiceName 'TpmHgs' -SigningCertificatePath 'C:\signingCert.pfx' -S
igningCertificatePassword $certificatePassword -EncryptionCertificatePath 'C:\encryptionCert.pfx' -EncryptionCertificate
Password $certificatePassword -TrustTPM -Confirm:$false
LogPath: C:\Windows\Logs\HgsServer\160527145250\HGS01
PS C:\Users\Administrator>

```

Figure 9 Initialize-HGSServer command

Configuring the Fabric DNS

Before Guarded Hosts can resolve the HGS server names, a DNS forwarder from the fabric domain to the HGS domain must be set up. There are several ways to configure name resolution on the fabric domain. One way is to set up a conditional forwarder zone in the fabric DNS manager, as we describe in this section.

The servers and IP addresses we used in our setup are listed in Table 3.

Note: Do all setup on a fabric DNS server, not the HGS server that you just configured.

Table 3 Fabric configuration of the HGS server, DNS server and Hyper-V hosts

FQDN	IP Address	Purpose	Initial Configuration
hgs01.relecloud.com	192.168.11.101	First HGS node	Windows Server 2016 TP5 Datacenter Edition
hgs02.relecloud.com	192.168.11.102	Second HGS node	Windows Server 2016 TP5 Datacenter Edition
hgs03.relecloud.com	192.168.11.103	Third HGS node	Windows Server 2016 TP5 Datacenter Edition
DNS-S1.fabrikam.com	192.168.11.1	DNS Server	Windows Server 2016 TP5 Datacenter Edition AD DC (configured) DNS (configured) DHCP (configured)
Hghost01.fabrikam.com	192.168.11.11	Guarded Host node	Windows Server 2016 TP5 Datacenter Edition
Hghost02.fabrikam.com	192.168.11.12	Guarded Host node	Windows server 2016 TP5 Datacenter Edition

These roles need to be added to the DNS server as shown in Figure 10 on page 9.

- ▶ Active Directory Domain Services
- ▶ DHCP Server
- ▶ DNS Server

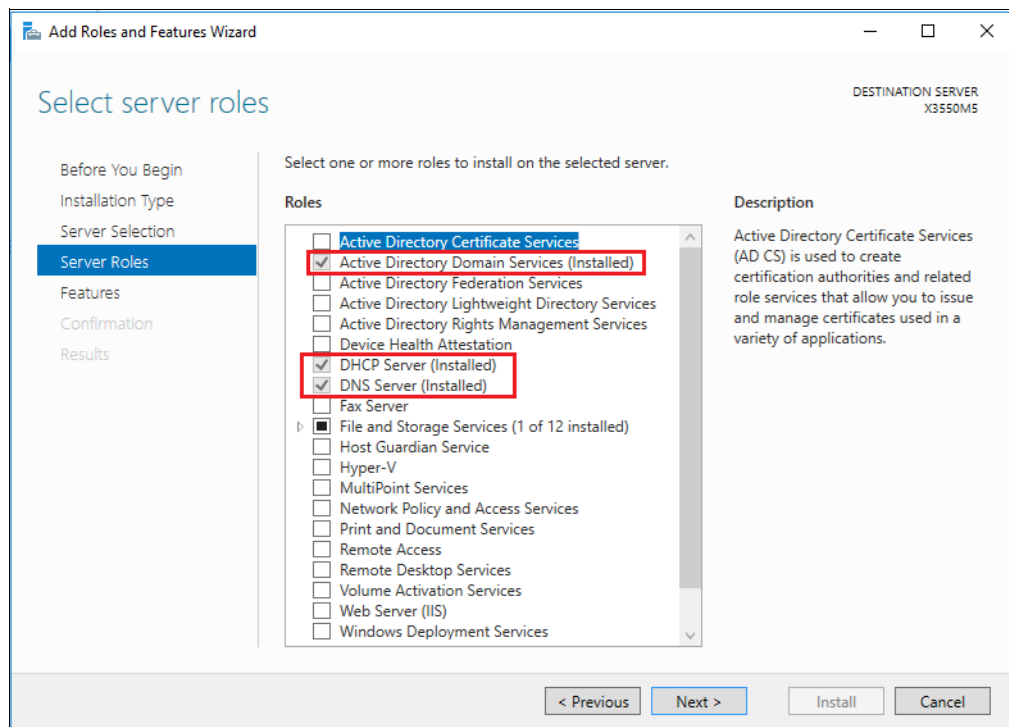


Figure 10 Select server roles

Configure Active Directory Domain Services in the Configuration Wizard as follows:

1. Select **Add a new forest** and enter **fabrikam.com** in the Root domain name field as shown in Figure 11, and then click **Next**.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the Windows logo, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls. The main window has a title bar with 'Deployment Configuration' and a 'TARGET SERVER X3550M5' label. On the left is a navigation pane with links: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this is a section titled 'Specify the domain information for this operation' with a text box labeled 'Root domain name:' containing the text 'fabrikam.com'. At the bottom right of the main area is a link 'More about deployment configurations'. The bottom of the window has a grey bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Figure 11 AD Domain Services wizard - Deployment Configuration

2. Enter the password and confirm it, as shown in Figure 12 and then click **Next**.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the Windows logo, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls. The main window has a title bar with 'Domain Controller Options' and a 'TARGET SERVER X3550M5' label. On the left is a navigation pane with links: 'Deployment Configuration', 'Domain Controller Options' (selected), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select functional level of the new forest and root domain' and contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server Technical Preview'. Below this is a section titled 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Below this is a section titled 'Type the Directory Services Restore Mode (DSRM) password' with two text boxes: 'Password:' and 'Confirm password:', both containing masked characters. At the bottom right of the main area is a link 'More about domain controller options'. The bottom of the window has a grey bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Figure 12 AD Domain Services wizard - Domain Controller options

3. In the DNS Options page, Figure 13, leave the click Next to move on.

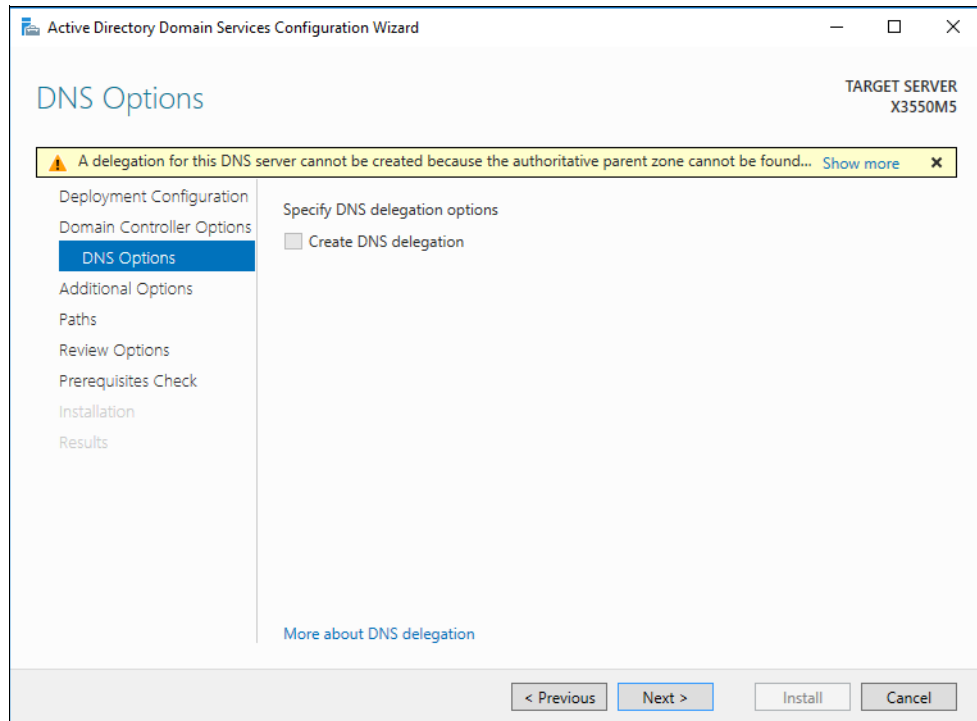


Figure 13 AD Domain Services wizard - DNS Options

4. The system now verifies the NetBIOS domain name and automatically fills it in as shown in Figure 14. Once it displays, click **Next**.

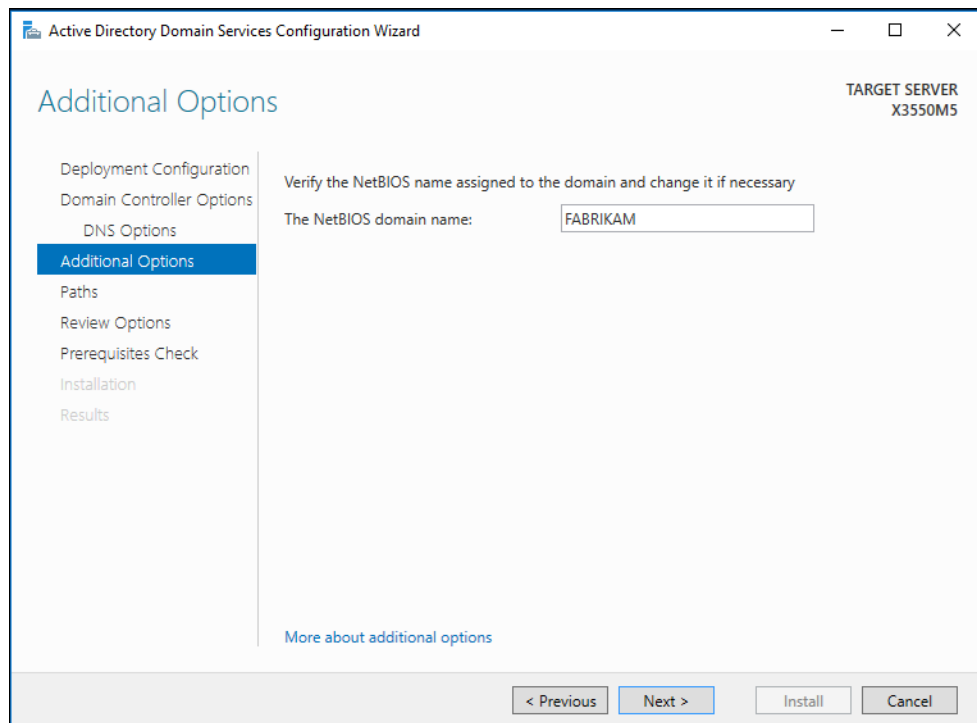


Figure 14 AD Domain Services wizard - Additional Options

5. On the Paths page, Figure 15, click **Next** to continue.

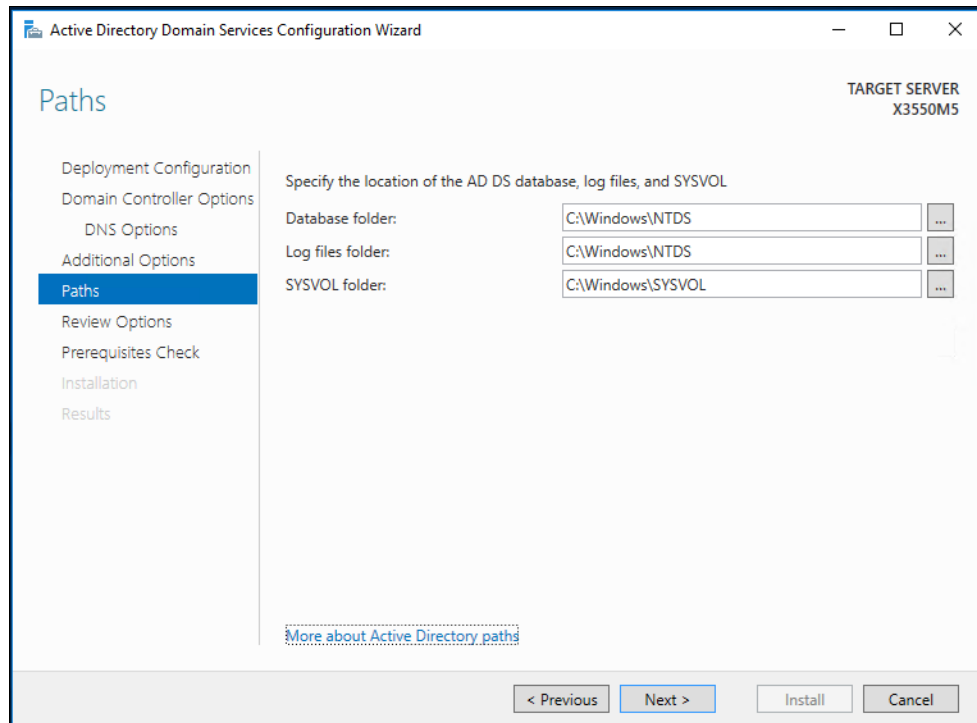


Figure 15 AD Domain Services wizard - Paths

6. On the Review Options page, Figure 16, click **Next**.

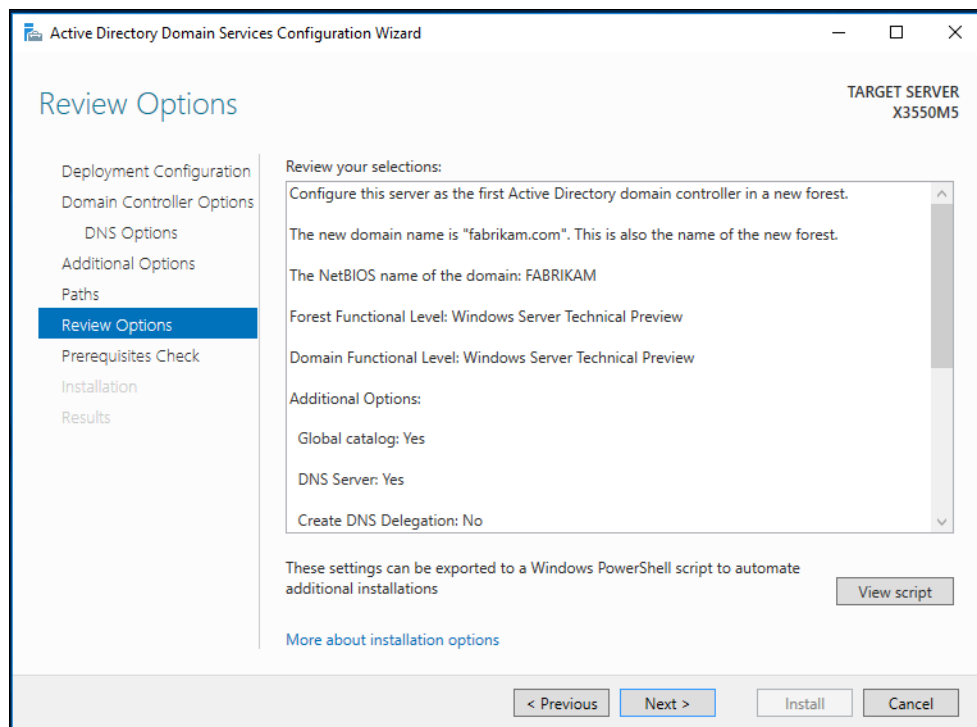


Figure 16 AD Domain Services wizard - Review Options

7. On the Prerequisites Check page, Figure 17, click **Install**.

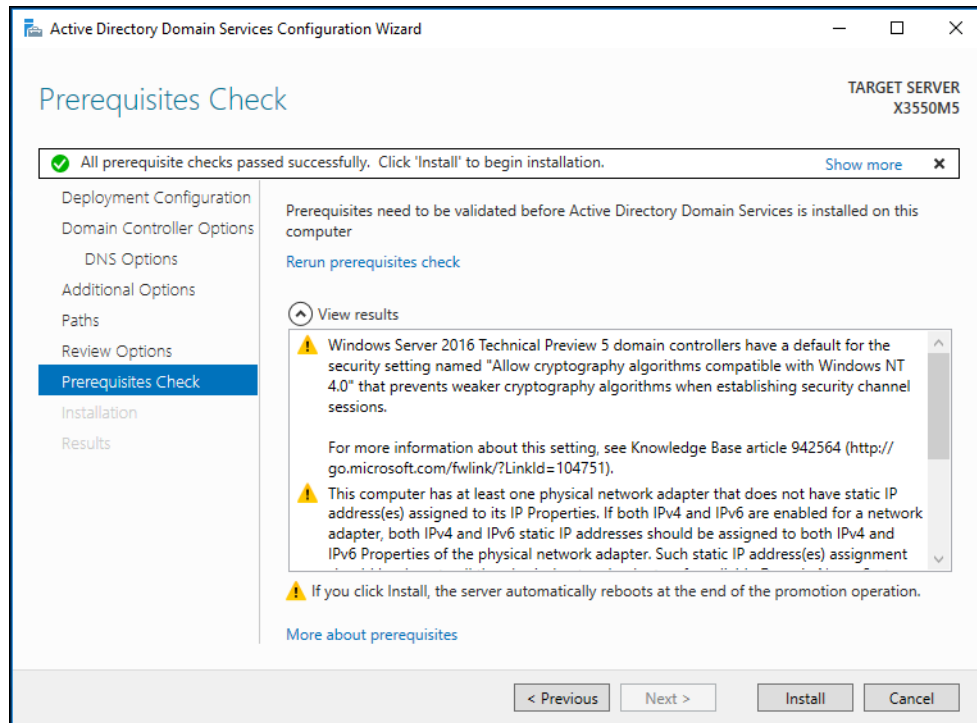


Figure 17 AD Domain Services wizard - Prerequisites Check

8. The installation proceeds, as shown in Figure 18 on page 13.

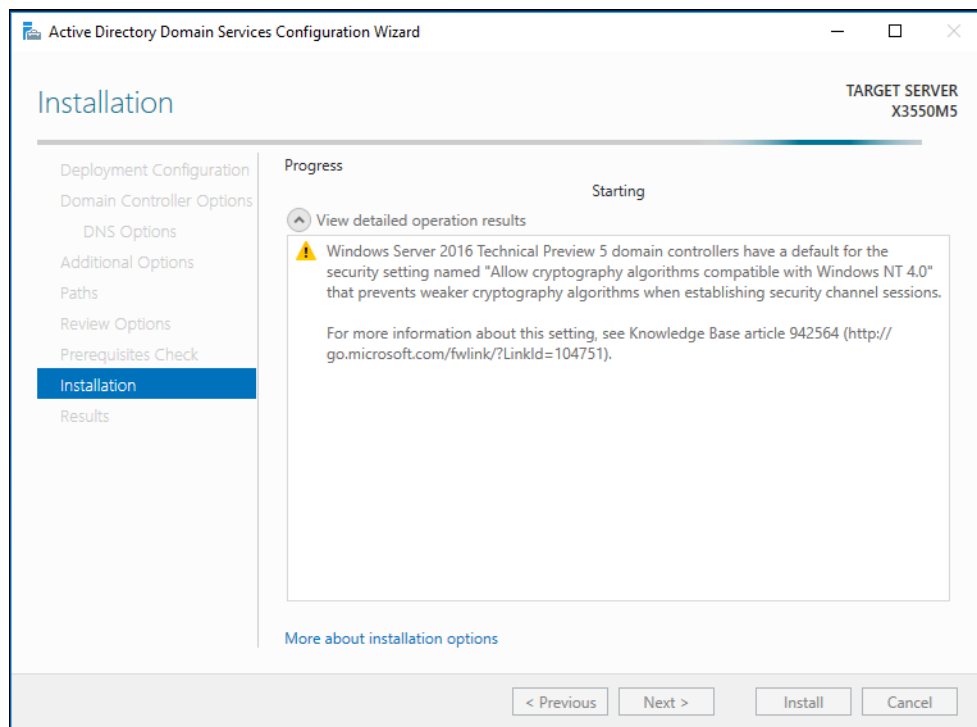


Figure 18 AD Domain Services wizard - Installation

9. Once installation is complete, the server will restart automatically.

10. To set up a conditional forwarder zone in the fabric DNS manager, run the following command in an elevated Windows PowerShell console on a fabric DNS server, as shown in Figure 19:

`Add-DnsServerConditionalForwarderZone -Name 'relecloud.com' -ReplicationScope "Forest" -MasterServers <IP addresses of HGS server>`

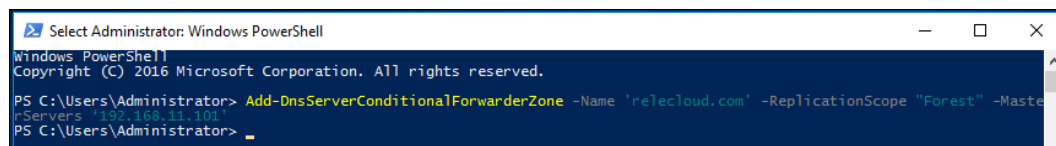


Figure 19 `Add-DnsServerConditionalForwarderZone` command

11. Reboot the server once the command completes.
12. After the system restarts, you should be able to find the relecloud.com item in DNS Manager on the DNS Server, as shown in Figure 20.

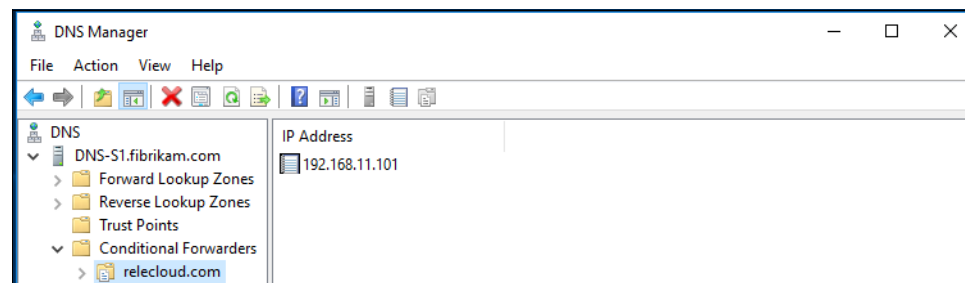


Figure 20 `relecloud.com` entry in the DNS Manager

Configuring the Guarded Host

The steps to configure the Guarded Host are as follows:

1. "Capture the TPM identifier"
2. "Create and apply a code integrity policy" on page 15
3. "Capture the TPM baseline for each unique class of hardware" on page 17

Capture the TPM identifier

To capture the TPM identifier (platform identifier or EKpub) for each host, do the following:

1. Ensure that the Trusted Platform Module (TPM) on each host is ready for use. In other words, the TPM is initialized and ownership obtained. You can check the status of the TPM by opening the TPM Management Console (tpm.msc) or by running the following command in an elevated Windows PowerShell console:

`Get-Tpm`

2. If your TPM is not in the Ready state, you will need to initialize it and set its ownership. This can be done in the TPM Management Console or by running the following command:

`Initialize-Tpm`

3. On each guarded host, run the following command in an elevated Windows PowerShell console to obtain its EKpub. For <HostName>, replace the unique host name with something suitable to identify this host—this can be its hostname or the name used by a

fabric inventory service (if available). For convenience, name the output file using the host's name.

```
(Get-PlatformIdentifier -Name '<HostName>').InnerXml | Out-file  
<Path><HostName>.xml
```

The command is shown in Figure 21.

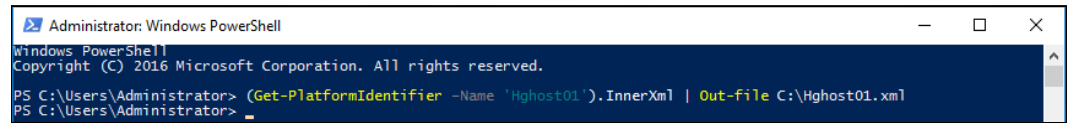


Figure 21 Command to get the EKpub

4. Copy the output XML file to an HGS server or a network share accessible by HGS.
5. In an elevated Windows PowerShell console on the HGS host, run the following command, Figure 22:

```
Add-HgsAttestationTpmHost -Path <Path><Filename>.xml -Name <HostName> -Force
```

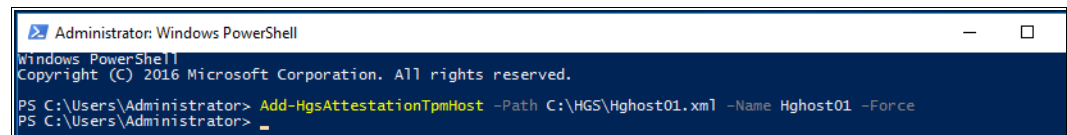


Figure 22 Add-HgsAttestationTpmHost command

Note: The **-Force** flag is used here to bypass a validation of the EKcert of the host's TPM. Hosts using TPMs without an EKcert or with an EKcert issued by an authority your HGS server does not trust will throw an error without the use of **-Force**. For the highest level of security, do not use the **-Force** flag to be alerted to potentially untrustworthy TPMs.

6. Repeat all of these steps for each host that will become a guarded host, being sure to give each XML file a unique name.

Create and apply a code integrity policy

To create and apply a code integrity policy, do the following:

1. On the reference host, generate a new code integrity policy. The following commands create a policy at the FilePublisher level with fallback to Hash. They then convert the XML file to the binary file format Windows and HGS need to apply and measure the CI policy, respectively. The commands are shown in Figure 23.

```
New-CIPolicy -Level FilePublisher -Fallback Hash -FilePath  
'C:\HW1CodeIntegrity.xml'
```

Note: It might take more than 30 minutes to finish this step.

```
ConvertFrom-CIPolicy -XmlFilePath 'C:\HW1CodeIntegrity.xml' -BinaryFilePath  
'C:\HW1CodeIntegrity.p7b'
```

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> New-CIPolicy -Level FilePublisher -Fallback Hash -FilePath 'C:\HW1CodeIntegrity.xml'
Scan completed successfully
PS C:\Users\Administrator> ConvertFrom-CIPolicy -XmlFilePath 'C:\HW1CodeIntegrity.xml' -BinaryFilePath 'C:\HW1CodeIntegrity.p7b'
C:\HW1CodeIntegrity.p7b
PS C:\Users\Administrator>

```

Figure 23 Commands to create a new code integrity policy

Logging mode only: The above command creates a CI policy in logging mode only. It will not block unauthorized binaries from running on the host. In order to enforce the policy, you must include the **-Deny** parameter in the **New-CIPolicy** command. It is recommended that you do this after you have verified the CI policy is working as expected.

2. Copy the binary file (HW1CodeIntegrity.p7b) to an HGS server or a network share accessible to HGS.
3. On an HGS server: To register the Code Integrity policy with the Attestation Service, run the following command, as shown in Figure 24:

`Add-HgsAttestationCIPolicy -Path <Path> -Name '<PolicyName>'`

For `<PolicyName>`, specify a name for the CI policy that describes the type of host it applies to. A best practice is to name it after the make/model of your machine and any special software configuration running on it.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-HgsAttestationCIPolicy -Path C:\HGS\HW1CodeIntegrity.p7b -Name 'Hghost01Policy'
Name          PolicyType State
-----
Hghost01Policy {CiPolicy} Enabled
PS C:\Users\Administrator>

```

Figure 24 Add-HgsAttestationCIPolicy command

4. Keep your Code Integrity policy file (XML file) where you can easily find it. You might need to update it or merge it with another policy in the future, and you might need it later if you choose to install System Center 2016 Virtual Machine Manager (VMM).
5. Finally, apply the CI policy to your hosts. Each host might have only one CI policy applied at a given time. To apply a CI policy, perform the following steps:
 - a. Copy the binary CI policy file (HW1CodeIntegrity.p7b) to `C:\Windows\System32\CodeIntegrity` on *each host*
 - b. Rename the file as **SIPolicy.p7b**, as shown Figure 25.

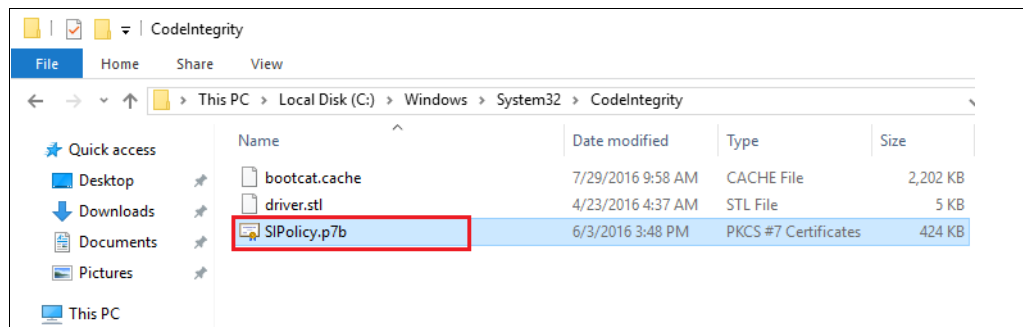


Figure 25 SIPolicy.p7b file in the CodeIntegrity folder on each host

- c. Restart the host to apply the policy.

Capture the TPM baseline for each unique class of hardware

The steps are as follows:

1. Run the following command in an elevated Windows PowerShell console to capture the baseline policy on the reference host:

```
Get-HgsAttestationBaselinePolicy -Path <Path><Filename>.tcglog
```

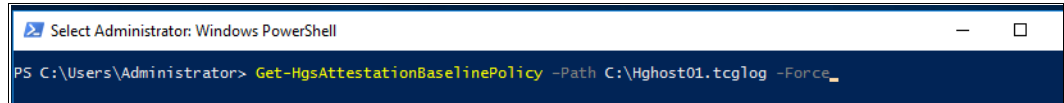


Figure 26 *Get-HgsAttestationBaselinePolicy* command

Note: You will need to provide the **-SkipValidation** flag if the reference host does not have a CI policy enforced or Secure Boot enabled. These validations are there to make you aware of the minimum requirements for running a Shielded VM, but do not affect the output of this command.

2. Copy the TCGlog file to an HGS server or a network share accessible by HGS.
3. On the HGS server where you copied the TCGlog file, add the baseline policy as an authorized baseline for attestation purposes using the following command, Figure 27 on page 17:

```
Add-HgsAttestationTpmPolicy -Path <Path><Filename>.tcglog -Name '<PolicyName>'
```

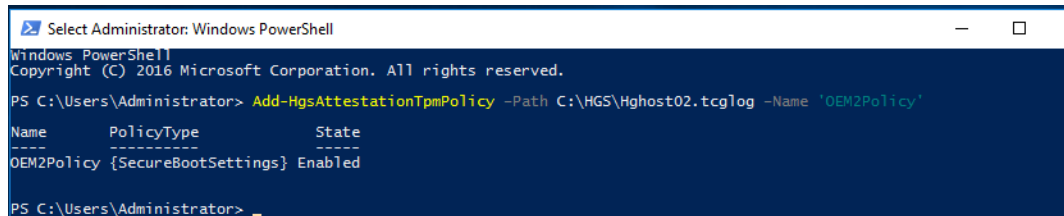


Figure 27 *Add-HgsAttestationTpmPolicy* command

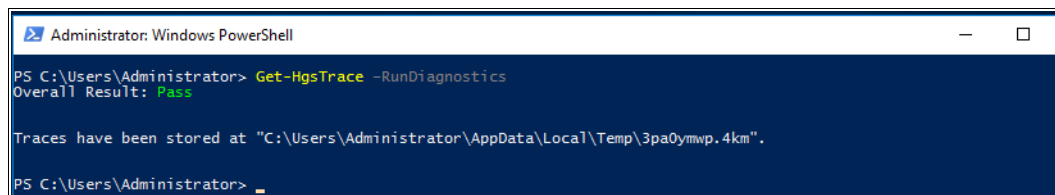
Verifying that HGS is configured properly

Now that HGS has been configured, it is time to check whether everything is configured correctly by running the HGS diagnostics tool. This tool will check for common misconfigurations and best practices and, when possible, provide information on how to fix any issues detected.

1. Run the HGS Diagnostics tool using the following command:

```
Get-HgsTrace -RunDiagnostics
```

2. In the output, check for any failures or warnings and address the concerns raised by the diagnostics tool. The output is saved to the file listed, as shown in Figure 28.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-HgsTrace -RunDiagnostics
Overall Result: Pass

Traces have been stored at "C:\Users\Administrator\AppData\Local\Temp\3pa0ymwp.4km".
PS C:\Users\Administrator>
```

Figure 28 *Get-HgsTrace command*

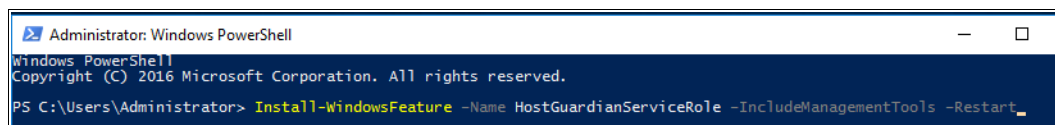
Configuring secondary HGS nodes

In production environments, HGS should be set up in a high-availability cluster to ensure that Shielded VMs will be able to be started even if an HGS node goes down. For test environments, secondary HGS nodes are not required.

The following steps will add an additional node to the HGS cluster that you previously set up. The computer should *not* be joined to any domain before you perform these steps.

1. To add the Host Guardian Service role to the computer, run the following command in an elevated Windows PowerShell console, as shown in Figure 29:

```
Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
```

Figure 29 *Installing the Host Guardian Service role*

2. Configure at least one NIC on this machine to use the DNS server on your first HGS server for name resolution. This is necessary to enable the machine to resolve and join the HGS domain and cluster in the next step.
3. Install the Host Guardian Service by running the following command in an elevated Windows PowerShell console as shown in Figure 30:

```
$adSafeModePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force
$cred = Get-Credential 'relecloud\Administrator'
```

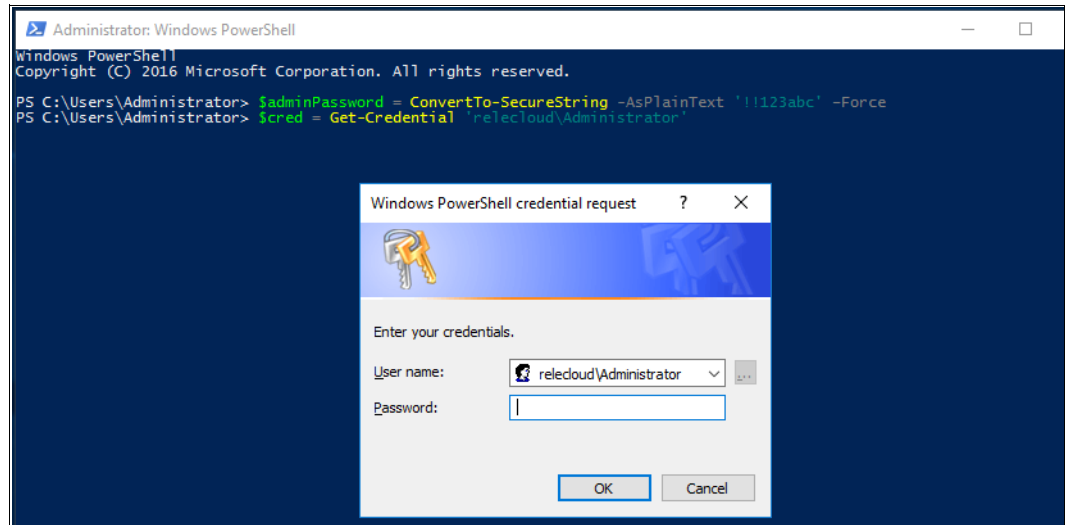


Figure 30 Install the Host Guardian Service

4. Enter the administrator password of the first HGS server and click OK.
5. Run the following command in an elevated Windows PowerShell console, Figure 31:
`Install-HgsServer -HgsDomainName 'relecloud.com' -HgsDomainCredential $cred -SafeModeAdministratorPassword $adSafeModePassword -Restart -Confirm:$false`

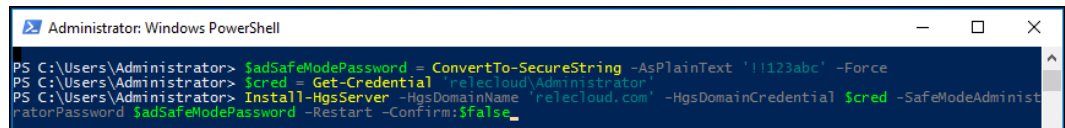


Figure 31 Install-HgsServer command

6. After the server restarts, sign in with the HGS domain administrator credentials.
7. Run the following command in an elevated Windows PowerShell console to finish adding the new node to the HGS cluster. Replace the IP address as appropriate for your environment, as shown in Figure 32 on page 19:

```
$cred = Get-Credential 'relecloud\Administrator'
```

```
Initialize-HgsServer -HgsServerIPAddress <IP address of first HGS Server> -HgsDomainCredential $cred -Confirm:$false
```

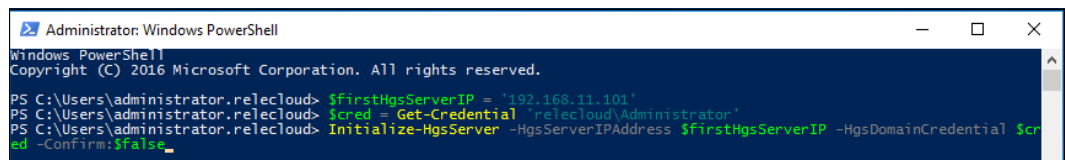


Figure 32 Initialize-HgsServer command

8. Allow up to 10 minutes for the encryption and signing certificates from the first HGS server to replicate to this node.
9. To validate that things are working as expected, run the following command in an elevated Windows PowerShell console:

```
Get-HGSTrace -RunDiagnostics
```

10. Review the results, paying careful attention to any tests that failed. If no failures occurred, the following will be shown:

Overall Result: Pass

If failures did occur, review the remediation steps provided or see the Troubleshooting Guide.

Perform steps on each node: It is important to repeat all of these steps for each additional node in your HGS cluster.

Confirming that hosts can attest successfully

Once your HGS nodes are set up, it is time to configure the Hyper-V hosts so that they can contact the HGS instance for attestation. If the previous configuration procedures for your chosen mode of attestation have been completed successfully, attestation will succeed on the hosts.

Complete the following steps on at least one host that you want to run as a guarded host:

1. Install Hyper-V and the Host Guardian Hyper-V Support features by running the following command in an elevated Windows PowerShell console, Figure 33:

`Install-WindowsFeature Hyper-V, HostGuardian -IncludeManagementTools -Restart`

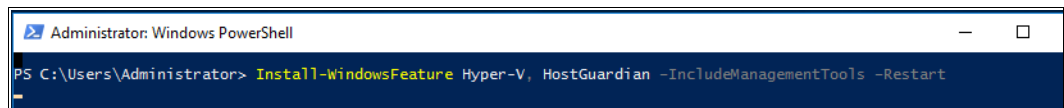


Figure 33 Installing Hyper-V and Host Guardian Hyper-V Support

2. Configure the host's Key Protection and Attestation URLs by running the following command in an elevated Windows PowerShell console:

`Set-HgsClientConfiguration -AttestationServerUrl 'http://<FQDN>/Attestation' -KeyProtectionServerUrl 'http://<FQDN>/KeyProtection'`

For <FQDN>, use the FQDN of your HGS cluster as shown in Figure 34 on page 20.

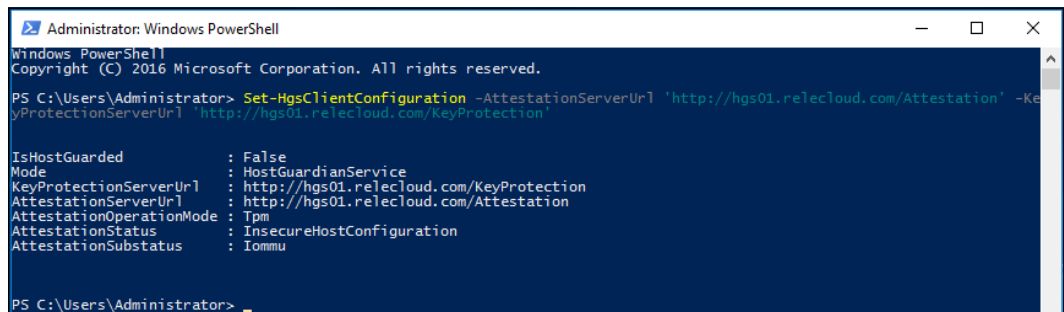


Figure 34 Set-HgsClientConfiguration command

3. Since this instruction uses TPM-based attestation mode as an example, we need to run the ModifyDeviceGuardKey script, which can be downloaded from the TechNet gallery at:

<https://gallery.technet.microsoft.com/Script-for-Setting-Up-f8bd7f7e>

4. Run the **ModifyDeviceGuardKey.PS1** script in an elevated Windows PowerShell console, and then restart the system. See Figure 35.

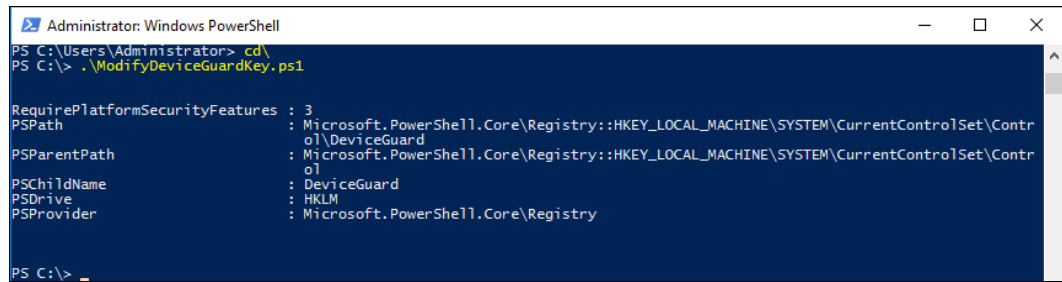


Figure 35 *ModifyDeviceGuardKey script*

5. Run the following command in an elevated Windows PowerShell console to initiate an attestation attempt on the host and view the attestation status:

`Get-HgsClientConfiguration`

The result shows whether attestation succeeded, that is, whether the host is now a guarded host. If the host is guarded, the information in Figure 36 is displayed:

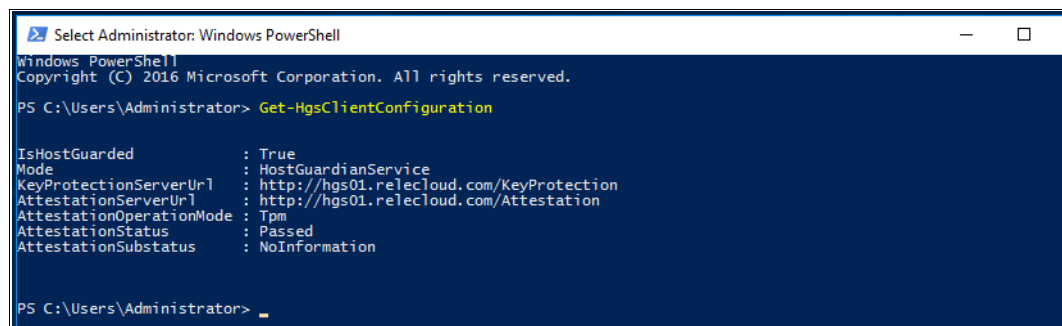


Figure 36 *Get-HgsClientConfiguration command*

You are now ready to begin using your guarded fabric.

Creating a new Shielded VM on-premises and moving it to a guarded fabric

There are possible scenarios of creating Shielded VMs in several other ways. This section describes the steps to create a Shielded VM using only Hyper-V; that is, without Virtual Machine Manager, template disks, or a shielding data file. This is an uncommon scenario for most public cloud hosting environments, but might be useful when testing a guarded fabric or in enterprise scenarios where a VM is being moved from a departmental fabric to shared IT infrastructure and must be encrypted before migration.

Importing the guardian configuration on the tenant Hyper-V server

Follow these steps:

1. Before beginning the procedure, make sure that you are on a Hyper-V host running Windows Server 2016 Technical Preview 5 with the following roles and features installed:
 - Hyper-V role, as shown in Figure 37

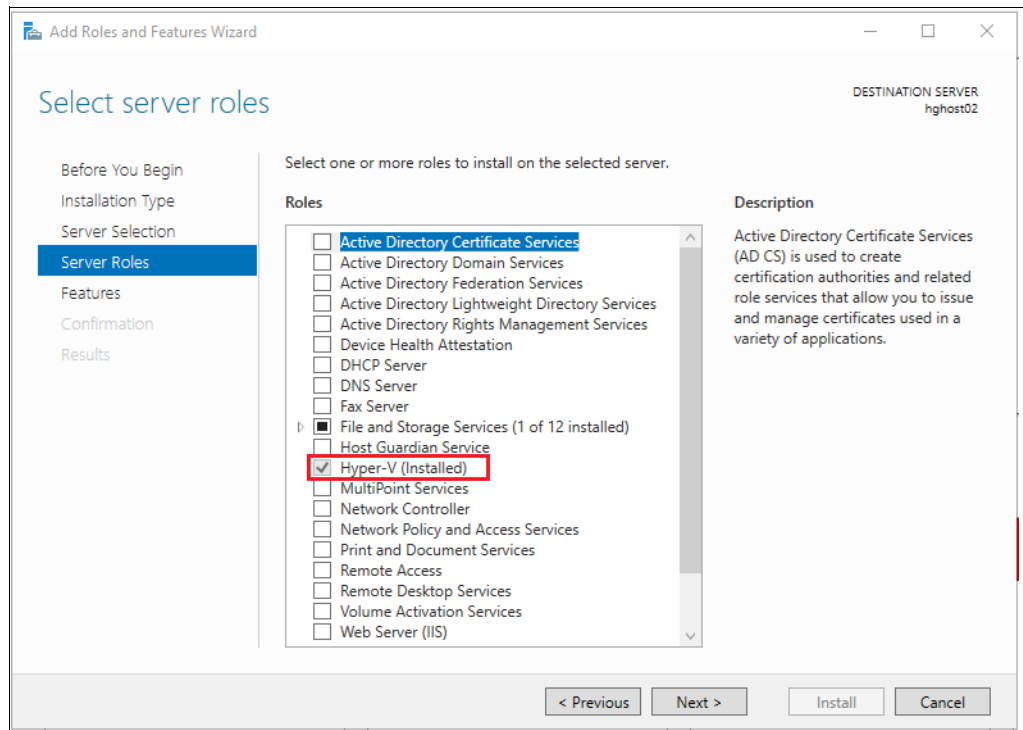


Figure 37 Verifying the Hyper-V role is installed

- Shielded VM Tools feature as shown in Figure 38 on page 22.

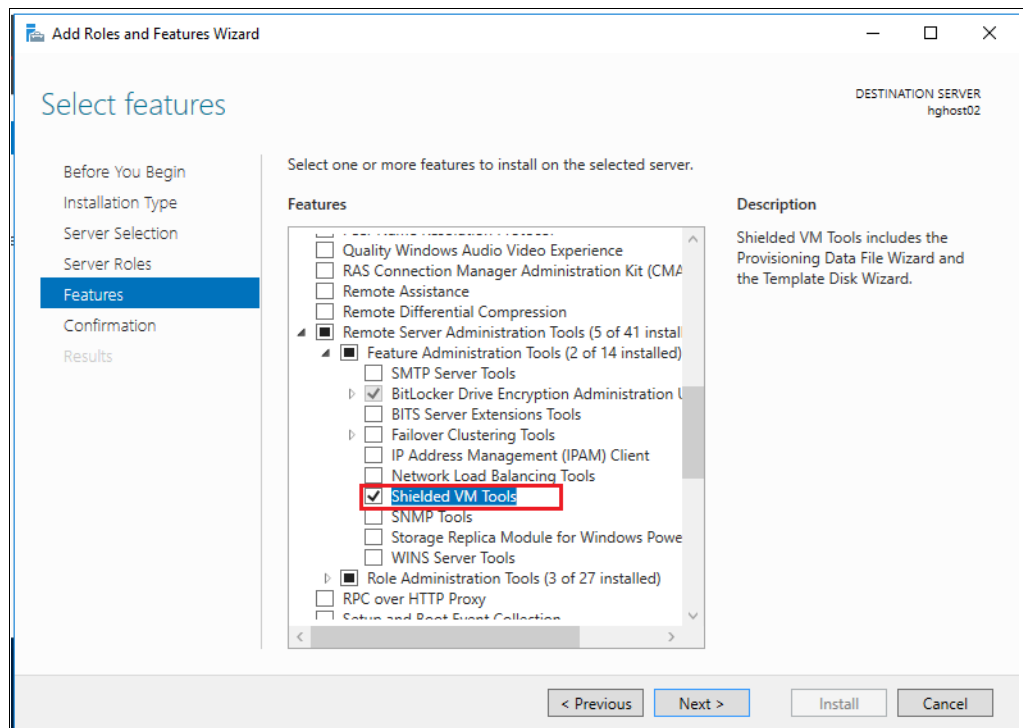


Figure 38 Verifying that the Shielded VM Tools feature is installed

Note: The host used here should not be a host in the guarded fabric. This is a separate host where VMs are prepared before being moved to the guarded fabric.

2. Acquire the guardian metadata for the guarded fabric where your VM will run. This metadata is used to authorize that fabric to run your Shielded VM. How you obtain this information will be different for each hosting service provider or enterprise.

The host administrator (or you, if you have access to the guarded fabric network) can acquire this information by running the following command in an elevated Windows PowerShell console, Figure 39:

```
Invoke-WebRequest  
'http://hgs01.relecloud.com/KeyProtection/service/metadata/2014-07/metadata.xml'  
-OutFile .\GuardianKey.xml
```

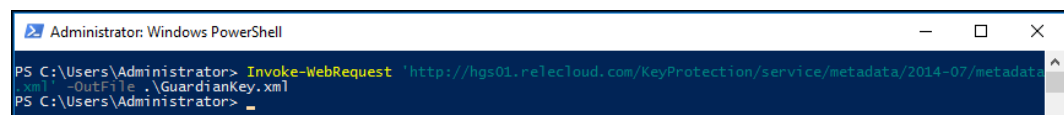


Figure 39 Invoke-WebRequest command

In Figure 39, hgs01 is the distributed network name of the HGS cluster and relecloud.com is the name of the HGS domain.

The file "RelecloudGuardian.xml" will be placed in C:\Users\Administrator.

Note: If you do not have name resolution and/or connectivity between the tenant Hyper-V Host and HGS infrastructure, you can download it on the HGS server and transfer it offline to the tenant Hyper-V Host.

3. Run the following command to import the guardian key, which you will need in a later procedure:

```
Import-HgsGuardian -Path '<Path><Filename>' -Name '<GuardianName>'  
-AllowUntrustedRoot
```

For <Path><Filename>, replace it with the path and filename of the XML file you saved in the previous step, for example: C:\temp\GuardianKey.xml

For <GuardianName>, specify a name for your hosting provider or enterprise datacenter, for example, HostingProvider1. Record the name for the next procedure.

Include -AllowUntrustedRoot only if the HGS server was set up with self-signed certificates. (These certificates are part of the Key Protection Service in HGS.)

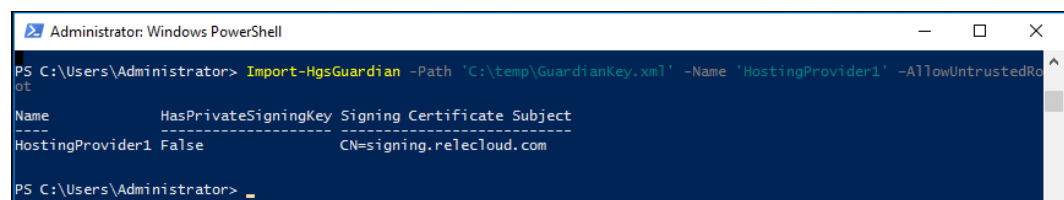


Figure 40 Import-HgsGuardian command

Creating a new Shielded VM on the host

In this procedure, you will create a VM on the Hyper-V host, and prepare it for export to your hosting provider or data center administrator, who can run it on a guarded host.

As part of the procedure, you will create a Key Protector that contains two important elements:

- **Owner:** In the Key Protector, you—or more likely, the group you work in that shares security elements such as certificates—are identified as “owner” of the VM. Your identity as owner is represented by a certificate that, if you run the related commands, is generated as a self-signed certificate. Optionally, you can instead use a certificate backed by PKI infrastructure, and omit the `-AllowUntrustedRoot` parameter in the commands.
- **Guardians:** Also in the Key Protector, your hosting provider or enterprise data center (which runs HGS and guarded hosts) is identified as a “guardian.” The guardian is represented by the guardian key that you imported in the previous procedure. Import the guardian configuration on the tenant Hyper-V server.

Perform the following steps to create a new Shielded VM:

1. On a tenant Hyper-V host, run the following command to create a new Generation 2 VM, as shown in Figure 41 on page 24.

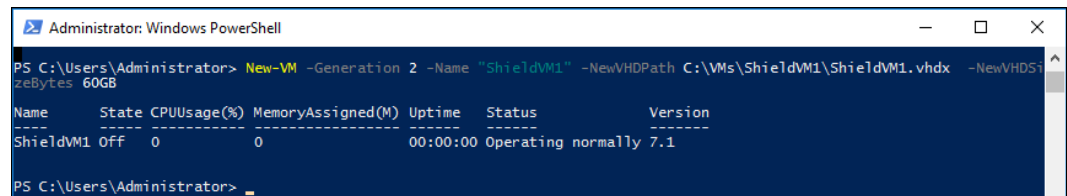
```
New-VM -Generation 2 -Name "<ShieldedVMname>" -NewVHDPATH <VHDPATH>.vhdx  
-NewVHDSIZEBYTES <nnGB>
```

For `<ShieldedVMname>`, specify a name for the VM, for example: `ShieldVM1`

For `<VHDPATH>`, specify a location to store the VHDX of the VM, for example:

`C:\VMs\ShieldVM1\ShieldVM1.vhdx`

For `<nnGB>`, specify a size for the VHDX, for example: `60GB`



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator> New-VM -Generation 2 -Name "ShieldVM1" -NewVHDPATH C:\VMs\ShieldVM1\ShieldVM1.vhdx -NewVHDSIZEBYTES 60GB  
Name      State CPUUsage(%) MemoryAssigned(M) Uptime   Status           Version  
-----  
ShieldVM1 Off    0          0              00:00:00 Operating normally 7.1  
PS C:\Users\Administrator>
```

Figure 41 New-VM command

2. Open Hyper-V Manager and perform the following tasks:
 - a. Configure a virtual switch via the Virtual Switch Manager via Hyper-V Manager as shown in Figure 42.

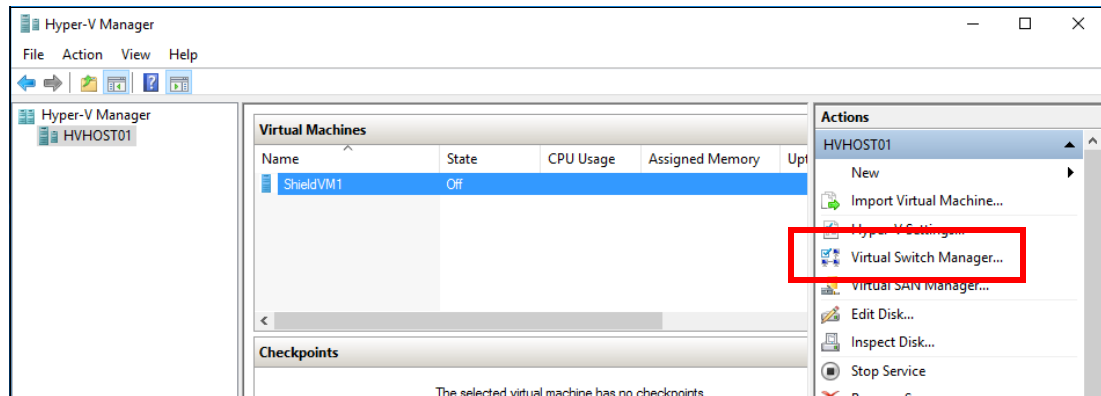


Figure 42 Hyper-V Manager

- b. Install a supported operating system (Windows Server 2012 or later, Windows 8 client or later) on the VM
- c. Enable the remote desktop connection, as shown in Figure 43

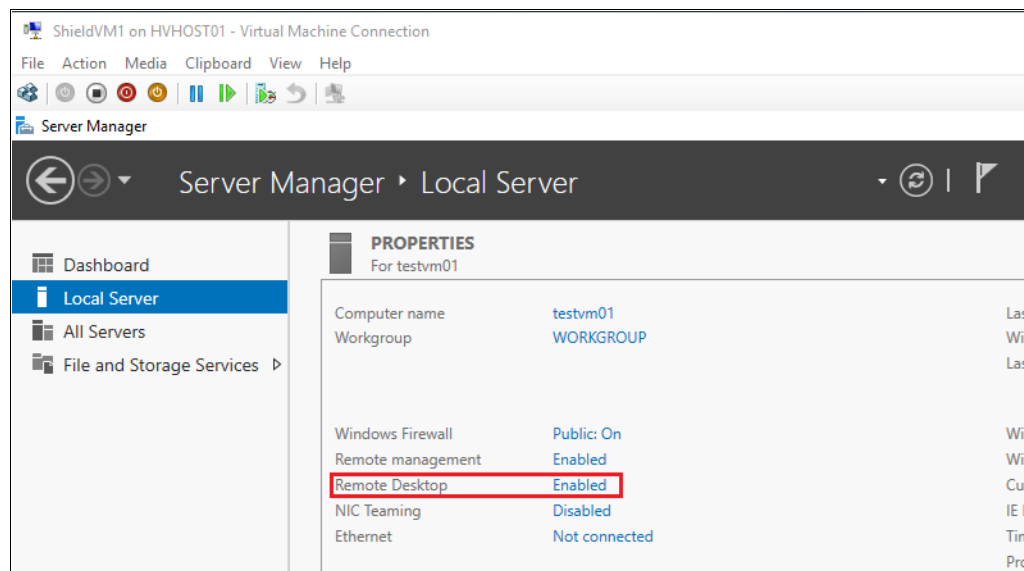


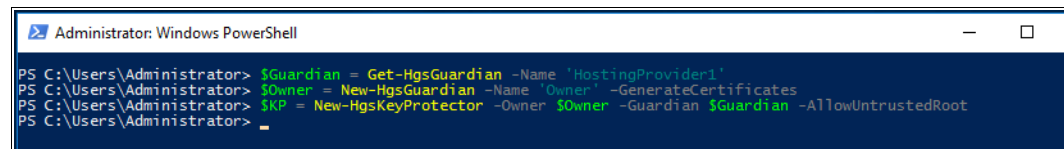
Figure 43 Remote Desktop enabled

- d. Enable the corresponding firewall rule as needed.
3. Record the VM's IP address and/or DNS name, which you will need to remotely connect to the VM.
 4. Use Remote Desktop Protocol (RDP) (run `mstsc`) to remotely connect to the VM and verify that RDP and the firewall are configured correctly. As part of the shielding process, console access to the VM through Hyper-V will be disabled, so it is important to ensure that you are able to remotely manage the system over the network.
 5. Create a new Key Protector by running the `New-HgsKeyProtector` command as follows and as shown in Figure 44:

```
$Guardian = Get-HgsGuardian -Name '<GuardianName>'
$Owner = New-HgsGuardian -Name 'Owner' -GenerateCertificates
$KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot
```

For <GuardianName>, use the name you specified in the previous procedure, for example: HostingProvider1

Include -AllowUntrustedRoot to allow for self-signed certificates.



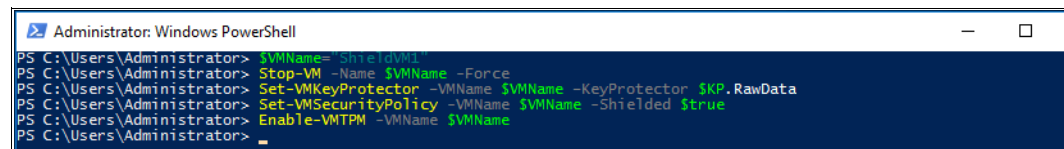
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> $Guardian = Get-HgsGuardian -Name 'HostingProvider1'
PS C:\Users\Administrator> $Owner = New-HgsGuardian -Name 'Owner' -GenerateCertificates
PS C:\Users\Administrator> $KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot
PS C:\Users\Administrator>
```

Figure 44 New-HgsKeyProtector command

6. If you need more than one data center to be able to run your Shielded VM (for example, a disaster recovery site and a public cloud provider), you can repeat the above command with varied <GuardianName> values for different guardians. Consult the PowerShell help information for the New-HgsKeyProtector command for more information.
7. Enable the vTPM using the Key Protector, with the following commands:

```
$VMName="<ShieldedVMname>"
Stop-VM -Name $VMName -Force
Set-VMKeyProtector -VMName $VMName -KeyProtector $KP.RawData
Set-VMSecurityPolicy -VMName $VMName -Shielded $true
Enable-VMTPM -VMName $VMName
```

For <ShieldedVMname>, use the same VM name used in previous steps.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> $VMName="ShieldedVM1"
PS C:\Users\Administrator> Stop-VM -Name $VMName -Force
PS C:\Users\Administrator> Set-VMKeyProtector -VMName $VMName -KeyProtector $KP.RawData
PS C:\Users\Administrator> Set-VMSecurityPolicy -VMName $VMName -Shielded $true
PS C:\Users\Administrator> Enable-VMTPM -VMName $VMName
PS C:\Users\Administrator>
```

Figure 45 Enabling the vTPM using the Key Protector

8. Start the VM to verify that the key protector is working with local owner certificates, by using the following command:

```
Start-VM -Name $VMName
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Start-VM -Name $VMName
PS C:\Users\Administrator>
```

Figure 46 Start-VM command

9. Verify that the VM has started (but not connectable) in the Hyper-V console. You will see Figure 47.

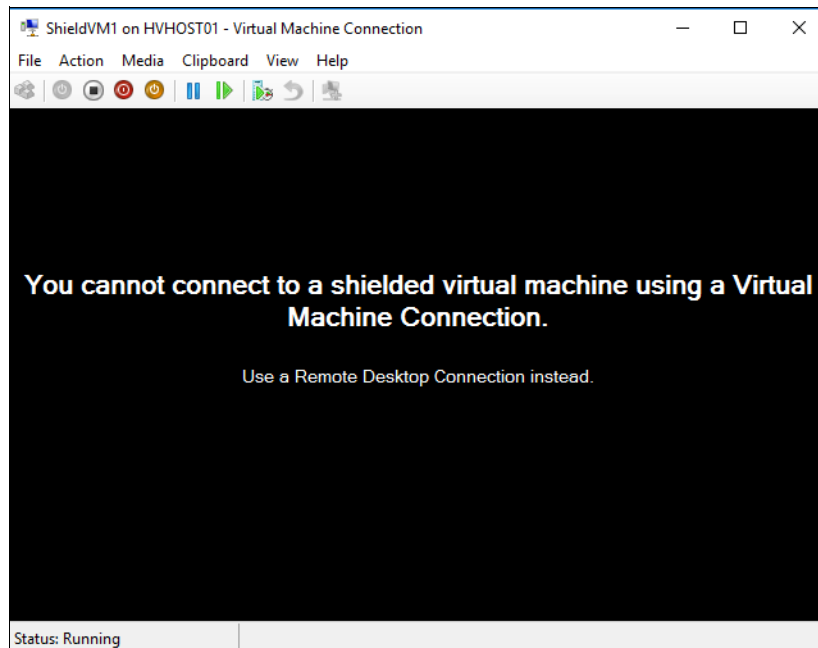


Figure 47 VM is started but not connectable in the Hyper-V Console

10. Use RDP to remotely connect to the VM.
11. Enable BitLocker on all partitions on all VHDXs that are attached to the Shielded VM, as shown in Figure 48. You need to create a shared folder to save the BitLocker recovery key.

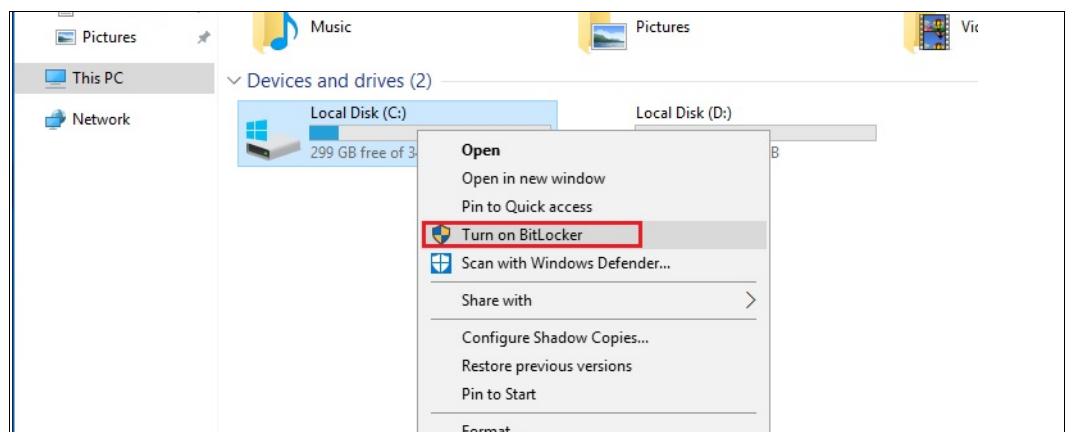


Figure 48 Enabling BitLocker on a partition

If you don't see Turn on BitLocker in the context menu, you will need to install the feature as shown in Figure 49 on page 28.

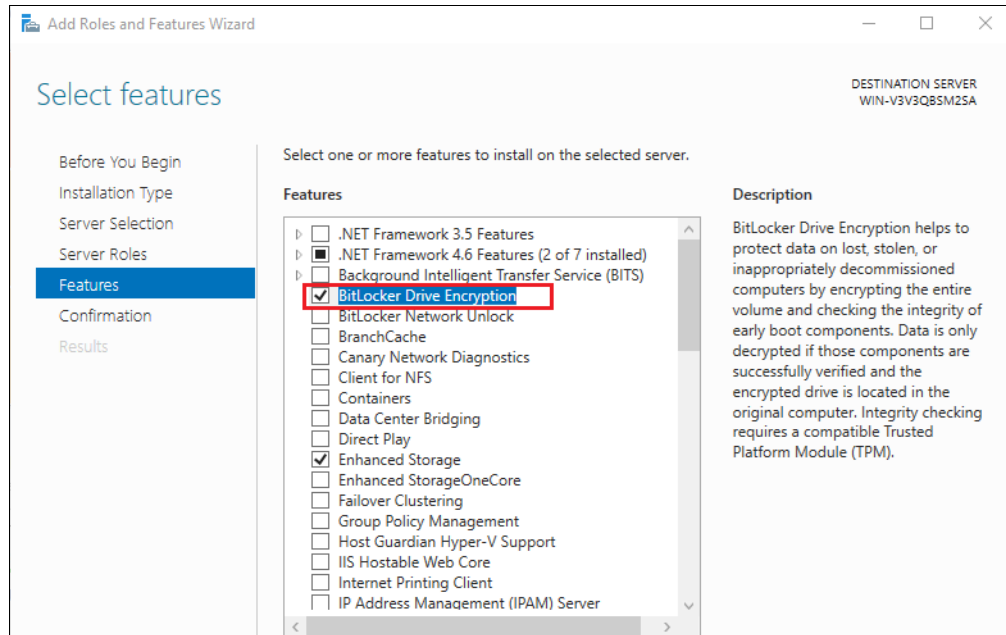


Figure 49 Installing BitLocker

12.Wait until BitLocker encryption is completed.

Note: Before proceeding to the next step, wait for BitLocker encryption to finish on all partitions where you have enabled it.

13.Shut down the VM when you are ready to move it to the guarded fabric.

14. On the tenant Hyper-V server, export the VM using the tool of your choice (Hyper-V Manager as shown in Figure 50 on page 29, or Windows PowerShell). Then copy the files to a guarded host maintained by your hosting provider or enterprise data center.

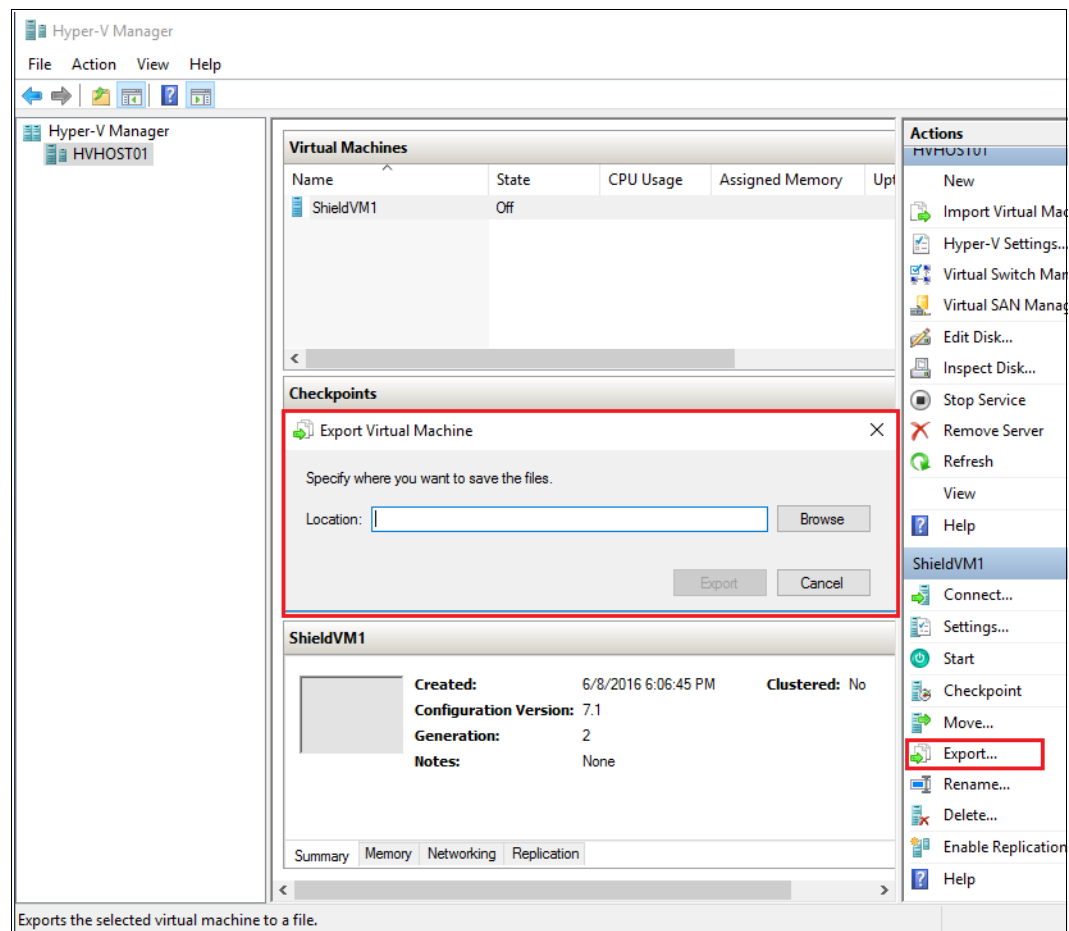


Figure 50 Exporting the VM using Hyper-V Manager

15. Wait for export to finish before continuing. You will see the **Export** action item again once the export function is complete.
16. Import the Shielded VM using Hyper-V Manager or Windows PowerShell. You must import the VM configuration file from the VM owner in order to start the VM. This is because the Key Protector which contains the VM's virtual TPM is stored in the configuration file. If the VM is configured to run on the guarded fabric, it should be able to start successfully.
- To import the Shielded VM, do the following:
- Choose Import Virtual Machine in Hyper-V Manager, Figure 51 on page 30.

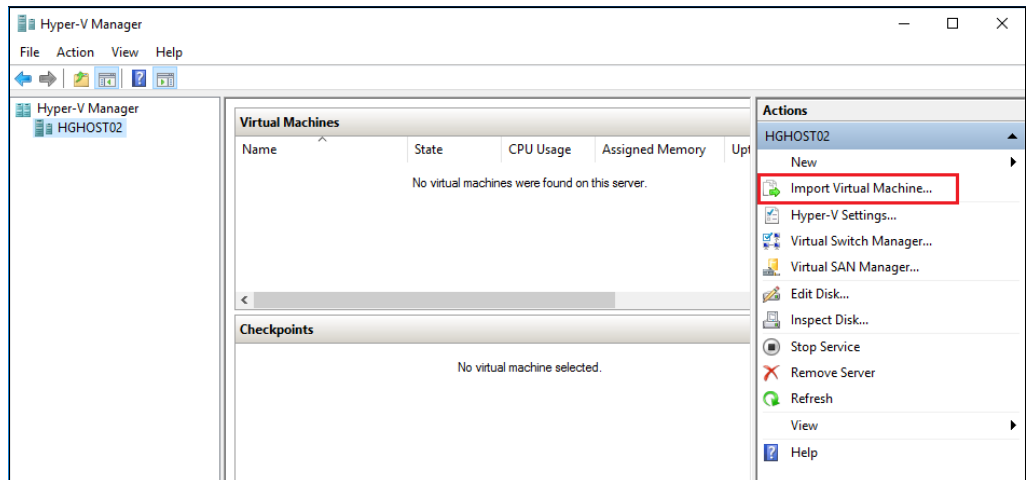


Figure 51 Launching the Import Virtual Machine wizard

- b. Browse the exported VM folder that you copied from the tenant Hyper-V server, Figure 52.

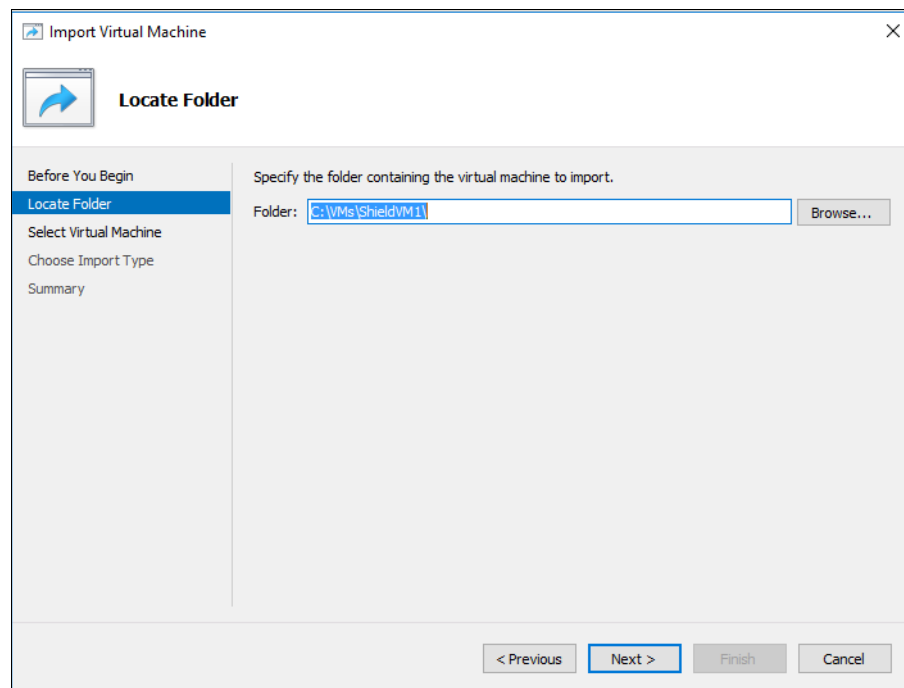


Figure 52 Import Virtual Machine wizard - Locate Folder

- c. If you see the name of the VM to be imported, which you created previously, Figure 53 on page 31, click **Next**.

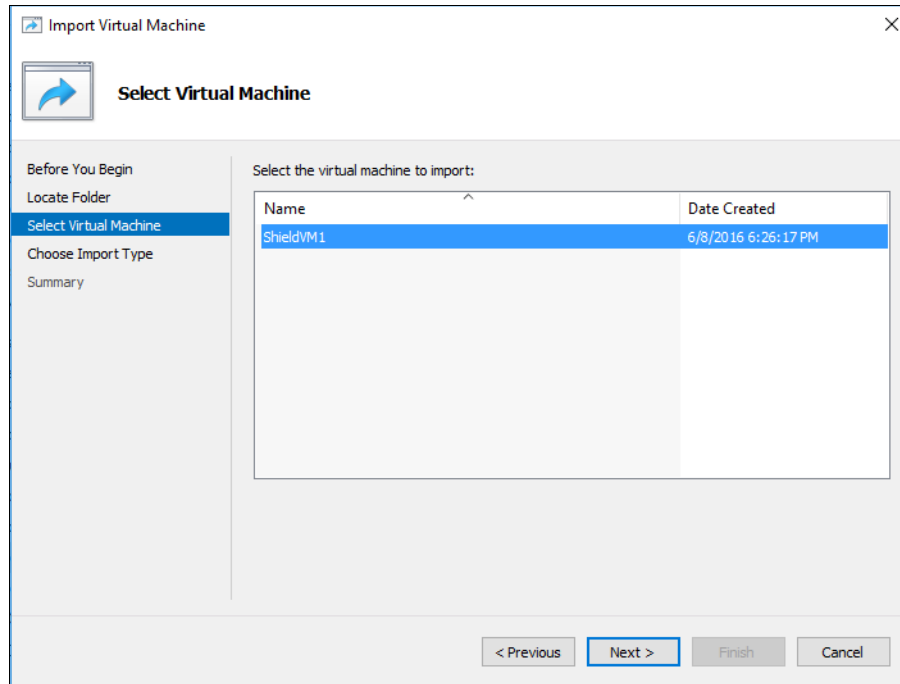


Figure 53 Import Virtual Machine wizard - Select Virtual Machine

- d. Choose the type of import to perform, as in Figure 54, and then click **Next**.

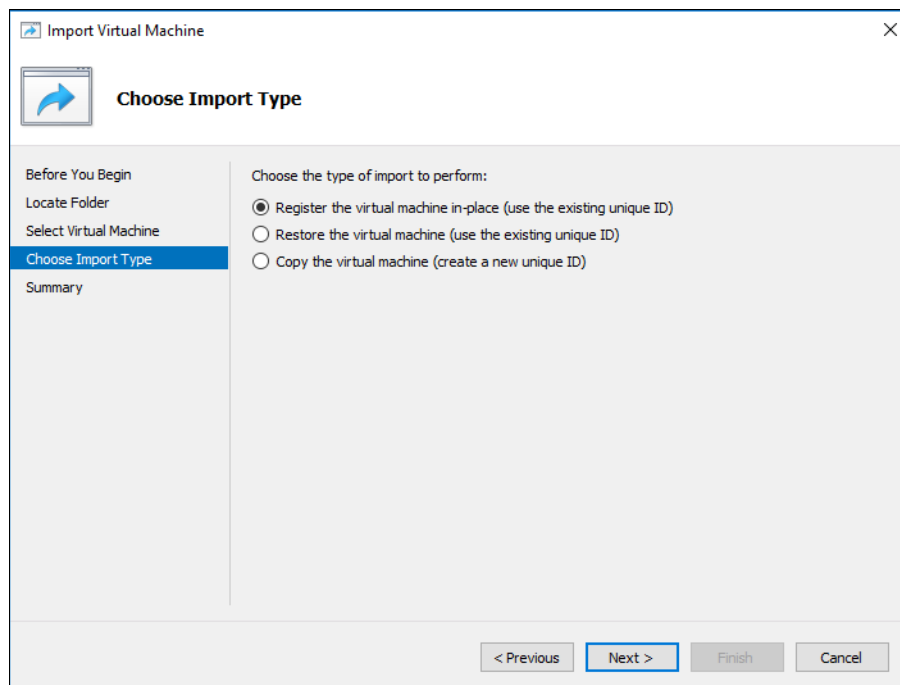


Figure 54 Import Virtual Machine wizard - Choose Import Type

- e. In Hyper-V Manager, start the Shielded VM. It should start successfully, Figure 55 on page 32.

Virtual Machines						
Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
ShieldVM1	Running	0 %	4096 MB	00:00:31		7.1

Figure 55 VM is started

If the VM successfully starts, it means that the Key Protector was configured correctly and that the VM is running securely on the Guarded Fabric.

Summary

Shielded VMs in Windows Server 2016 is a Generation 2 VM feature that comes with a virtual Trusted Platform Module (TPM), is encrypted using BitLocker, and runs on healthy and approved hosts in the fabric. This paper describes how to deploy a guarded fabric and create a Shielded VM on Lenovo servers.

For more information on Shielded VMs, see these following articles:

- ▶ What are Shielded VMs in Windows Server 2016 Hyper-V?
<https://blogs.technet.microsoft.com/datacentersecurity/2016/03/14/windows-server-2016-shielded-vms-protecting-tenant-secrets/>
- ▶ Guarded Fabric Deployment Guide for Windows Server 2016
<https://gallery.technet.microsoft.com/shielded-vms-and-guarded-98d2b045>

Change history

December 7, 2016:

- ▶ Grammar and style corrections

Authors

This paper was produced by the following specialist:

Boyong Li is a Windows Engineer of the Lenovo Data Center Group in Beijing, China. He has two years experience as a Software Architecture engineer, ten years experience as a BIOS engineer and one year of experience with Windows debugging.

Thanks to the following people for their contributions to this project:

- ▶ Michael J. Miller, Lenovo Windows Integration & Enablement
- ▶ Jerry Tang, Lenovo Information Development
- ▶ David Watts, Lenovo Press
- ▶ Mark T. Chapman, Lenovo Marketing Enablement

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document was created or updated on December 7, 2016.

Send us your comments via the **Rate & Provide Feedback** form found at <http://lenovopress.com/lp0540>

Trademarks

Lenovo, the Lenovo logo, and For Those Who Do are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. These and other Lenovo trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by Lenovo at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of Lenovo trademarks is available on the Web at <http://www.lenovo.com/legal/copytrade.html>.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo(logo)®

Lenovo®

The following terms are trademarks of other companies:

Active Directory, BitLocker, Hyper-V, Windows, Windows PowerShell, Windows Server, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.