Aia Al-Qasab

T5616SN

Advanced Enterprise Server Environment

Lab 4

**Virtualization Lab 4. Implementing shielded virtual machines**

February 2019



# Virtualization Lab 4. Implementing shielded virtual machines

A shielded virtual machine is a generation 2 virtual machine that is hardened to mitigate risk from unauthorized access and is permitted to run only on healthy and approved hosts. Shielded virtual machines are encrypted using BitLocker, and they leverage the virtual Trusted Platform Module (TPM) to mitigate security risks. Because virtual machines are essentially files that encapsulate an operating system and the applications running on that operating system, they present security challenges and risks that are distinct and different from the security risks attached to physical servers. Any virtual machine, including those that reside on disks encrypted with BitLocker, are vulnerable to threats caused by rogue administrators. This risk is especially problematic in multi-tenant situations in which fabric administrator’s virtualization host administrators, network administrators, storage administrators, backup administrators, and so on have access to the virtual machine running on the virtualization host.

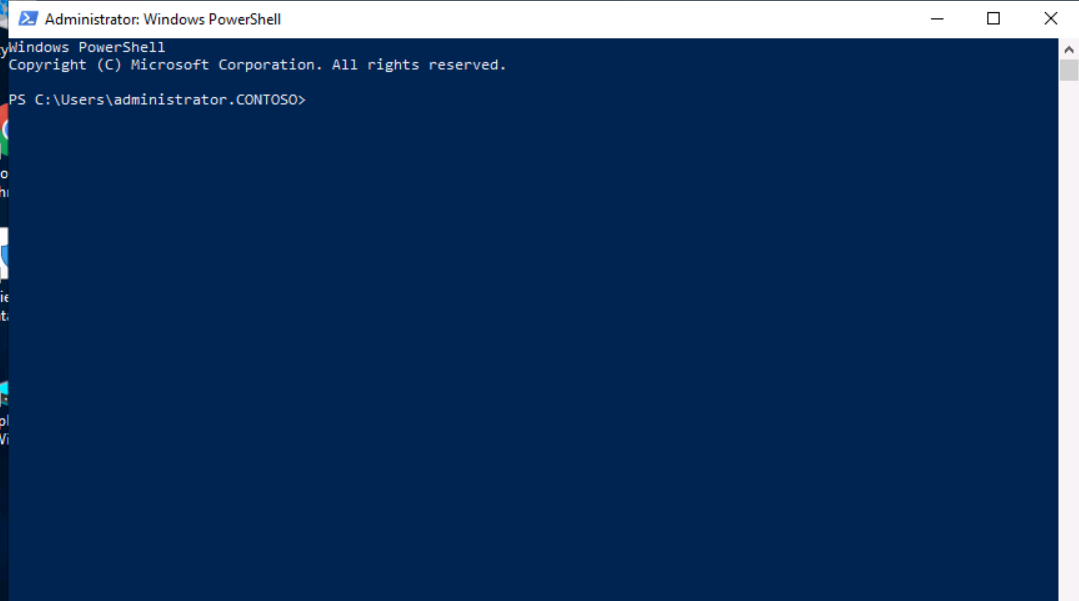
**Step 1: Deploy a Windows shielded virtual machine using host key attestation:**

This step we will deploy a shielded virtual machine that is protected using an attestation mode new to Windows Server 2019: host key attestation. This attestation mode provides similar assurances to Active Directory attestation mode for circumstances in which TPM attestation mode is not possible.

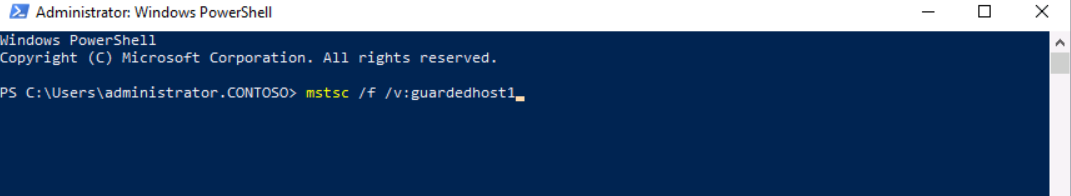
Sign in to the **SVR01** virtual machine as Contoso\Administrator using Passw0rd! as the password.

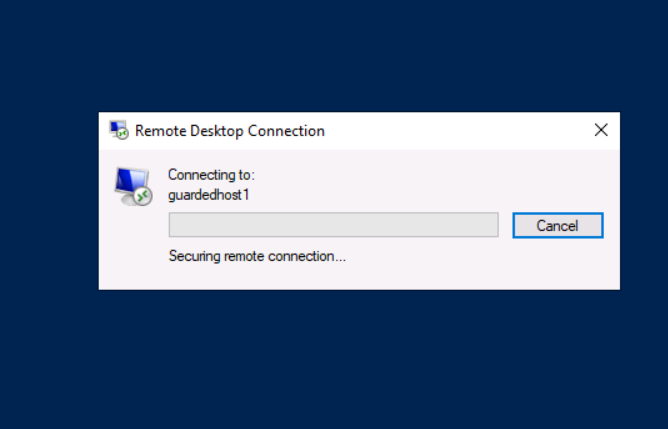


Open **Windows PowerShell**.



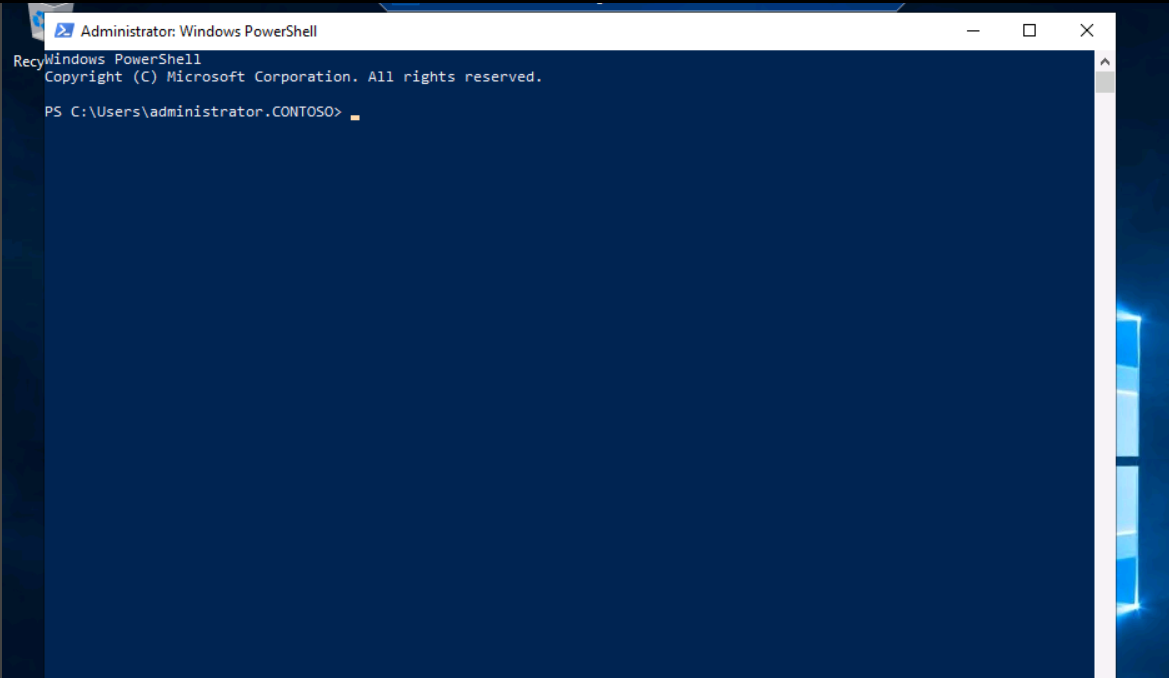
At the Windows PowerShell command prompt, run the following command to establish an RDP connection to **GuardedHost1**.







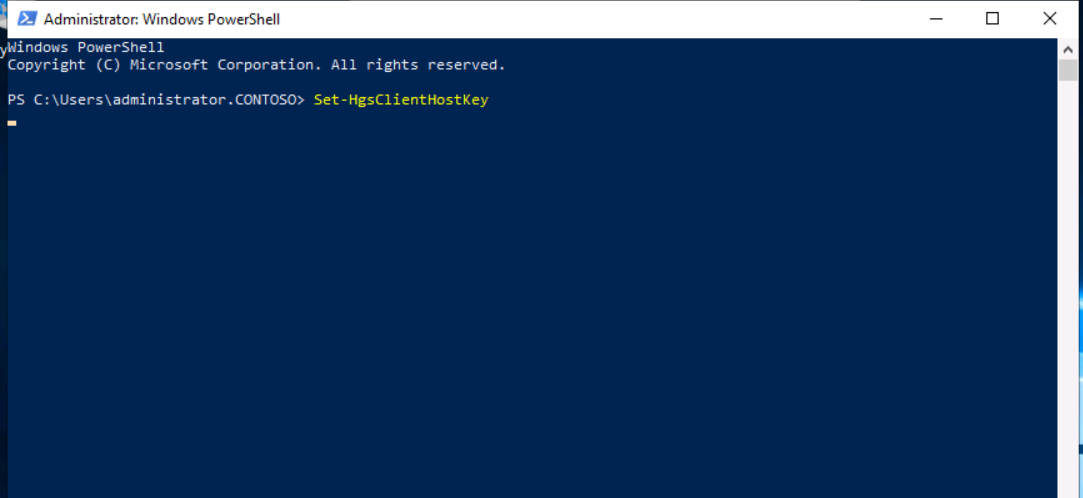
On **GuardedHost1**, open **Windows PowerShell**.



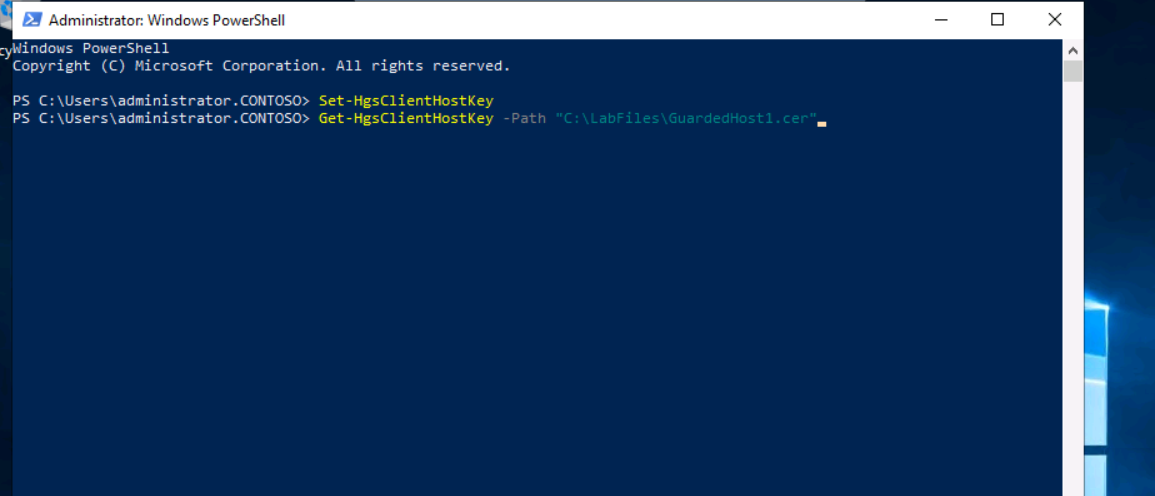
Run the following command to generate a self-signed asymmetric key pair for use with host key attestation.

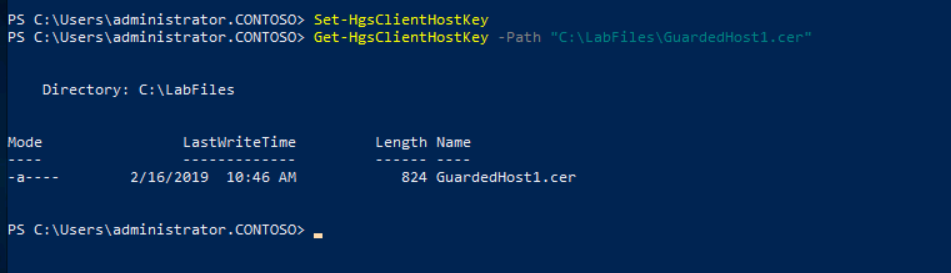
PowerShell

Set-HgsClientHostKey

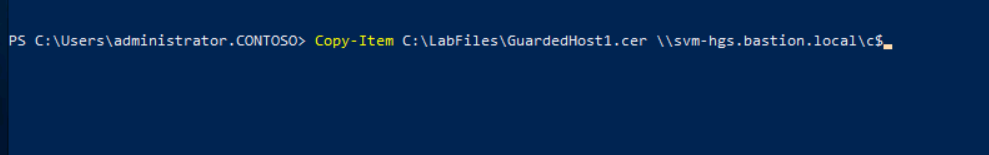


Run the following command to generate the self-signed certificate containing the public key of the asymmetric key pair you generated in the previous step.





Run the following command to copy the public certificate to the HGS server, svm-hgs.bastion.local.



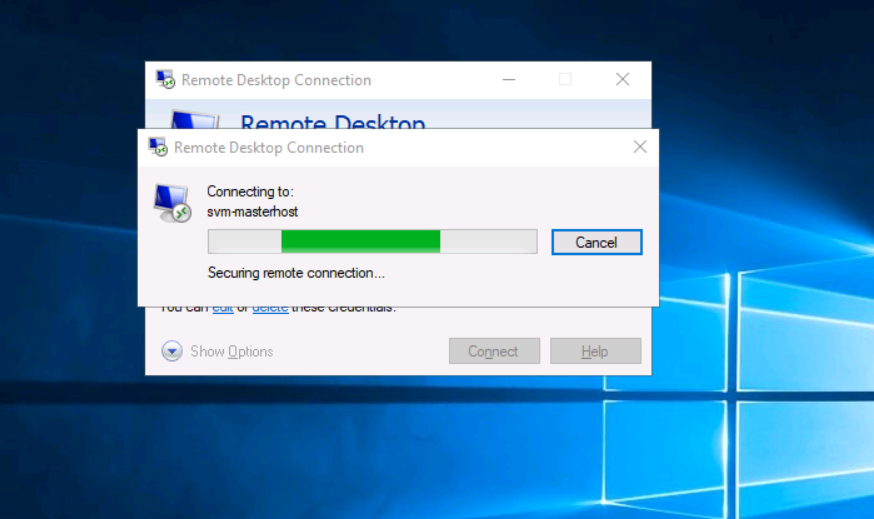
Minimize the remote desktop session to **GuardedHost1**.



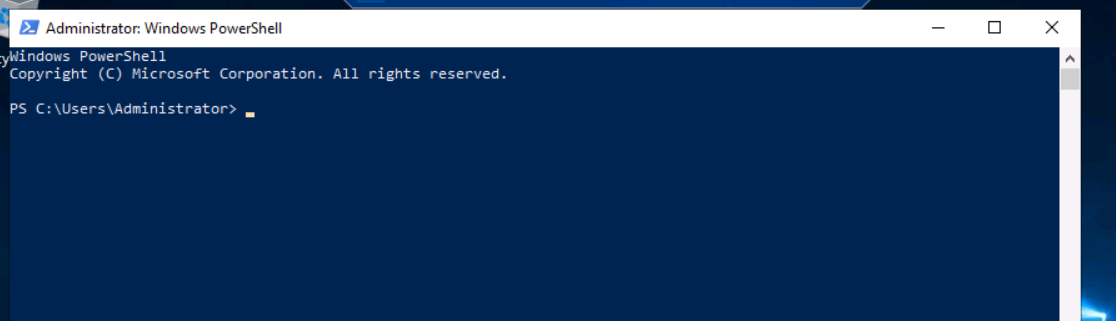
On **SRV01**, run the following command to establish an RDP connection to the HGS server.



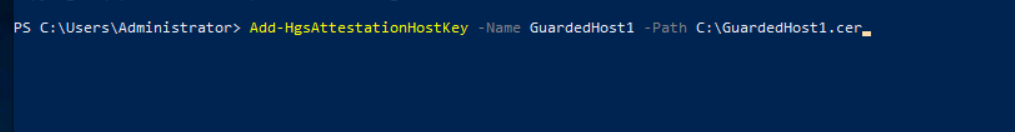
When prompted, sign in as Bastion\Administratorusing Passw0rd! as the password.



On **SVM-HGS**, open **Windows PowerShell**.



Run the following command to add the public key to the attestation service to allow the host to run shielded virtual machines.

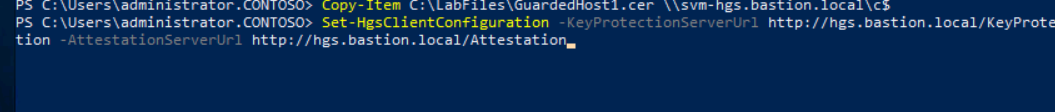


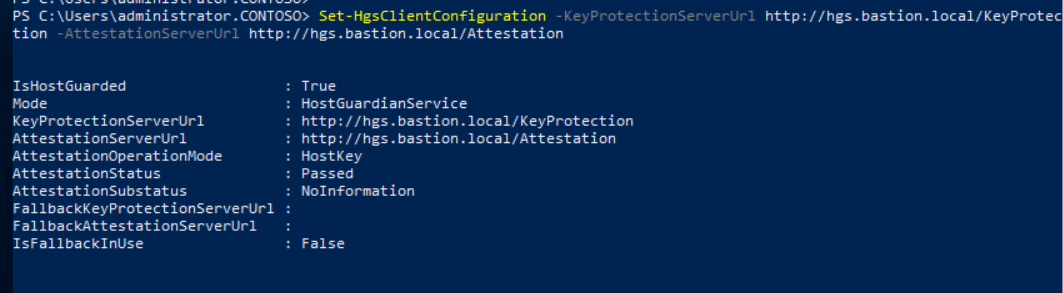


Minimize the RDP session for SVM-HGS, and then restore the RDP session for **GuardedHost1**.



On **GuardedHost1**, run the following command to configure the host to use the HGS server for attestation and key protection.



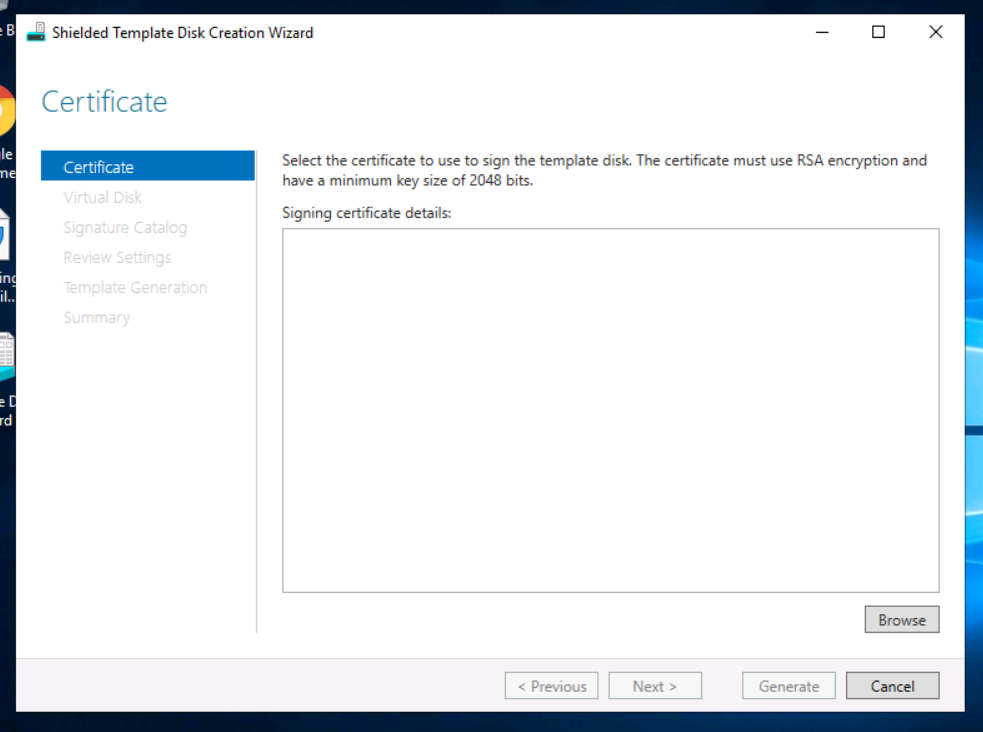


**Step 2: Create a shielded virtual machine template disk:**

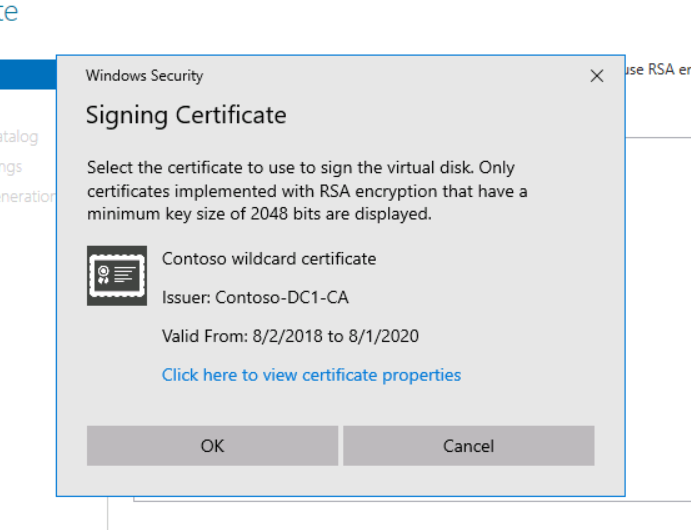
A shielded virtual machine uses a specially prepared disk that is encrypted with Bit Locker. Therefore, to deploy a shielded virtual machine, you must take additional steps to prepare the template disk you will use to deploy the virtual machine. The requirements for a shielded virtual machine template disk include the following:

* The virtual disk meets the following requirements of generation 2 virtual machines:
  + Must be a GUID partition table (GPT) disk.
  + Must use the Basic disk type.
  + Must use NTFS.
* A suitable operating system (recent versions of Windows) is installed on the virtual disk.
* The operating system is generalized using sysprep.
* The disk is prepared and encrypted with BitLocker using the Shielded Template Disk Creation Wizard.

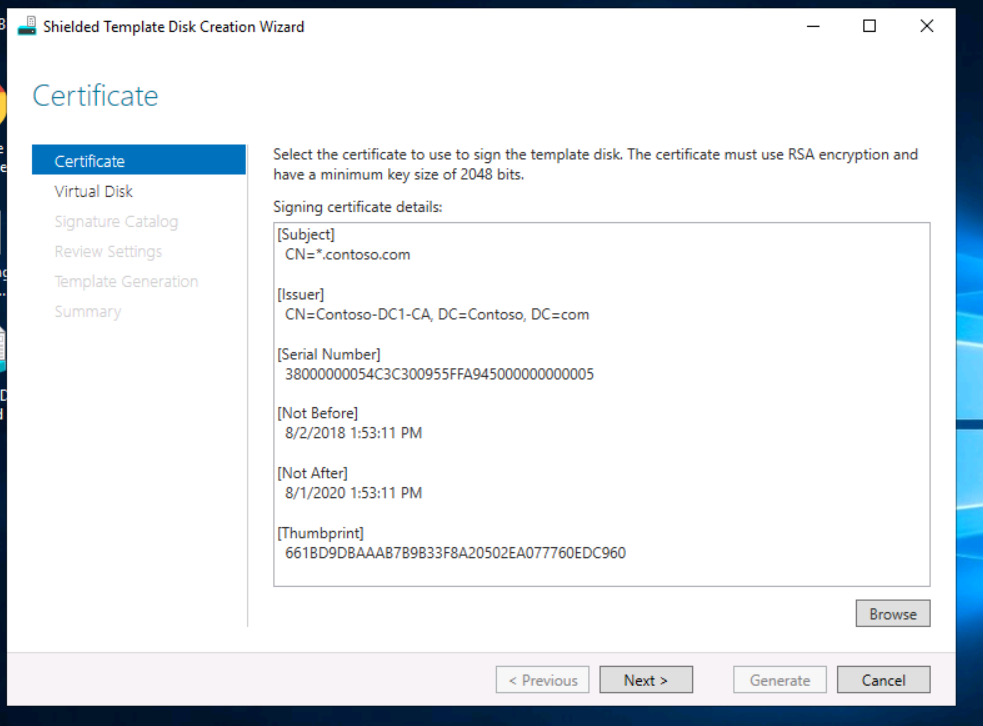
On the desktop of **SVR01**, open the **Template Disk Wizard**.



On the Certificate page, select **Browse**, and then select **OK** to select the Contoso wildcard certificate.



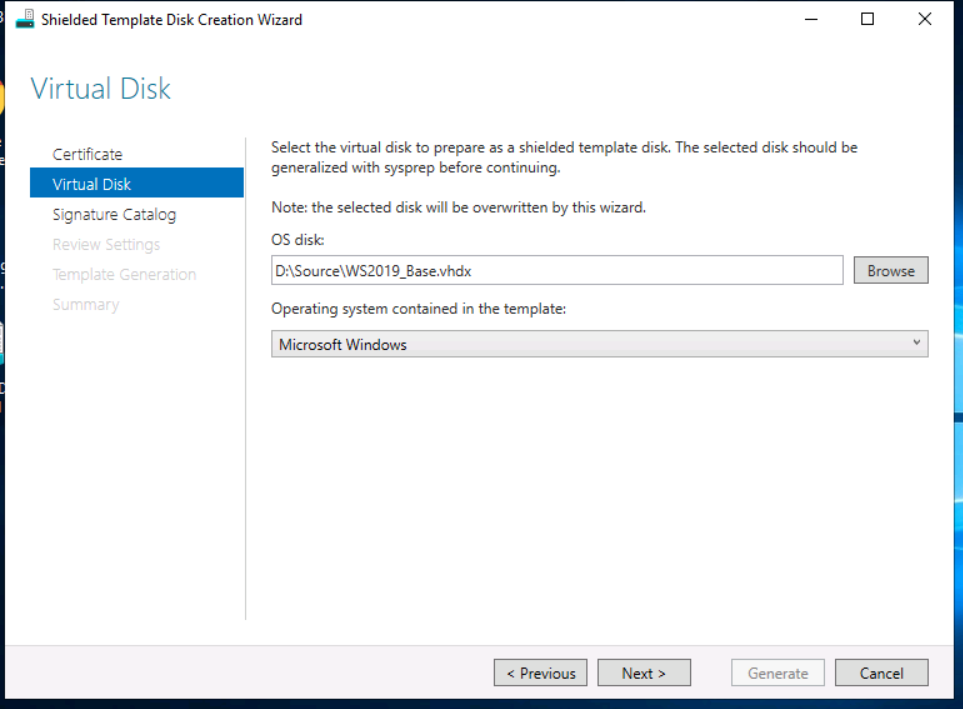
Select **Next**.



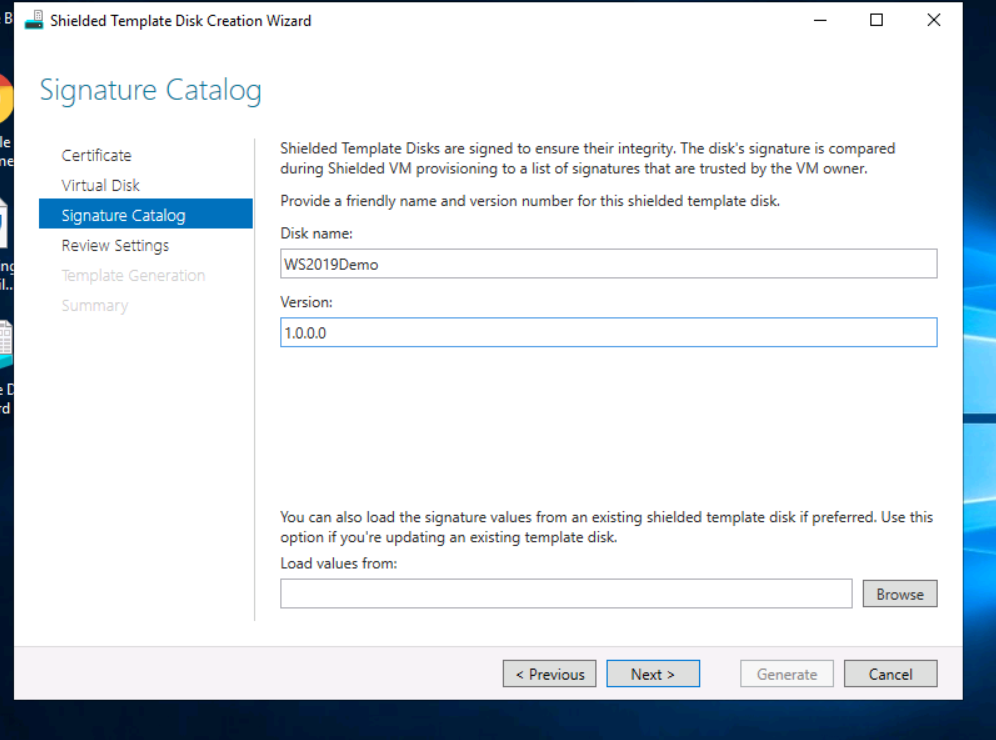
On the Virtual Disk page, select **Browse**, and then select **WS2019\_Base.vhdx**.



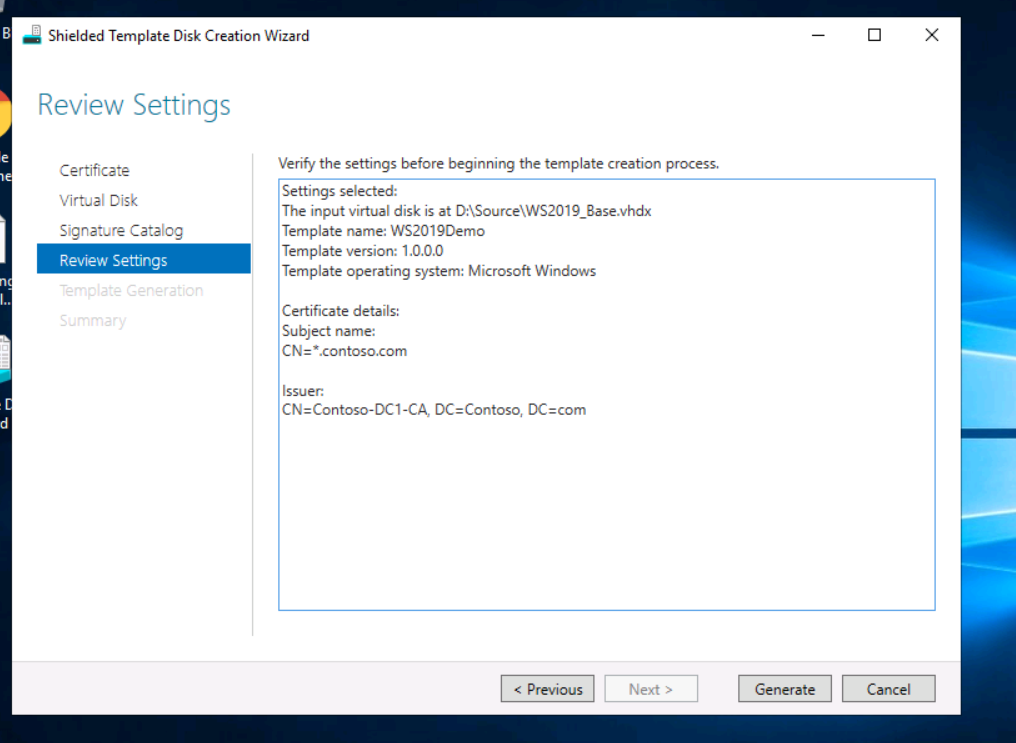
Select **Next**.



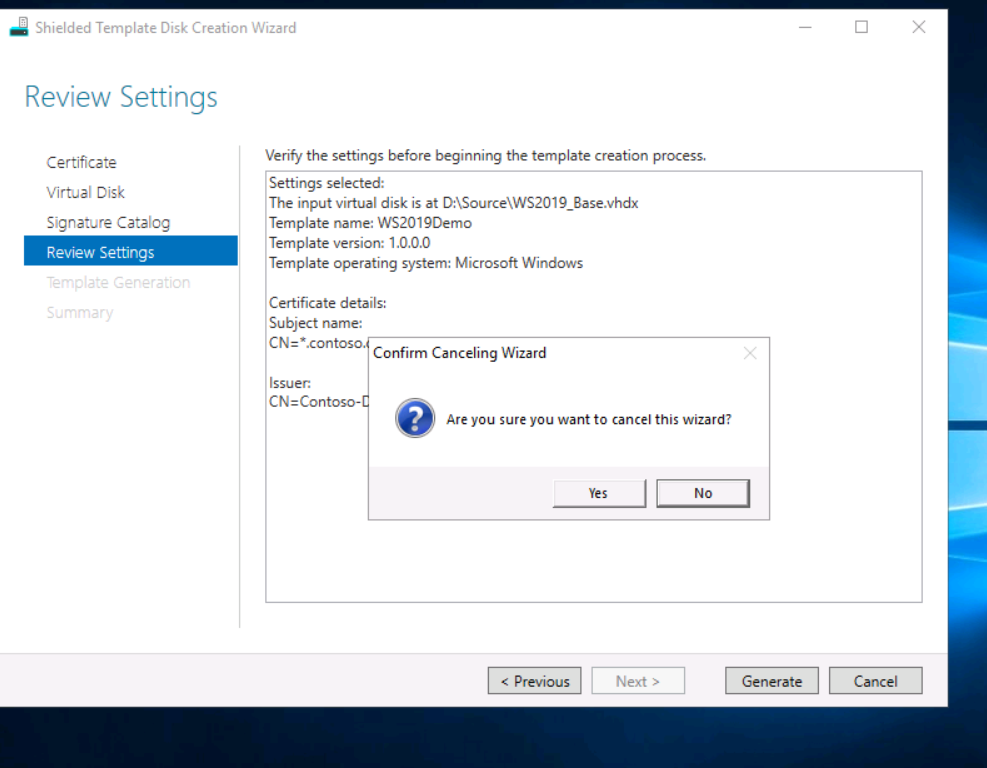
On the Signature Catalog page, in Disk name, enter WS2019Demo, and then in version, enter 1.0.0.0.



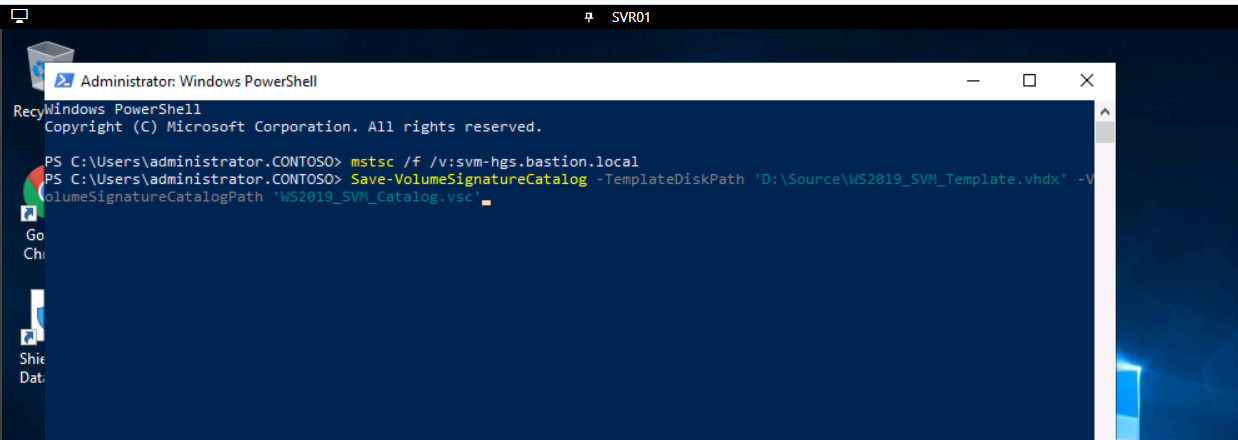
Select **Next**, and then review the settings.



Cancel the wizard.



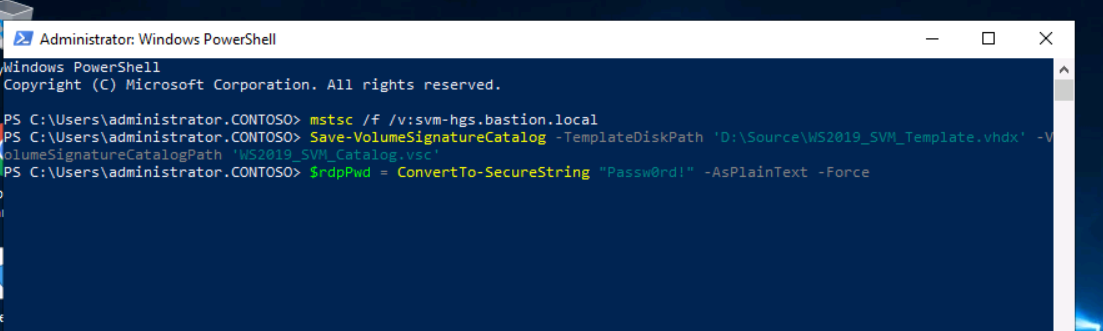
Run the following command to extract the volume signature catalog from the encrypted disk.



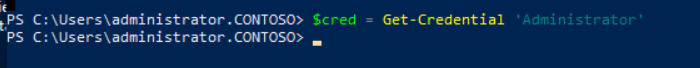
**Step 3: Create an unattend.xml file:**

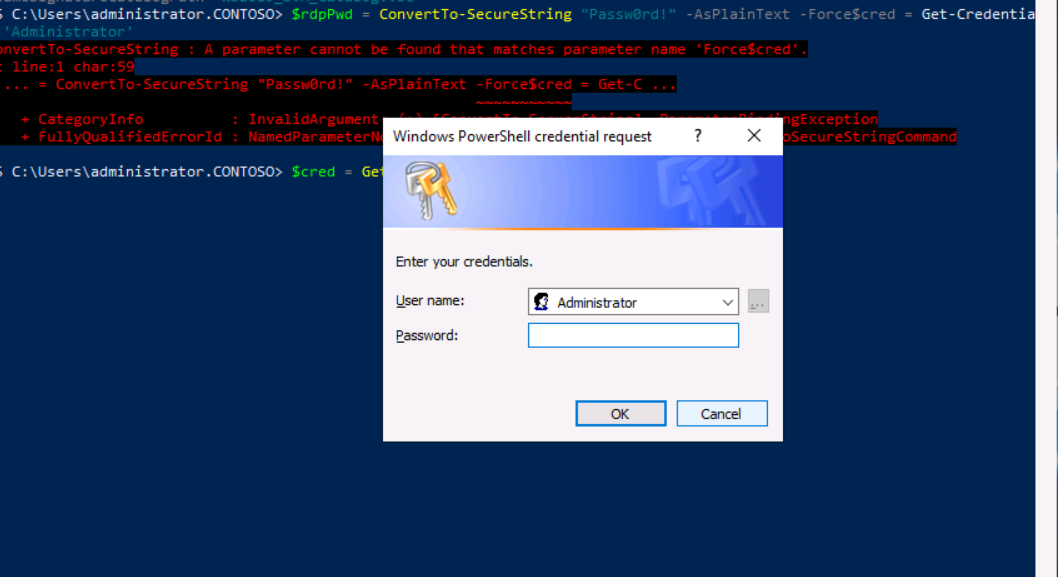
Because we will be using a generalized, sysprepped operating system image to deploy a shielded virtual machine, you may want to use an operating system specialization answer file, also known as unattend.xml, to configure the installation on first boot. Because creating an answer file for shielded virtual machines can be challenging, you can use the New-ShieldingDataAnswerFile Windows PowerShell function to simplify the creation of the answer file. The unattend.xml file, along with (optionally) other artifacts, is packaged into a shielded data (PDK) file to allow you to create the shielded virtual machines from templates.

On **SRV01**, in Windows PowerShell, run the following command to convert a plain text password to a secure string and store it in a variable.



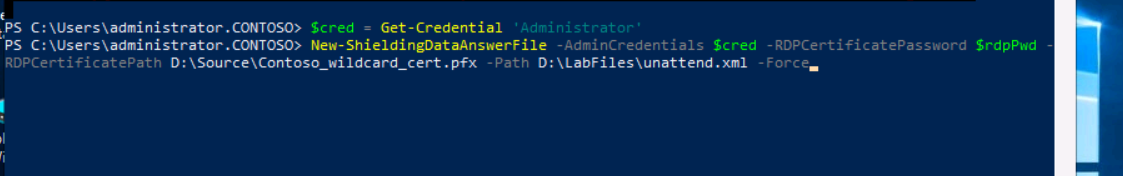
Run the following command to create a variable to store the administrator credentials.

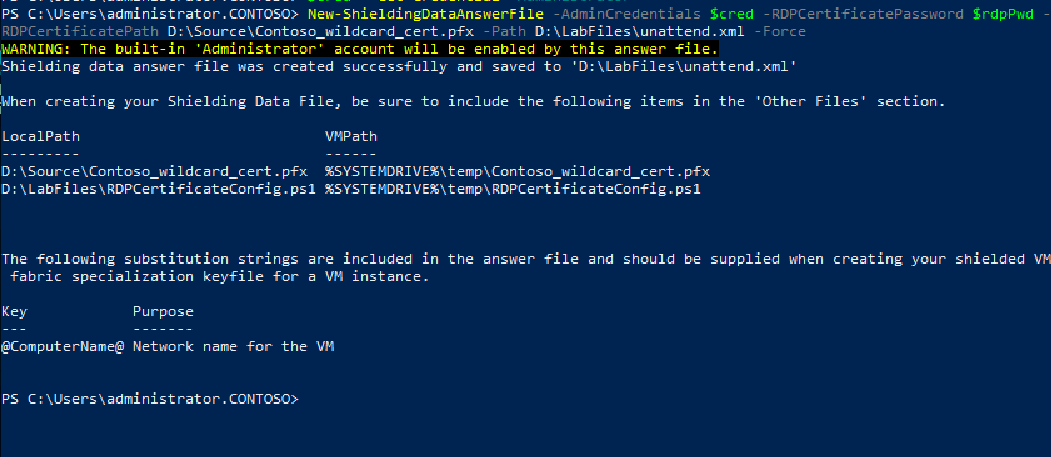




When prompted, enter Passw0rd! as the password.

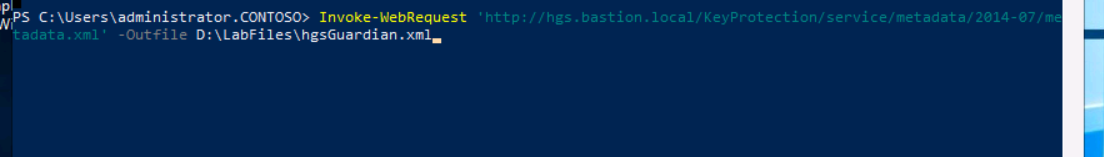
Run the following command to generate an attend.xml file to configure the shielded virtual machine on first boot.

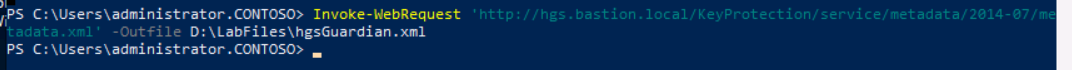




We will download HGS guardian metadata from the HGS server as an XML file. The HGS guardian, described in the XML file, is added to a Key Protector when you create a shielding data file. The Key Protector is then used to shield the virtual machine, ensuring that the shielded virtual machine will start only after the guarded host is able to successfully attest against the HGS server.

Run the following command to download the guardian metadata and save the file.





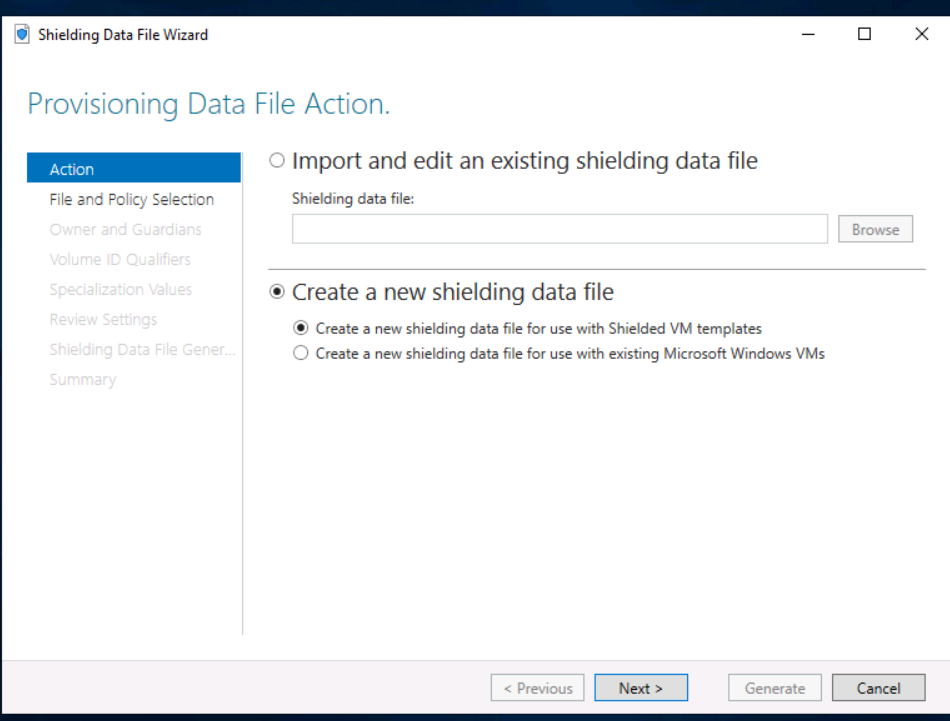
**Step 4: Generate a shielding data file:**

We will generate a shielding data file, also known as a provisioning data file (PDK). A PDK is an encrypted file that contains all of the information necessary to deploy a new shielded virtual machine—for example, a Windows Setup answer file, a certificate for RDP, and approved disk signatures. The PDK file provides assurance that a virtual machine is deployed exactly as the tenant owner specifies. The fabric administrator cannot view or modify the contained elements required for deployment—such as the answer file, the certificates, the domain join credentials, and other sensitive information that must remain confidential. Furthermore, because of the use of signed disks, the hard drive specified for the deployment cannot be substituted.

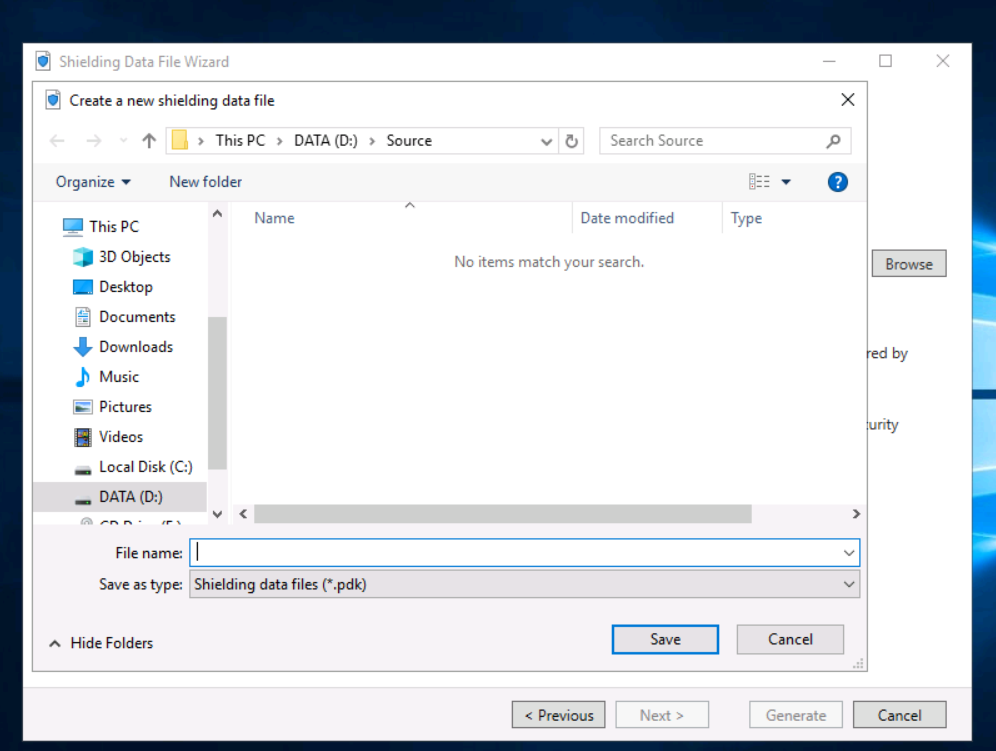
On the desktop of **SVR01**, open the **Shielding Data File wizard**.



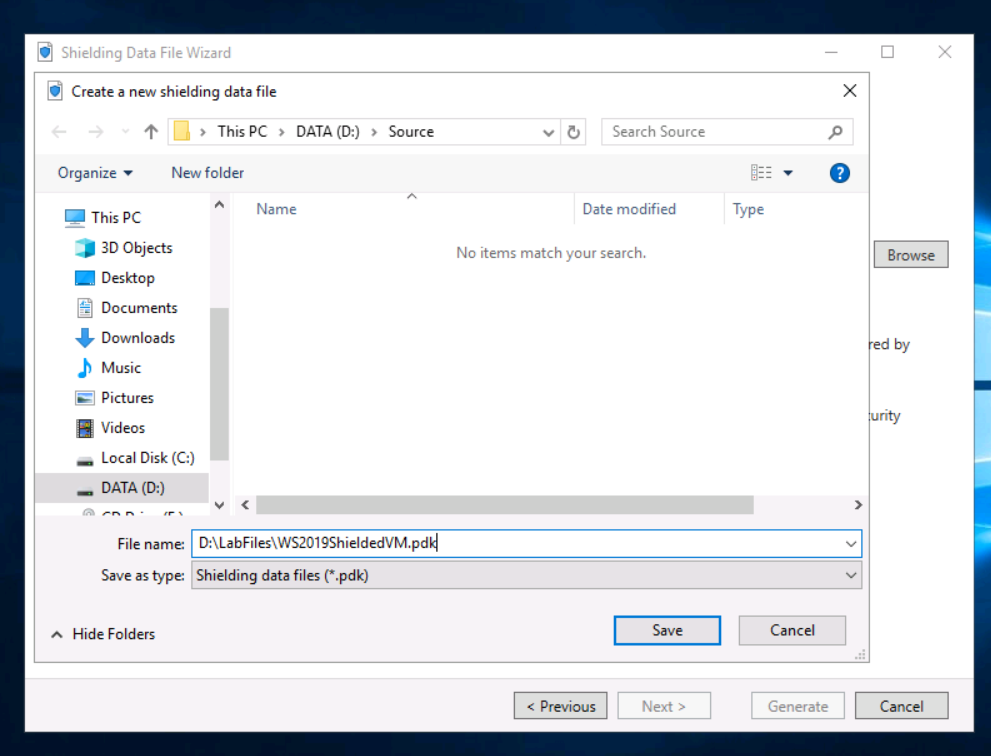
In Shielding data file, ensure that **Create a New Data File** is selected, select **Create a new shielding data file for use with Shielded VM templates**, and then select **Next**.



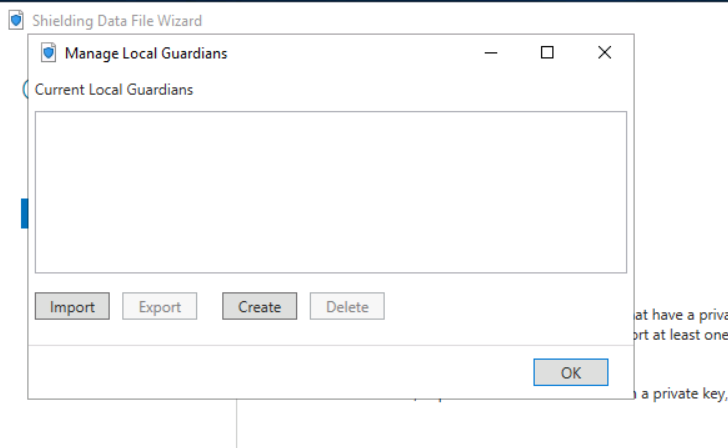
On the File and Policy Selection page, select **Browse**.



In the Create a new shielding data file dialog box, in File name, enter D:\LabFiles\WS2019ShieldedVM.pdk, select **Save**, and then select **Next**.

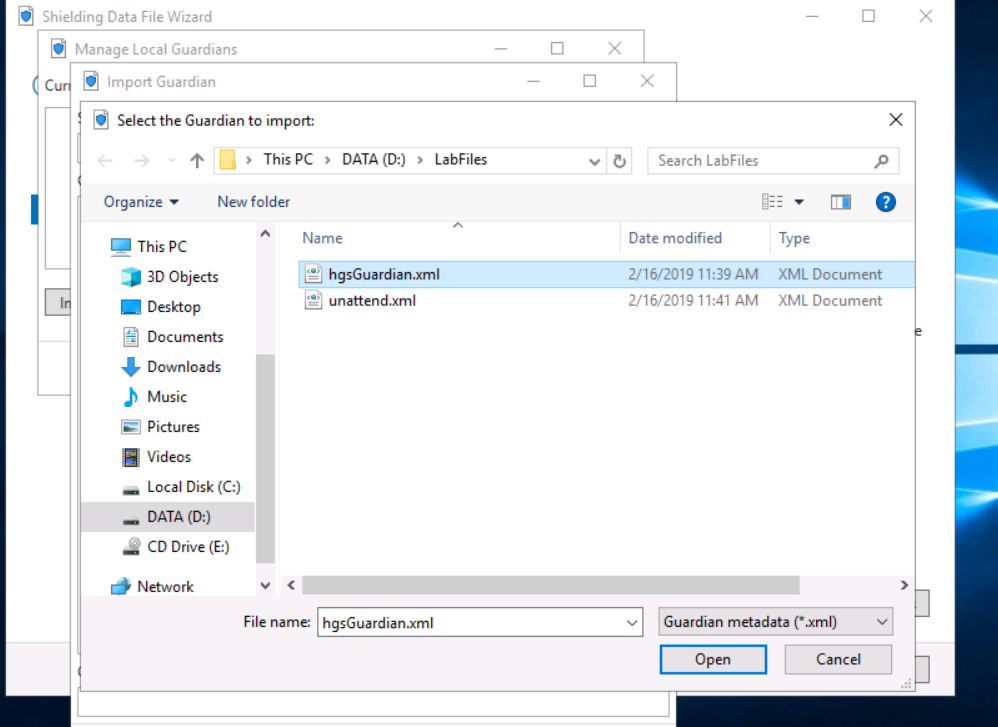


On the Owner and Guardians page, select **Manage Local Guardians**.

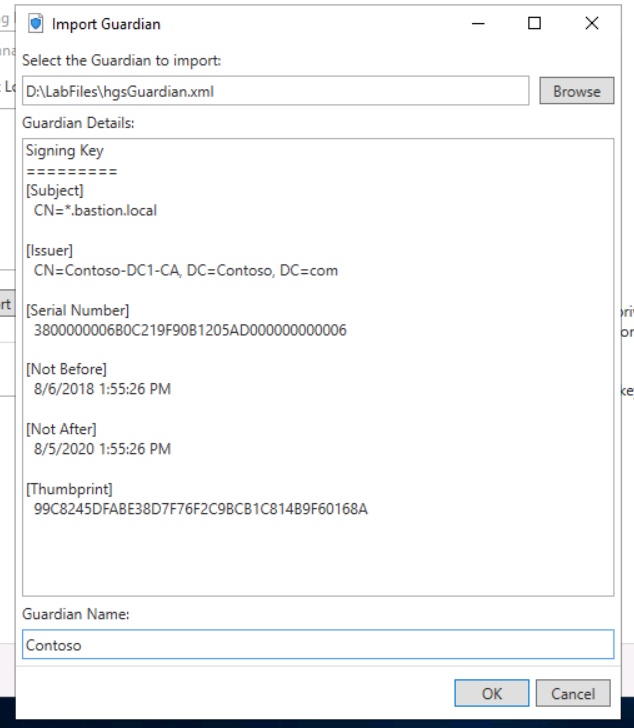


In the Current Local Guardians dialog box, select **Import**.

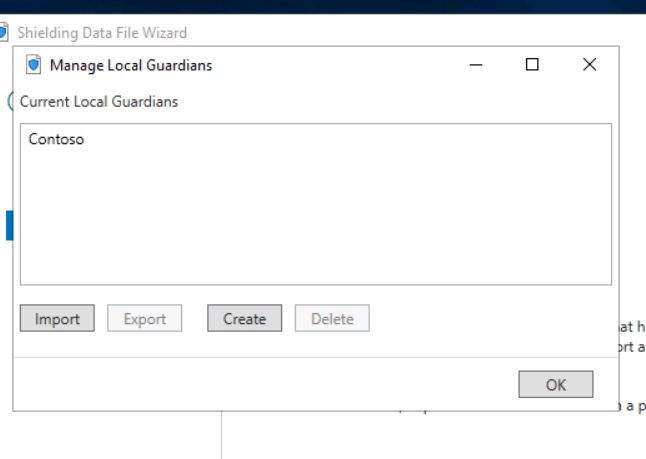
In the Import Guardian dialog box, select **Browse**, select **hgsGuardian.xml**, and then select **Open**.



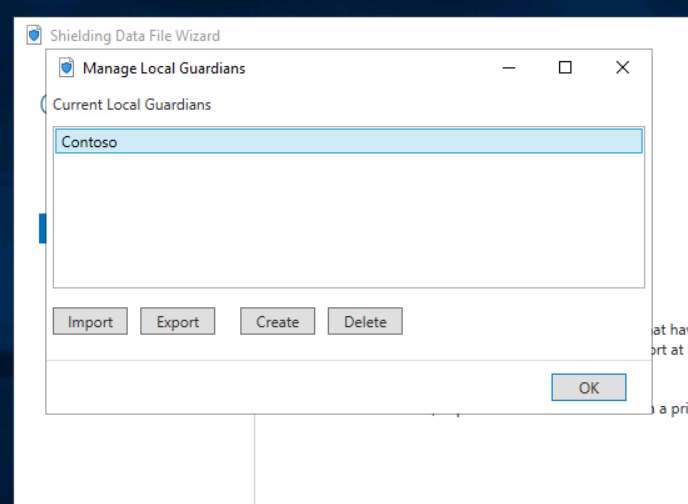
In the Import Guardian dialog box, in Guardian Name, enter Contoso, and then select **OK**.



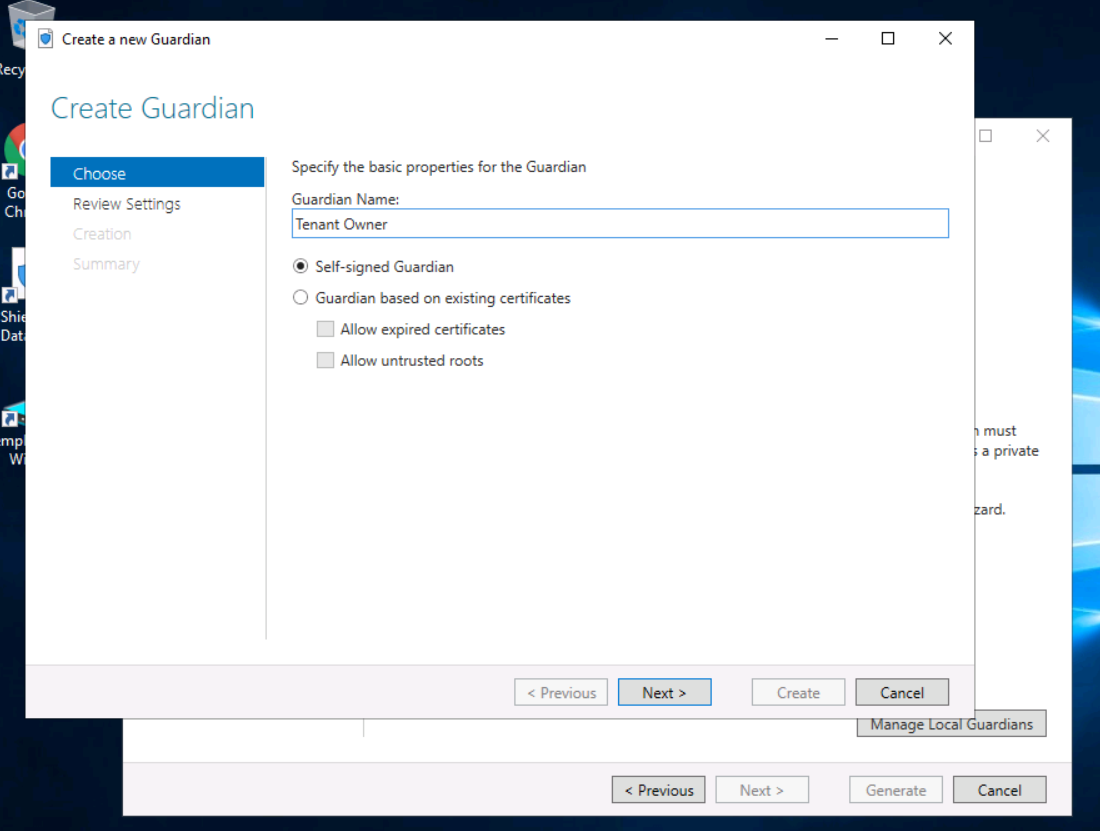
Wait until the name Contoso appears in the Manage Local Guardians dialog box.



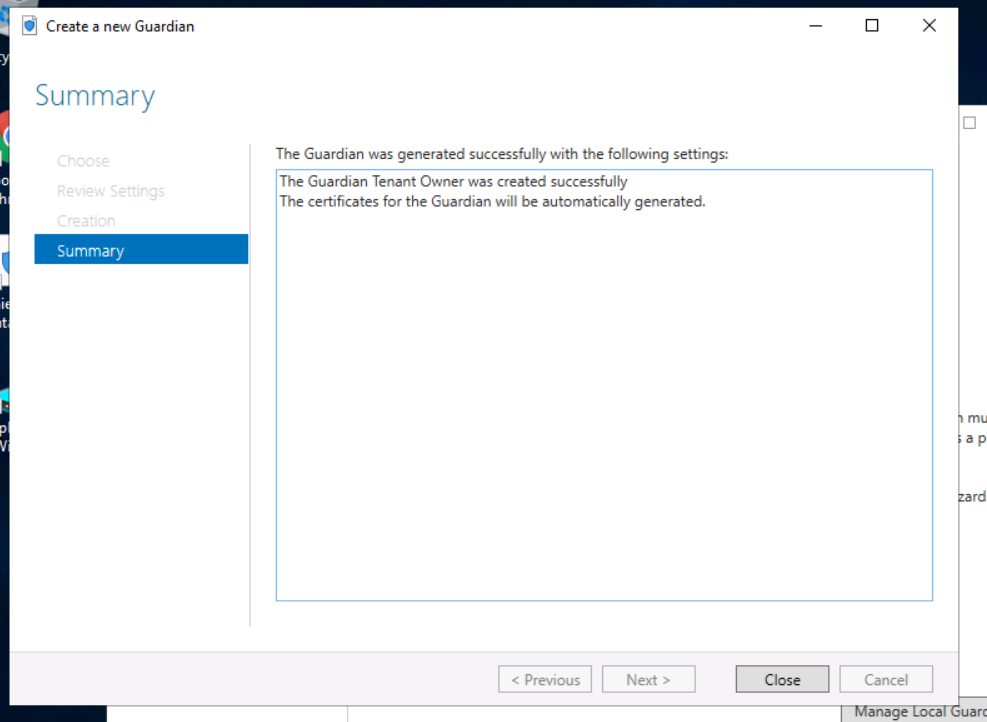
In the Manage Local Guardians dialog box, select **Contoso**, and then select **Create** to launch the Create a new Guardian wizard.



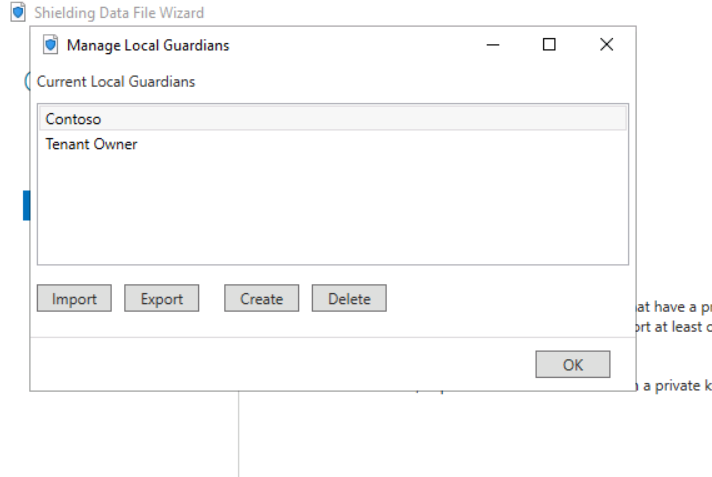
On the Create Guardian page, in Guardian Name, enter Tenant Owner, and then select **Next**.



On the Review Settings page, select **Create**, and then select **Close**.



In the Manage Local Guardians dialog box, select **OK**.

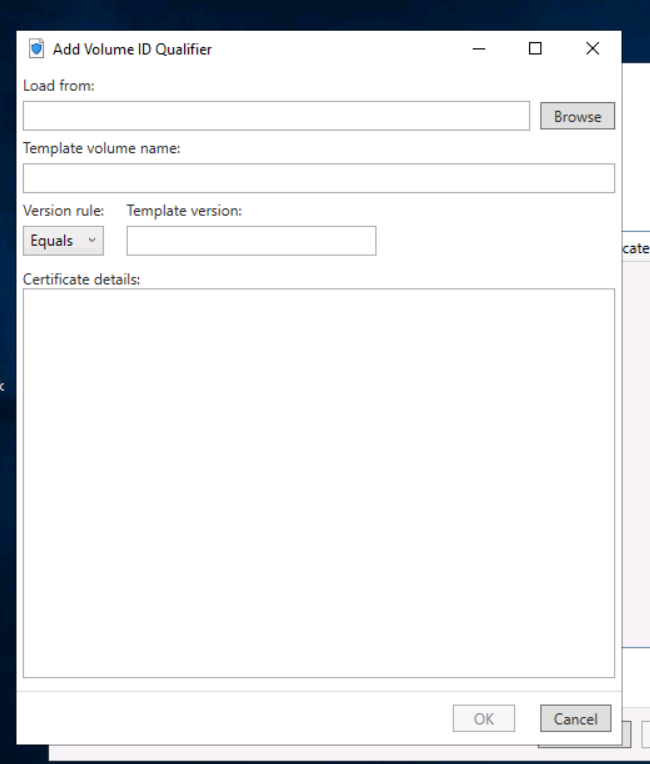


Wait a few moments for the Owners and Guardians page to refresh.

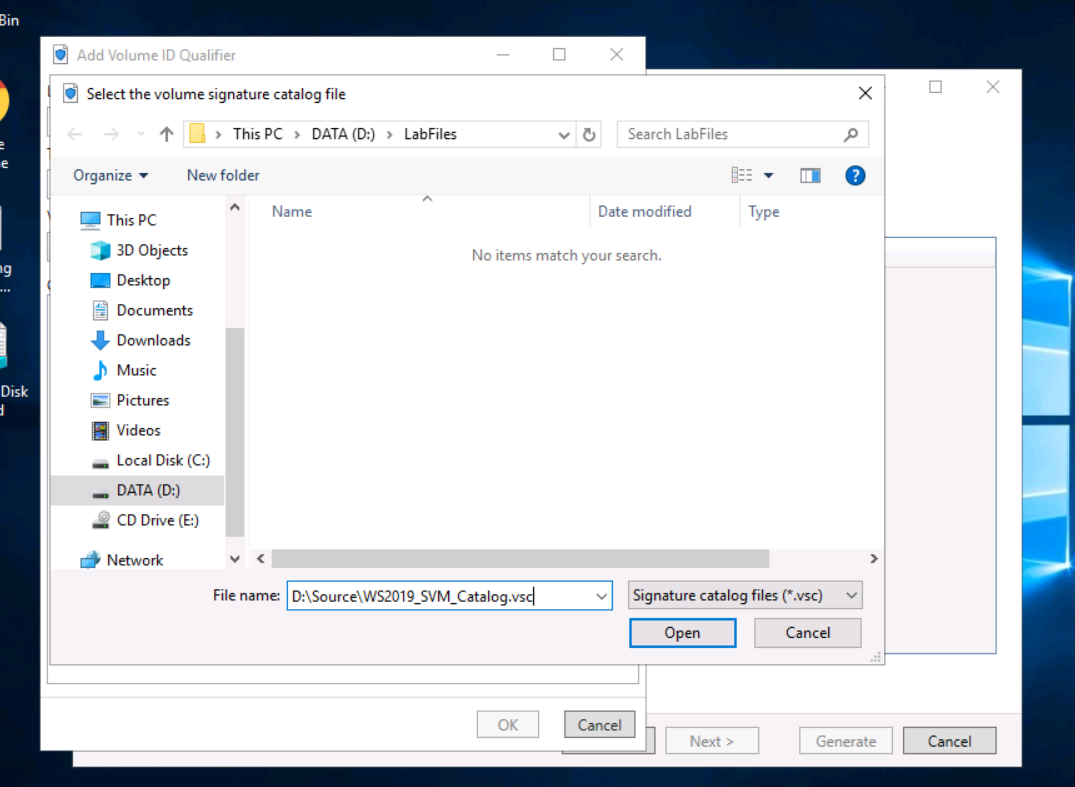
In Select the owner for the shielding data file, select **Tenant Owner**, in Select any guardians, select **Contoso**, and then select **Next**.



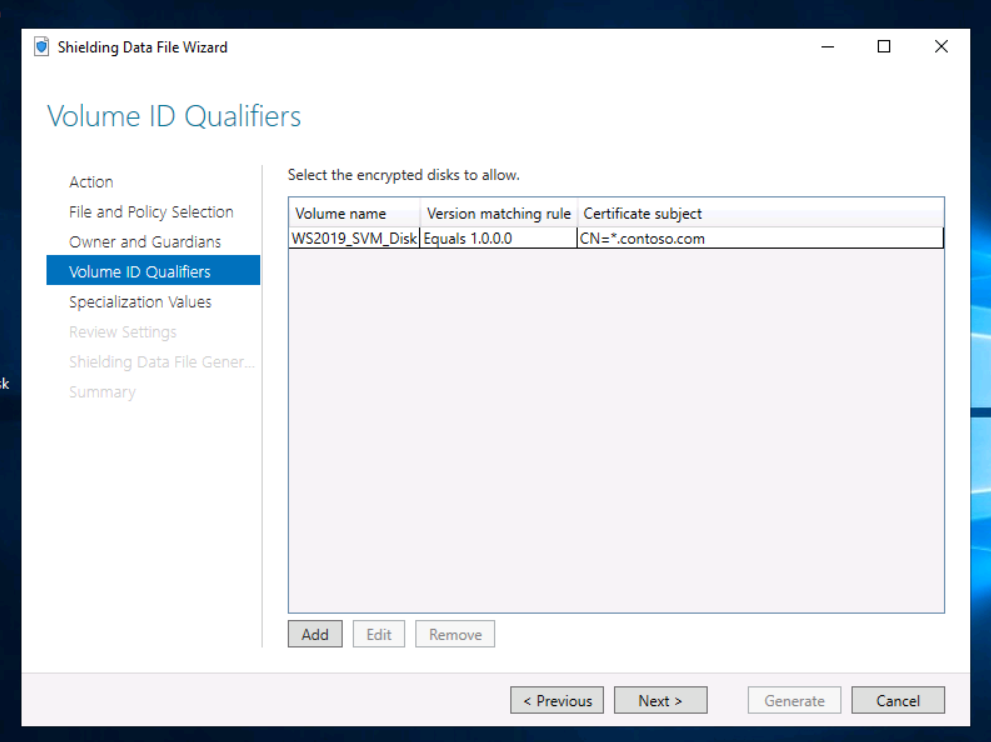
On the Volume ID Qualifiers page, select **Add**.



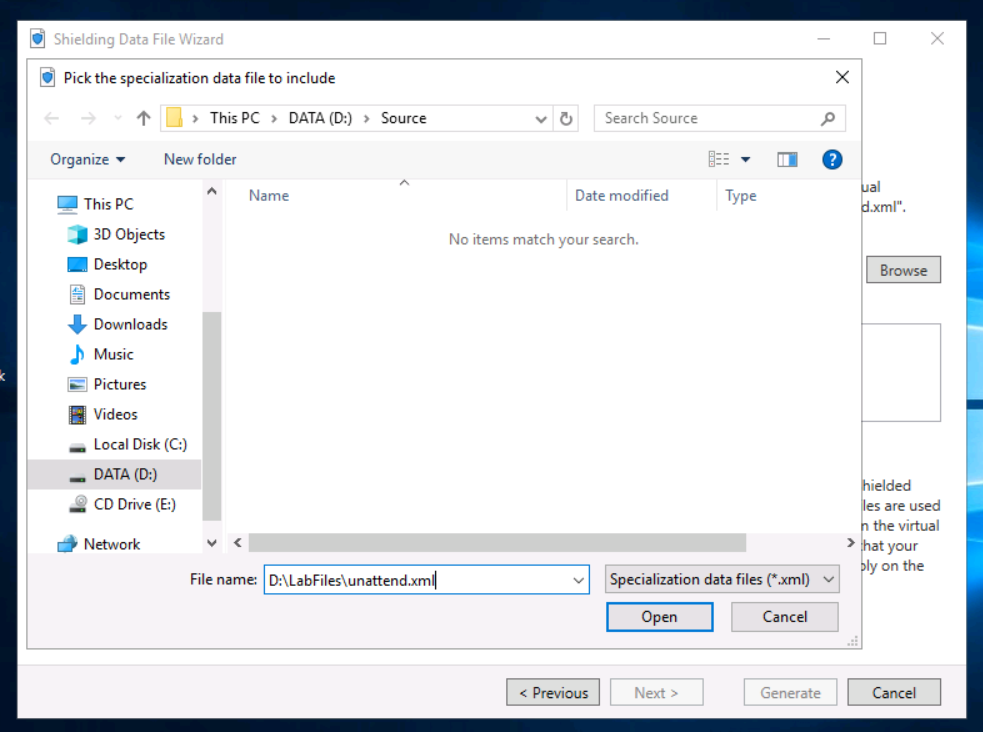
In the Add Volume ID Qualifier, select **Browse**.



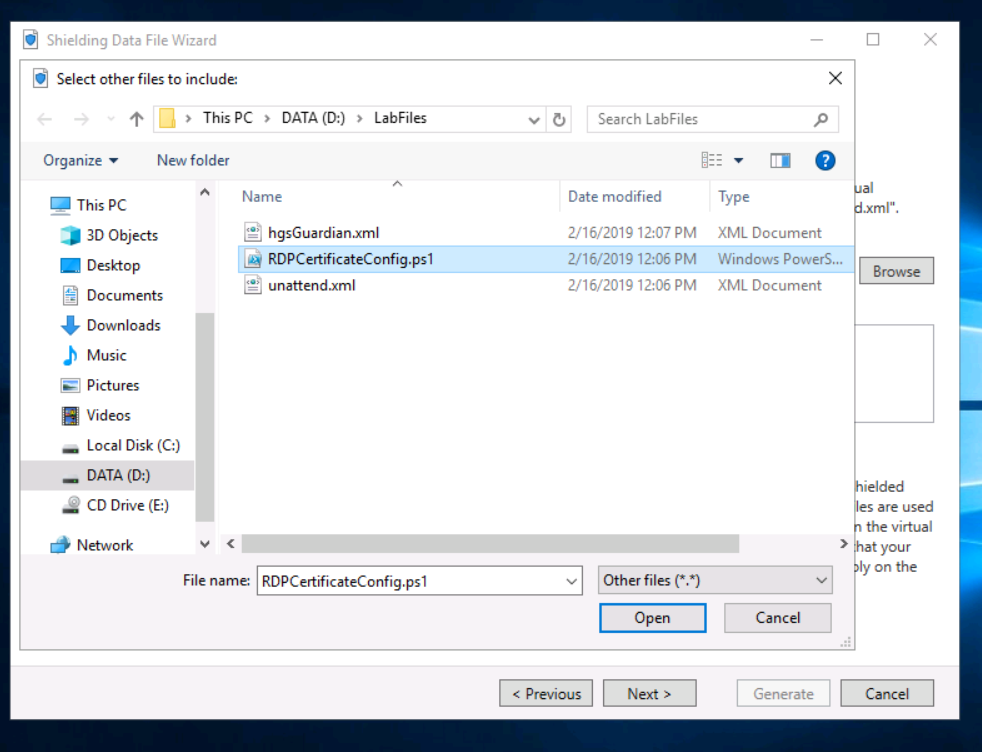
Select **Next** to advance the wizard.



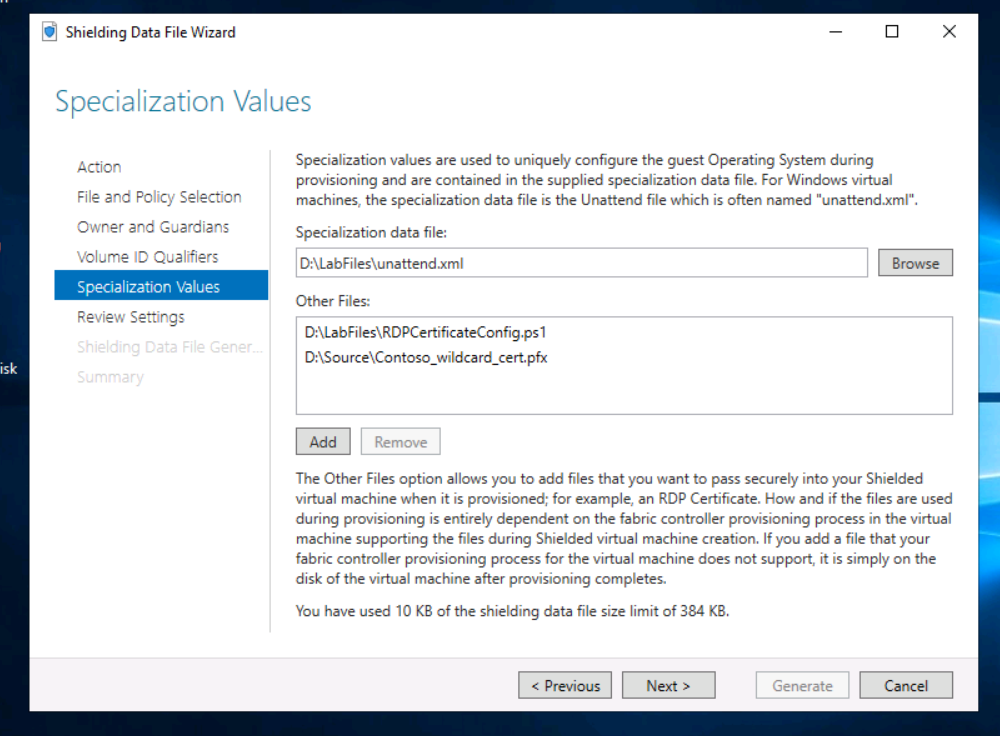
In Specialization data file, select **Browse**.



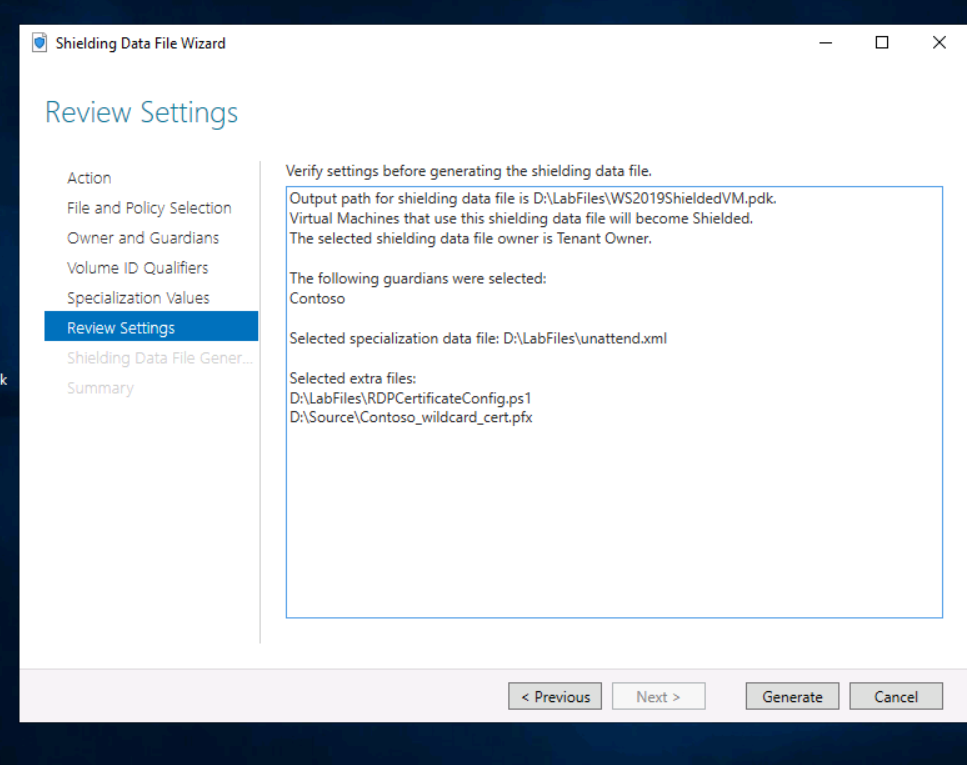
In Other files, select **Add**. Select **RDPCertificateConfig.ps1**, and then select **Open**



In Other files, select **Add**. In the dialog box, in File Name, enter D:\Source\Contoso\_wildcard\_cert.pfx.

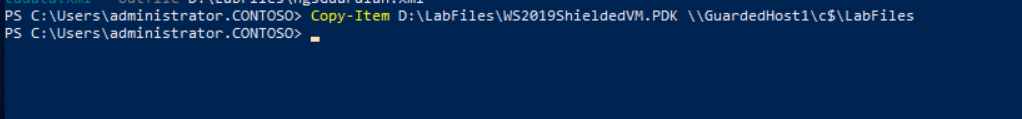


Select **Next**, review the settings, and then select **Generate**.



Select **Close** to close the wizard.

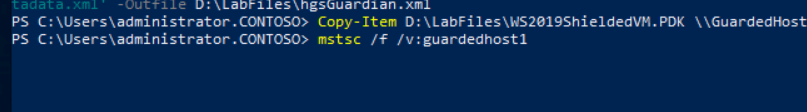
On **SVR01**, run the following command to copy the PDK file to the guarded host in preparation for deploying the shielded virtual machine.

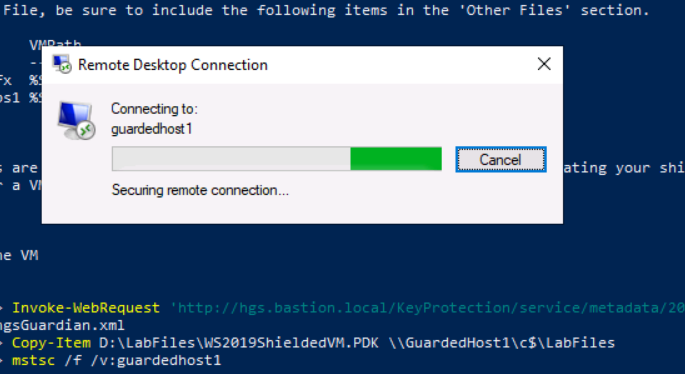


**Step 5: Deploy a Windows virtual machine:**

We will deploy a new shielded virtual machine by using your shielding data files and the template VHD that you created earlier in this lab.

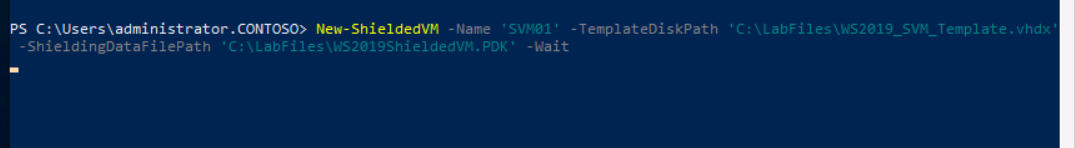
Restore the RDP session for **GuardedHost1**.





On **GuardedHost1**, open Windows PowerShell, if not already open.

Run the following command to deploy the shielded virtual machine.

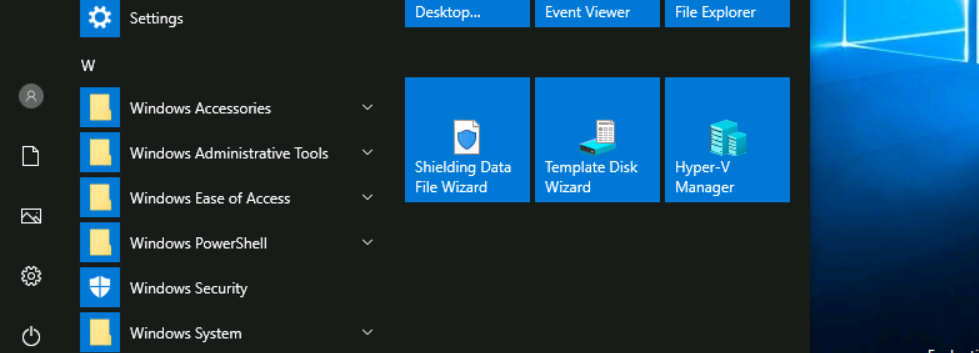


Wait until the output from the Windows PowerShell command indicates that the provisioning job is complete, and then minimize the remote desktop connection to GuardedHost1.

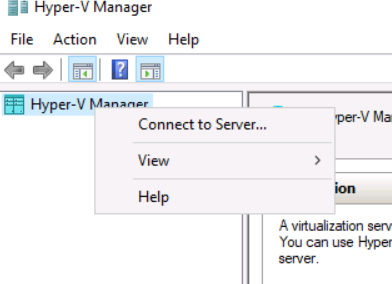
**Step 6: Verify shielded virtual machine security:**

We will verify the shielded virtual machine security. We will verify that the fabric administrator cannot gain access to the virtual machine in any way. Note that it is theoretically possible for HGS administrators to access the shielded virtual machine if they have access to both HGS and the fabric. As long the organization maintains strict role separation, and your fabric administrators and HGS administrators are separate sets of people, neither group has access to breach the shielded virtual machine while it is in the guarded fabric.

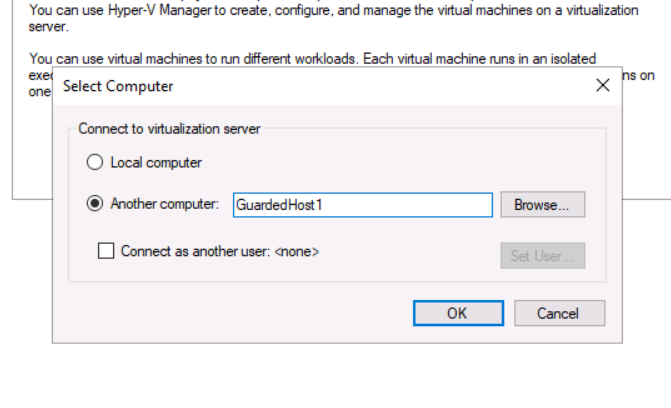
On **SVR01**, on the Start menu, open **Hyper-V Manager**.

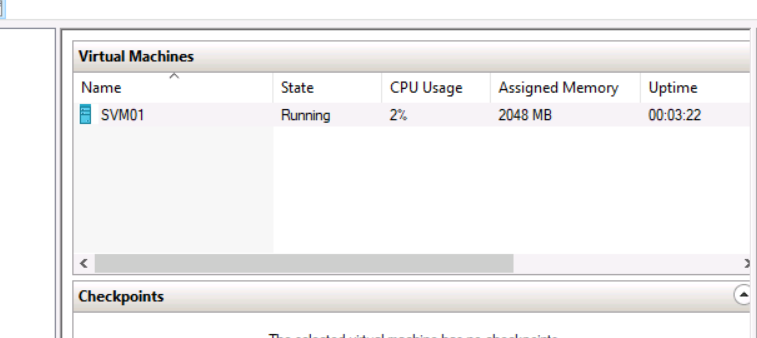


In Hyper-V manager, right-click **Hyper-V Manager**, and then select **Connect to Server**.

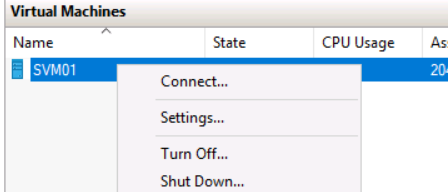


In the Select Computer dialog box, enter GuardedHost1, and then select **OK**.

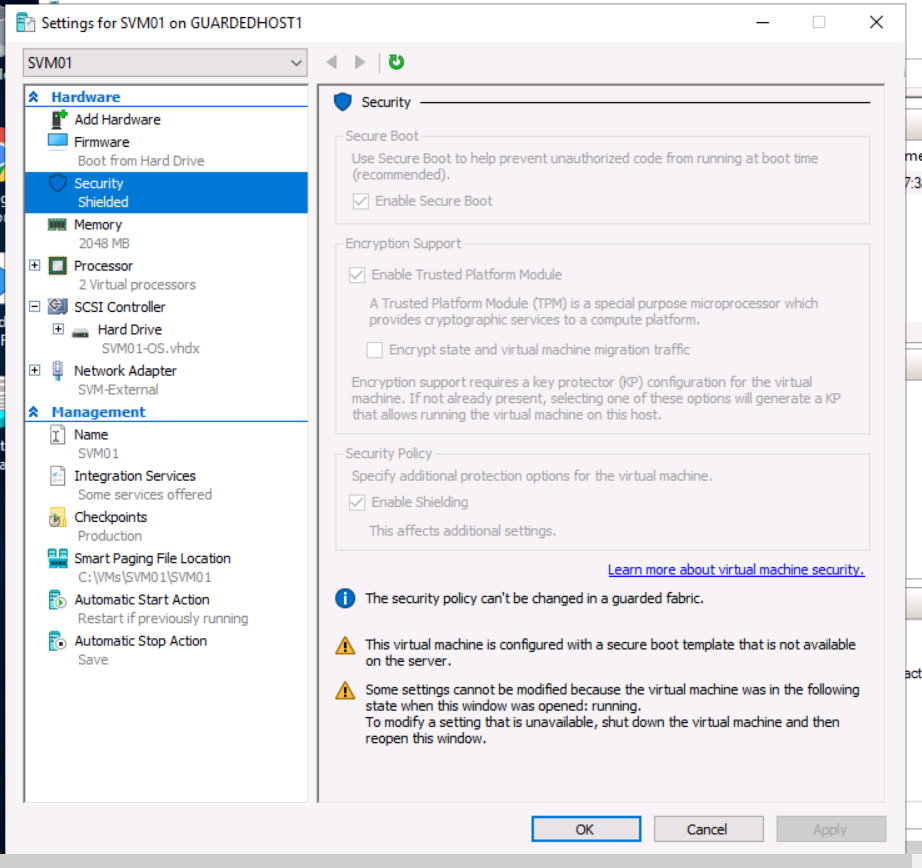




Wait until SVM01 has shut down, right-click **SVM01**, and then select **Settings**.

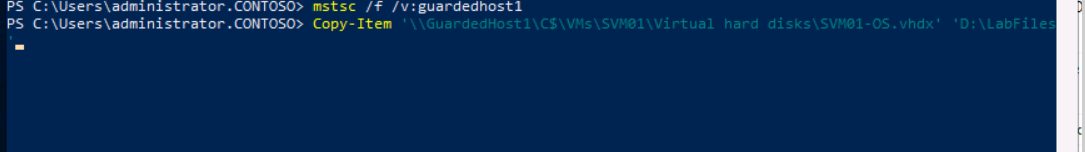


In the Settings for SVM01 on GUARDEDHOST1 dialog box, select **Security**.

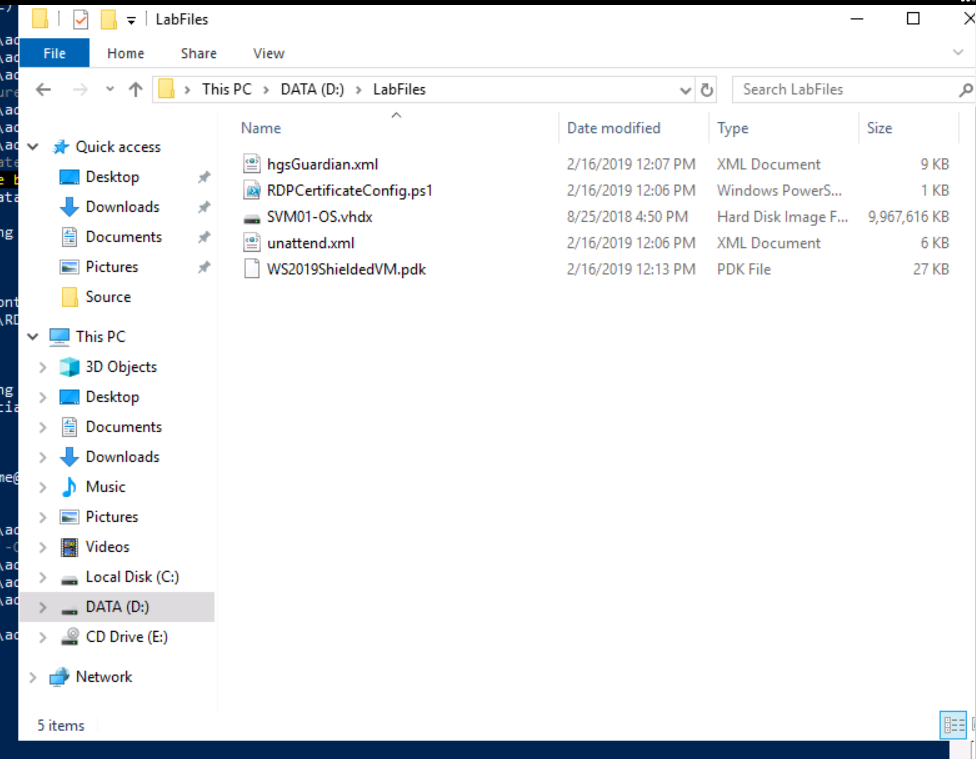


In the Settings for SVM01 on GUARDEDHOST1 dialog box, select **Cancel**.

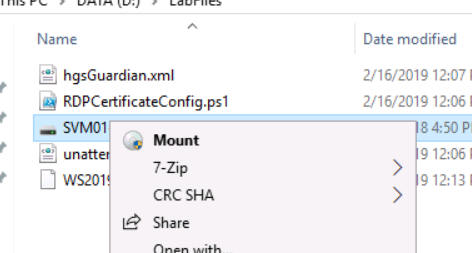
In Windows PowerShell, run the following command to copy the .vhdx file from GuardedHost1

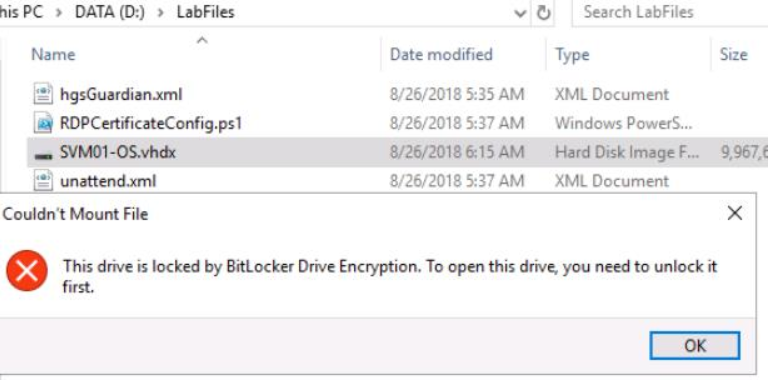


Open **File Explorer**, and then go to **D:\LabFiles**.

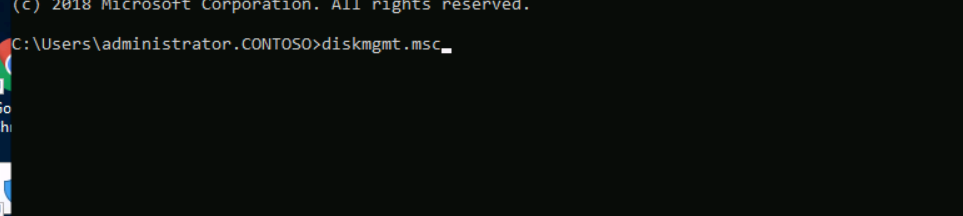


Right-click **SVM01-OS.vhdx**, and then select **Mount**.

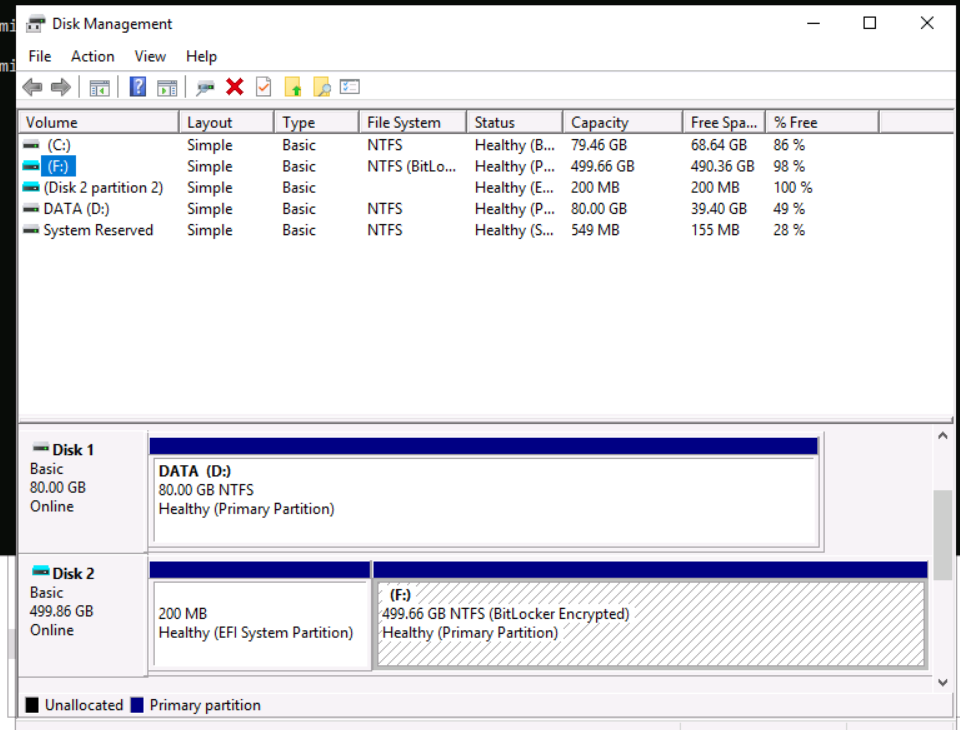




Run the following command to open the Disk Management console.

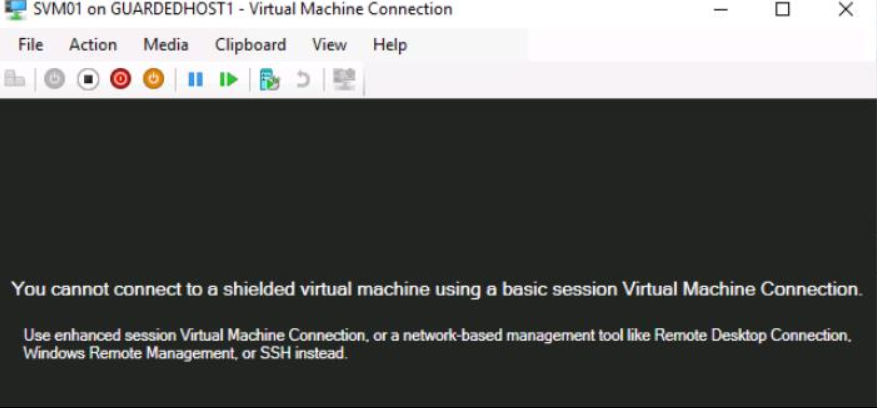


In the Disk Management console, select **(F:)**.



Switch to Hyper-V manager, right-click **SVM01**, and then select **Start**.

Wait until the virtual machine has started, and then double-click **SVM01** to connect to it.



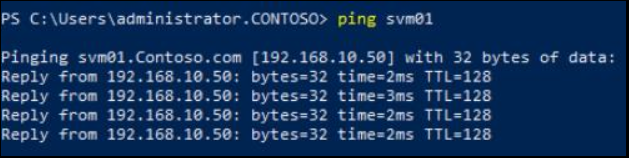
Run the following command to verify the IP address of SVM01

Ping 192.168.10.50

Run the following command to add a resource record for the IP address of SVM01.

Add-DnsServerResourceRecordA -ComputerName DC1 -Name "SVM01" -ZoneName "contoso.com" -IPv4Address "192.168.10.50" -PassThru

cmd ping SVM01



Run the following command to establish a remote desktop session with SVM01. When prompted, enter Passw0rd!as the password.

mstsc /f /v:svm01.contoso.com

Implement shielded VM on Windows Server 2019 is one of the common administrative and security concerns for hosters and tenants is the amount of access that fabric administrators have to the virtual machines running on the fabric in the datacenter. To mitigate this potential risk, it is now possible configure shielded virtual machines that provide a high degree of protection against potential threats posed by compromised fabric administrators. In this lab, you will learn about the end-to-end configuration of a guarded fabric for hosters and hosting workloads on that fabric for tenant administrators by using Trusted Platform (TPM) attestation with Windows Server 2019 and System Center 2016 - Virtual Machine Manager. In the first part of this lab, you will assume the role of a tenant and learn the process for created a shielded virtual on the guarded fabric that has been created for the lab. In the second part of the lab, you will assume the role of the fabric and Host Guardian Service (HGS) administrators and perform administrative tasks related to those respective roles, including provisioning guarded hosts and create template VHDs for use with shielded virtual machines.

Launch