

Deploying Shielded Virtual Machines – Part3

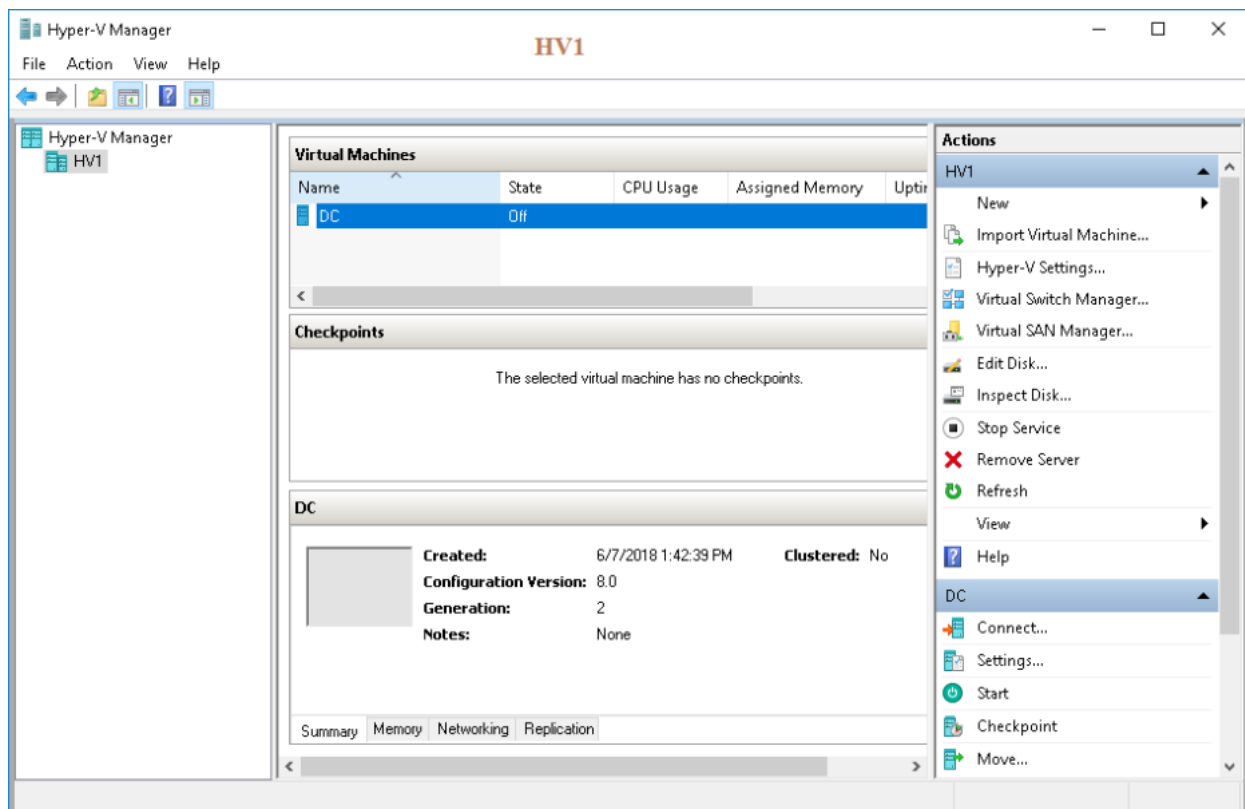
 michaelfirsov.wordpress.com/deploying-shielded-virtual-machines-part3

June 19, 2018

Part2

Part 3: Deploying shielded VM

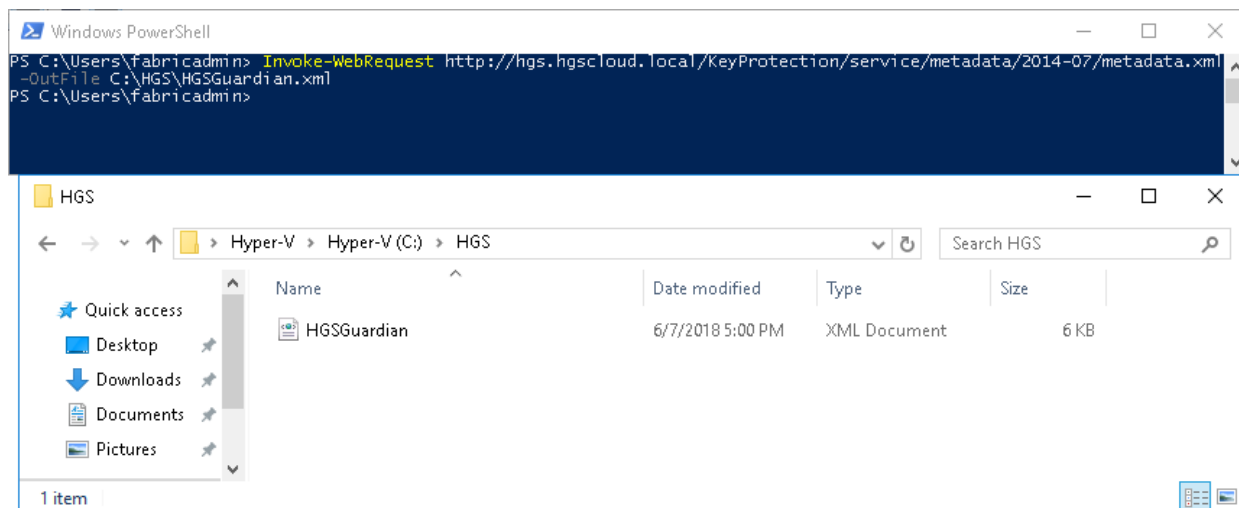
Once the HGS service and guarded fabric are in place I can move on to the final step of this test deployment – shielding the existing virtual machine(s). The high-level steps for this procedure includes configuring the virtual machine on some other Hyper-V host – MS calls such hosts the *tenant* Hyper-V hosts – exporting and importing it to some guarded host. In my network there're two guarded hosts – Host1 and Host2 – and two tenant Hyper-V hosts – HV1 and HV2. So the next steps will be done on my **HV1** host (I'll repeat the final test on HV2 at the end of this post).



Please note that the VM (DC in this case) must be stopped before it can be secured.

1) First off I retrieve HGS guardian metadata from the HGS server:

Invoke-WebRequest <http://hgs.hgsccloud.local/KeyProtection/service/metadata/2014-07/metadata.xml> -OutFile C:\HGS\HGSGuardian.xml

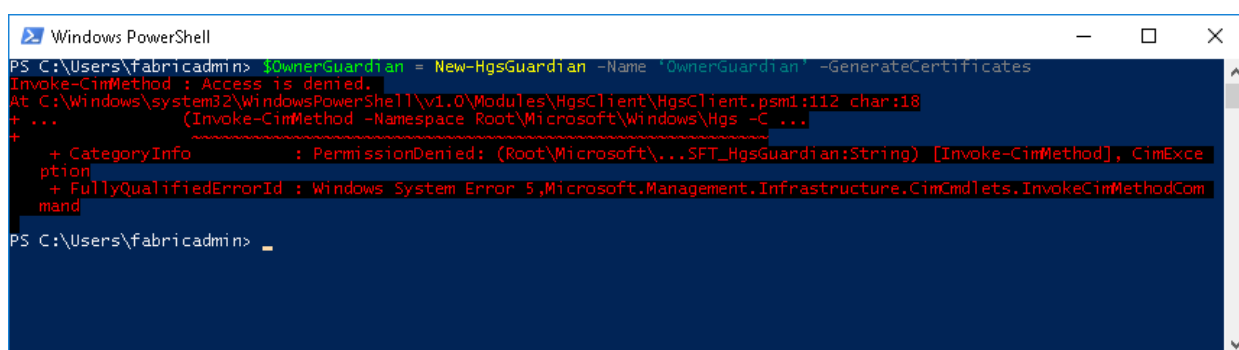


Advertisements

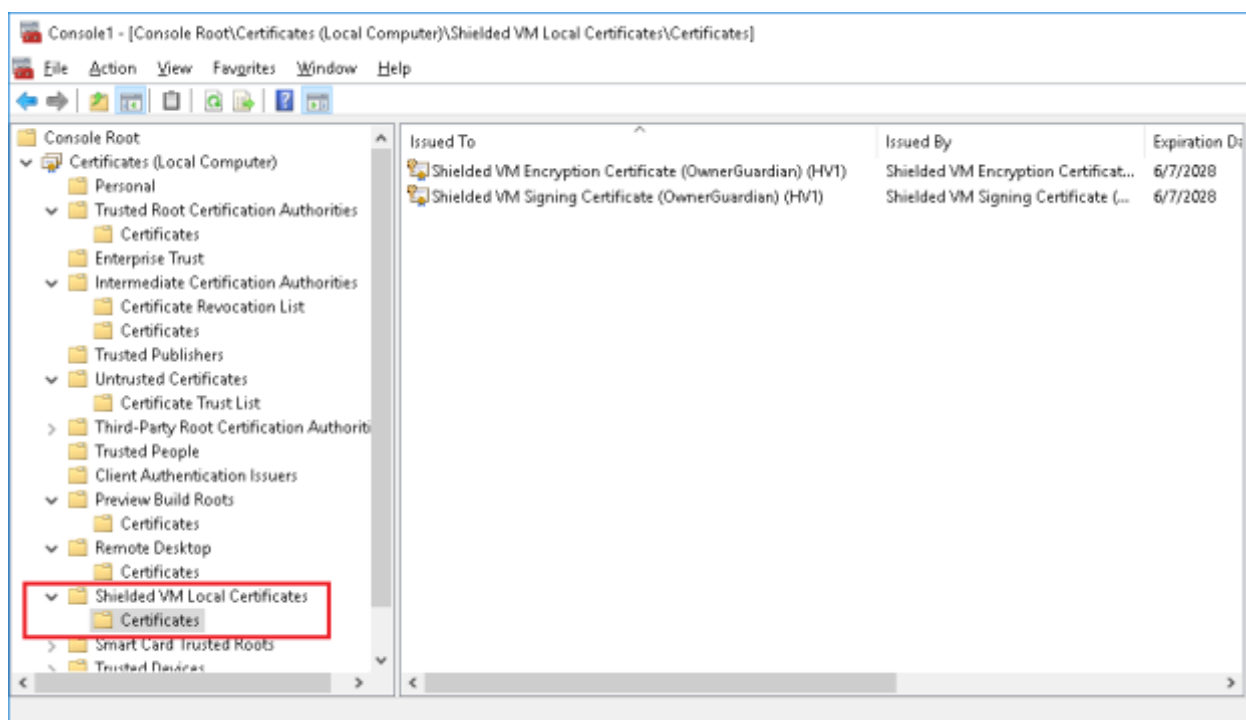
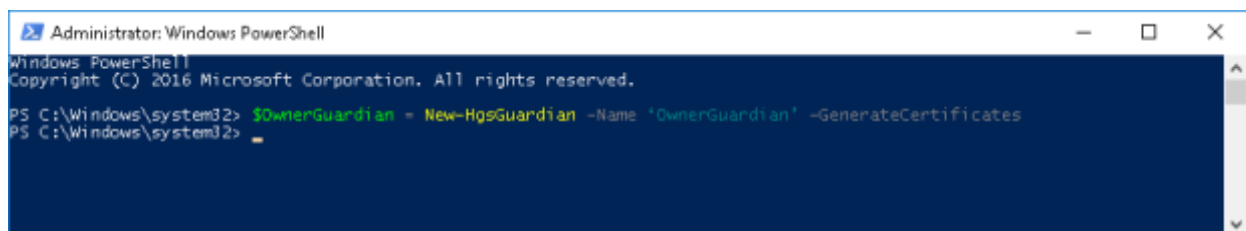
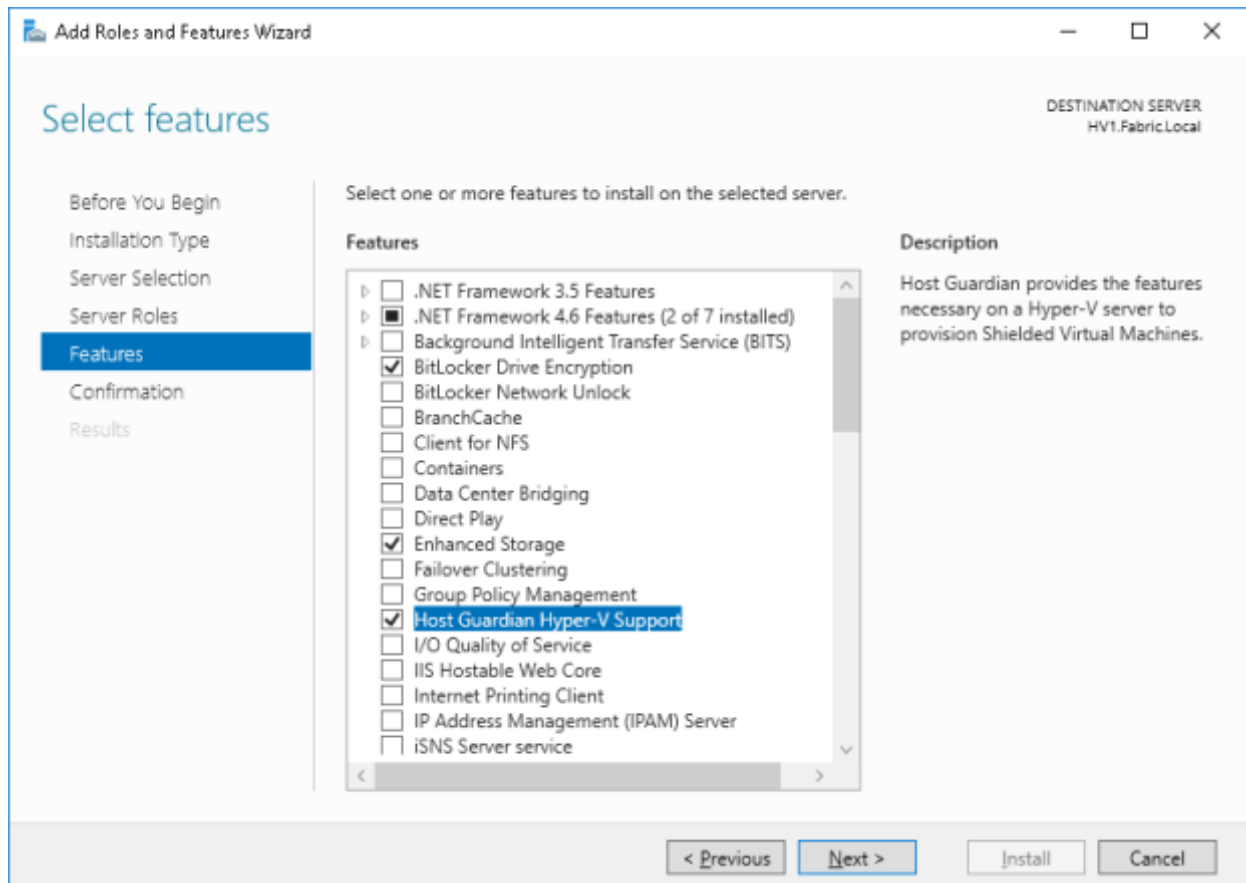
Report this adPrivacy

2) Then let's create the new guardian object that will serve as the VM's owner using the new self-signed certificates:

```
$OwnerGuardian = New-HgsGuardian -Name 'OwnerGuardian' -GenerateCertificates
```



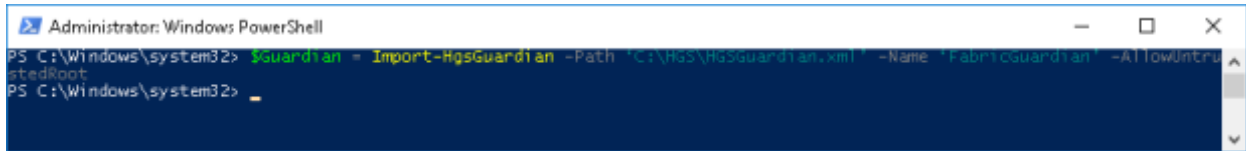
??? It is because HGS Service also needs to be installed on the tenant host:



3) Create another guardian object by importing the HGS guardian

```
$Guardian = Import-HgsGuardian -Path 'C:\HGS\HGSGuardian.xml' -Name  
'FabricGuardian' -AllowUntrustedRoot
```

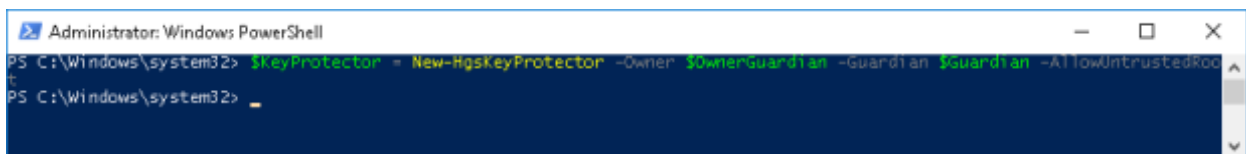
-AllowUntrustedRoot must be used because we are using self-signed certificates.



```
Administrator: Windows PowerShell  
PS C:\Windows\system32> $Guardian = Import-HgsGuardian -Path 'C:\HGS\HGSGuardian.xml' -Name 'FabricGuardian' -AllowUntrustedRoot  
PS C:\Windows\system32>
```

4) The following command will create the key protector wrapped for the OwnerGuardian and grants access to it to the \$Guardian


```
$KeyProtector = New-HgsKeyProtector -Owner $OwnerGuardian -Guardian $Guardian -  
AllowUntrustedRoot
```



```
Administrator: Windows PowerShell  
PS C:\Windows\system32> $KeyProtector = New-HgsKeyProtector -Owner $OwnerGuardian -Guardian $Guardian -AllowUntrustedRoot  
PS C:\Windows\system32>
```

5) Configure a key protector for the DC virtual machine:

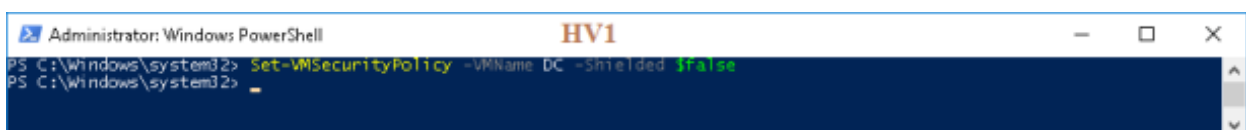
```
Set-VMKeyProtector -VMName DC -KeyProtector $KeyProtector.RawData
```



```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Set-VMKeyProtector -VMName DC -KeyProtector $KeyProtector.RawData  
PS C:\Windows\system32>
```

6) Set the security policy for the DC virtual machine:

```
Set-VMSecurityPolicy -VMName DC -Shielded $false
```



```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Set-VMSecurityPolicy -VMName DC -Shielded $false  
PS C:\Windows\system32>
```

7) Enable vTPM on the DC VM to be able to use it for Bitlocker later:

```
Enable-VMTPM -VMName DC
```

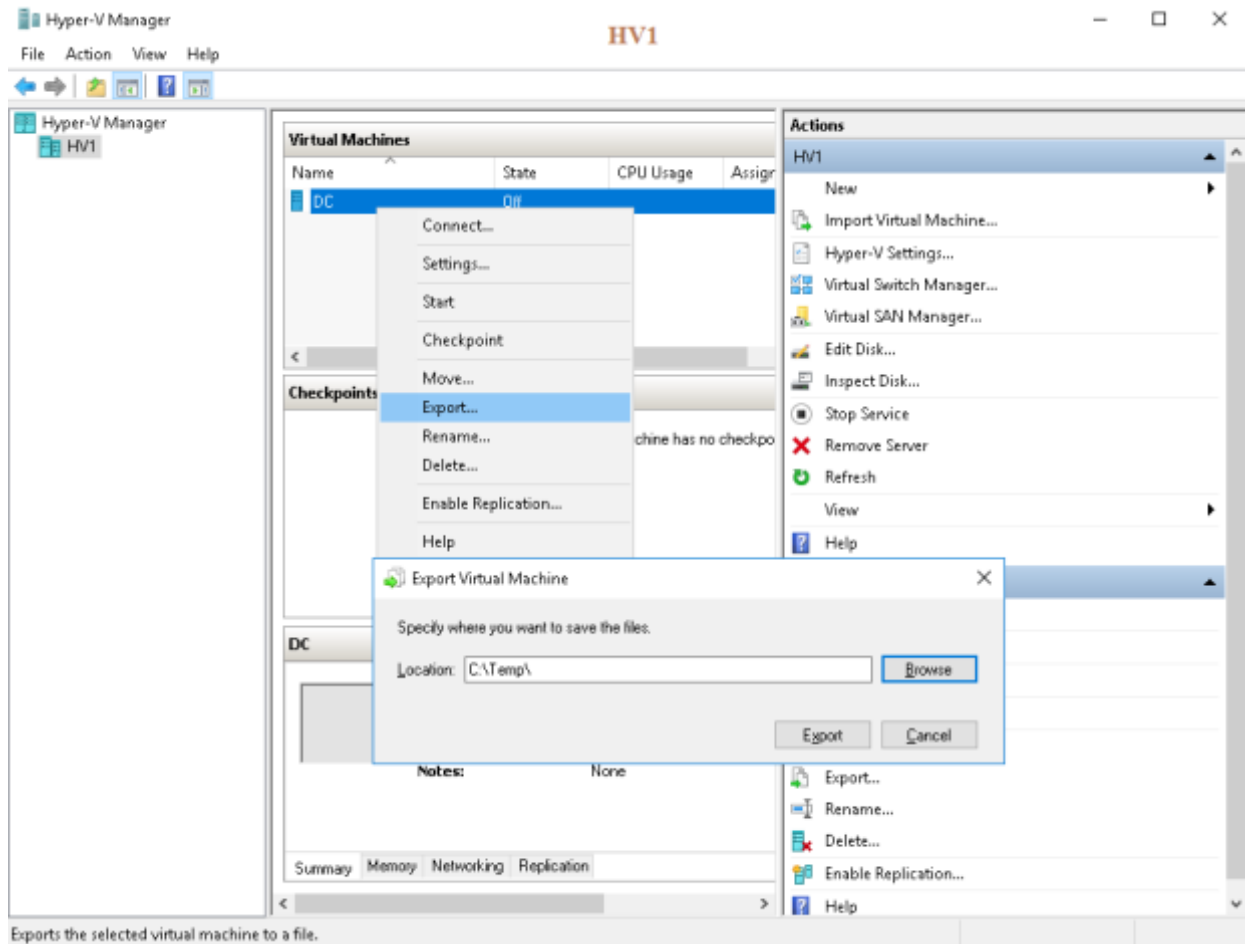


```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Enable-VMTPM -VMName DC  
PS C:\Windows\system32>
```

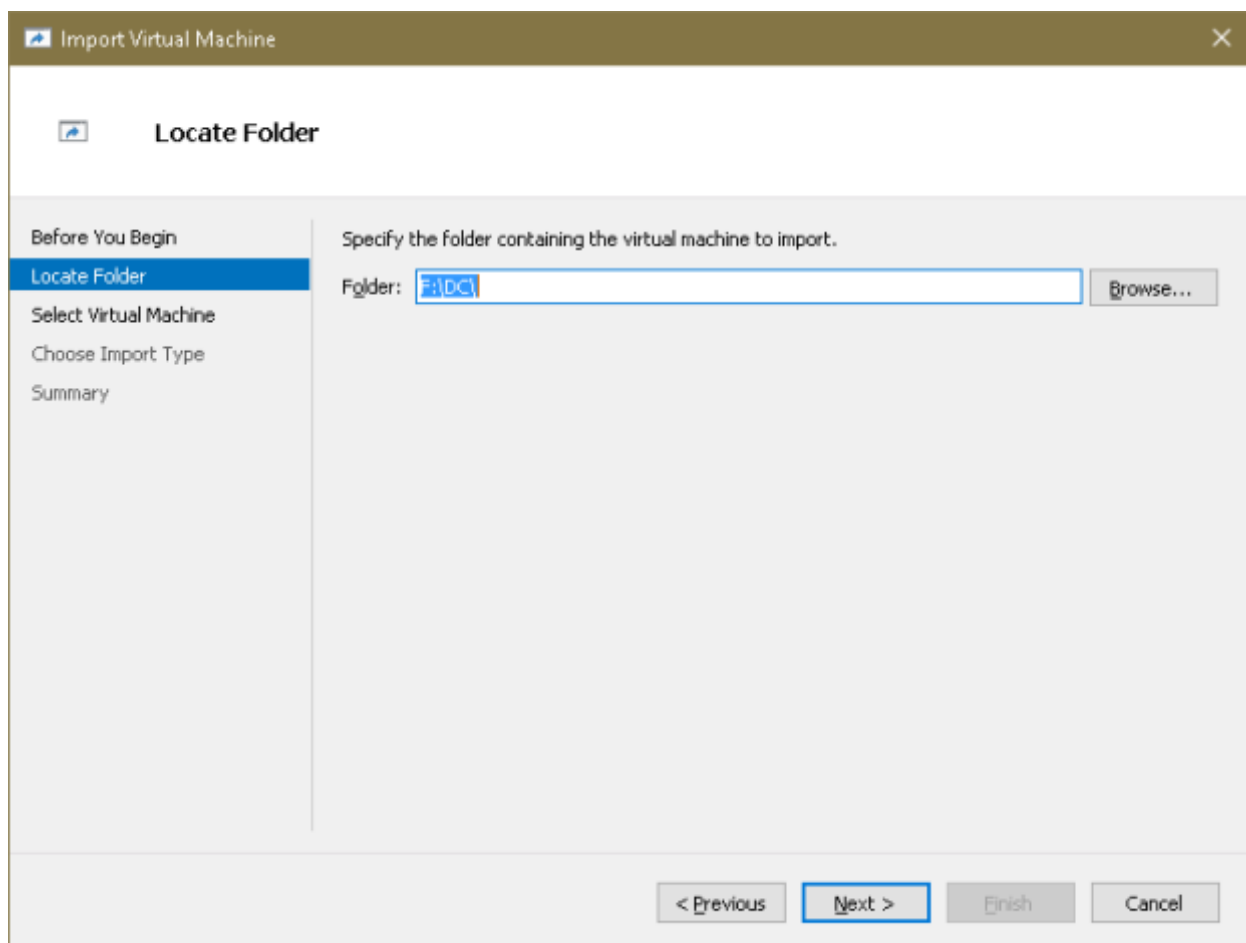
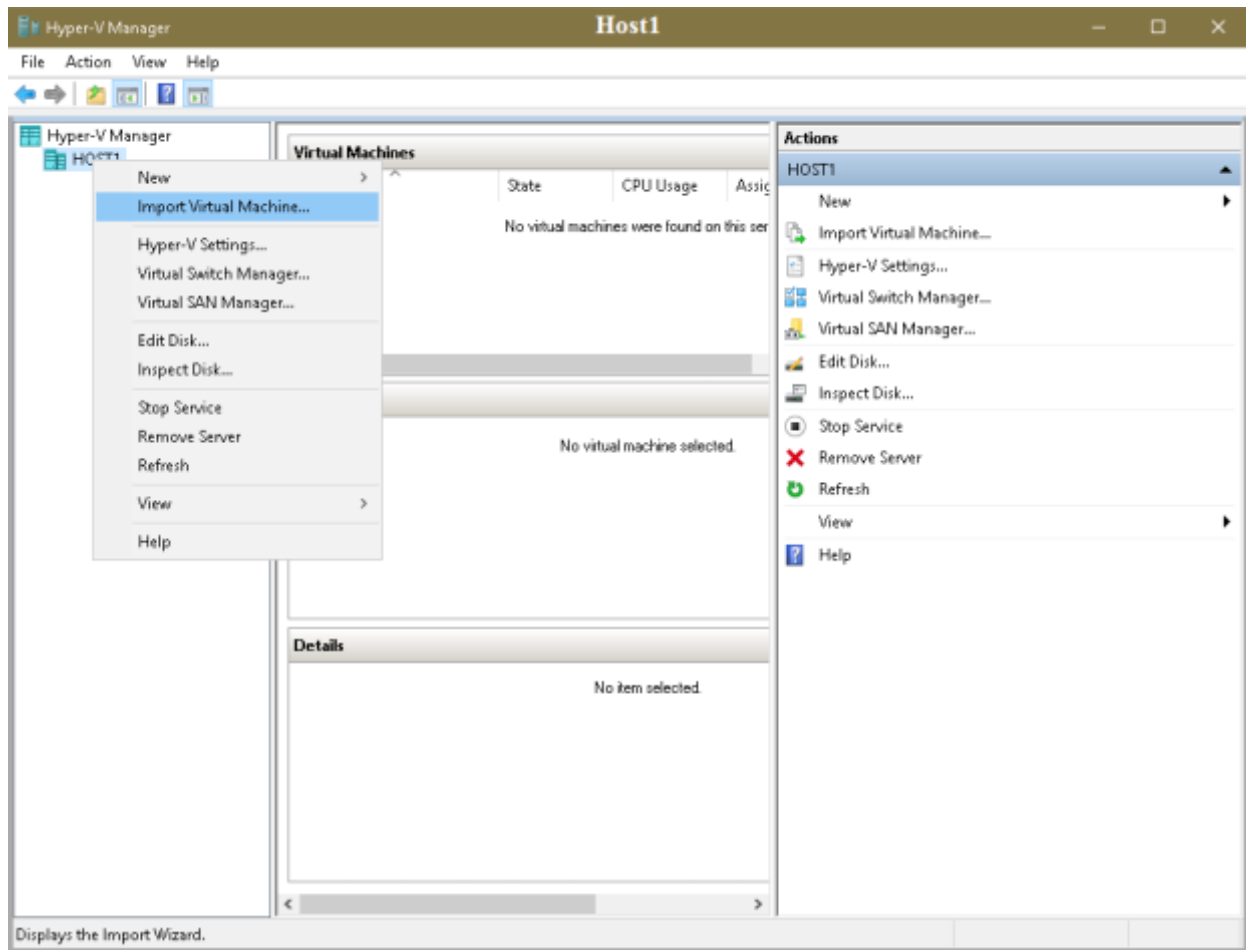
Attention! Before you move a shielded VM to the guarded host it must be prepared for the remote management (WSMan, RDP)! In this test I used the -Shielded \$false vm security policy that means fabric administrators still can access the DC virtual machine because it

has been shielded using **Encryption Supported** mode which permits Hyper-V console connections to the shielded VMs. If I had used -Shielded \$true vm security policy the only way to connect to the DC vm would be via RDP or WSman.

8) Export the DC vm from HV1 Hyper-V host and import it to Host1 which is one of the two guarded hosts.



On Host1 (the guarded host):



Import Virtual Machine

Select Virtual Machine

Before You Begin

Locate Folder

Select Virtual Machine

Choose Import Type

Summary

Select the virtual machine to import:

Name	Date Created
DC	6/7/2018 1:42:39 PM

< Previous

Next >

Finish

Cancel

Import Virtual Machine

Choose Import Type

Before You Begin

Locate Folder

Select Virtual Machine

Choose Import Type

Summary

Choose the type of import to perform:

☒ Register the virtual machine in-place (use the existing unique ID)

☐ Restore the virtual machine (use the existing unique ID)

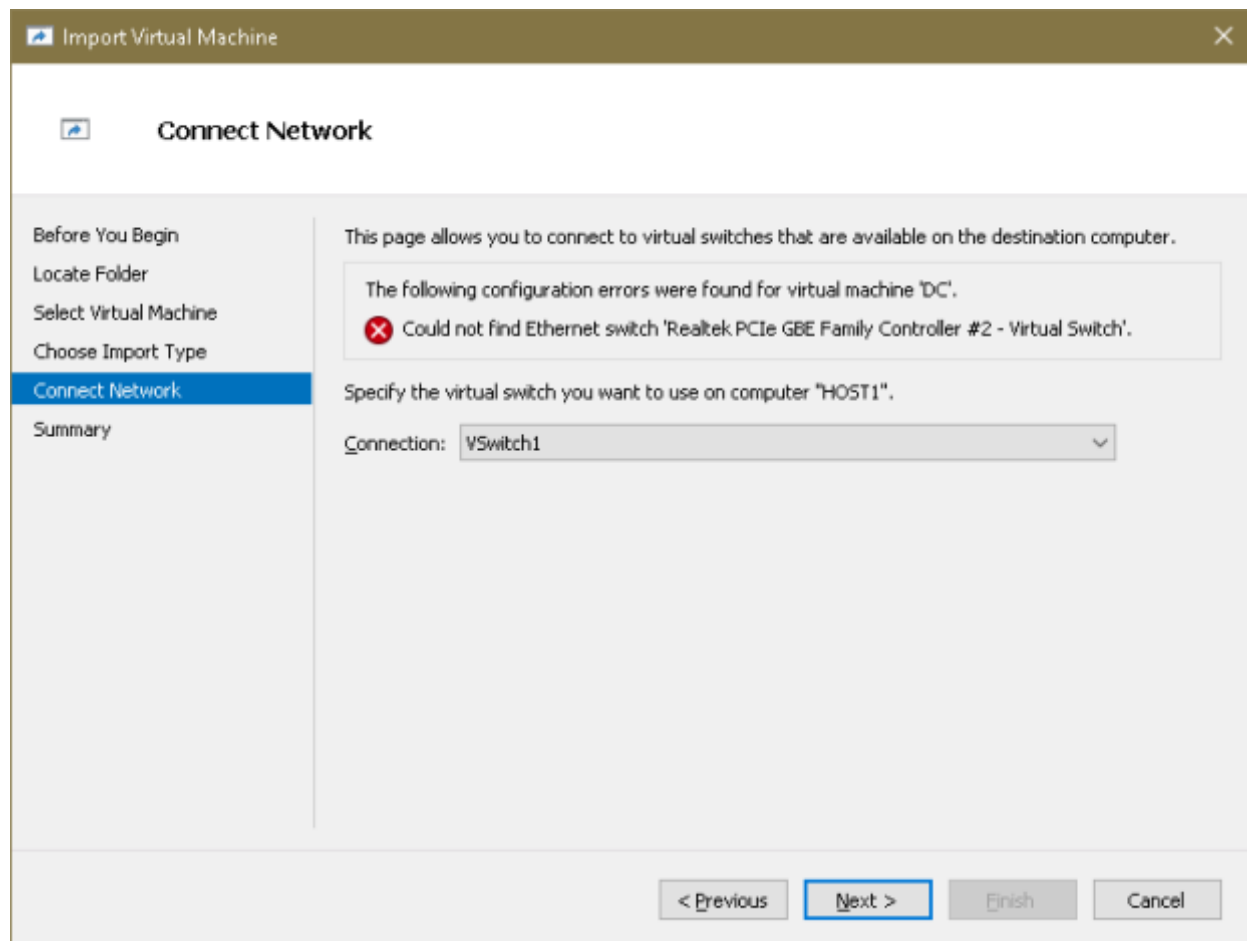
☐ Copy the virtual machine (create a new unique ID)

< Previous

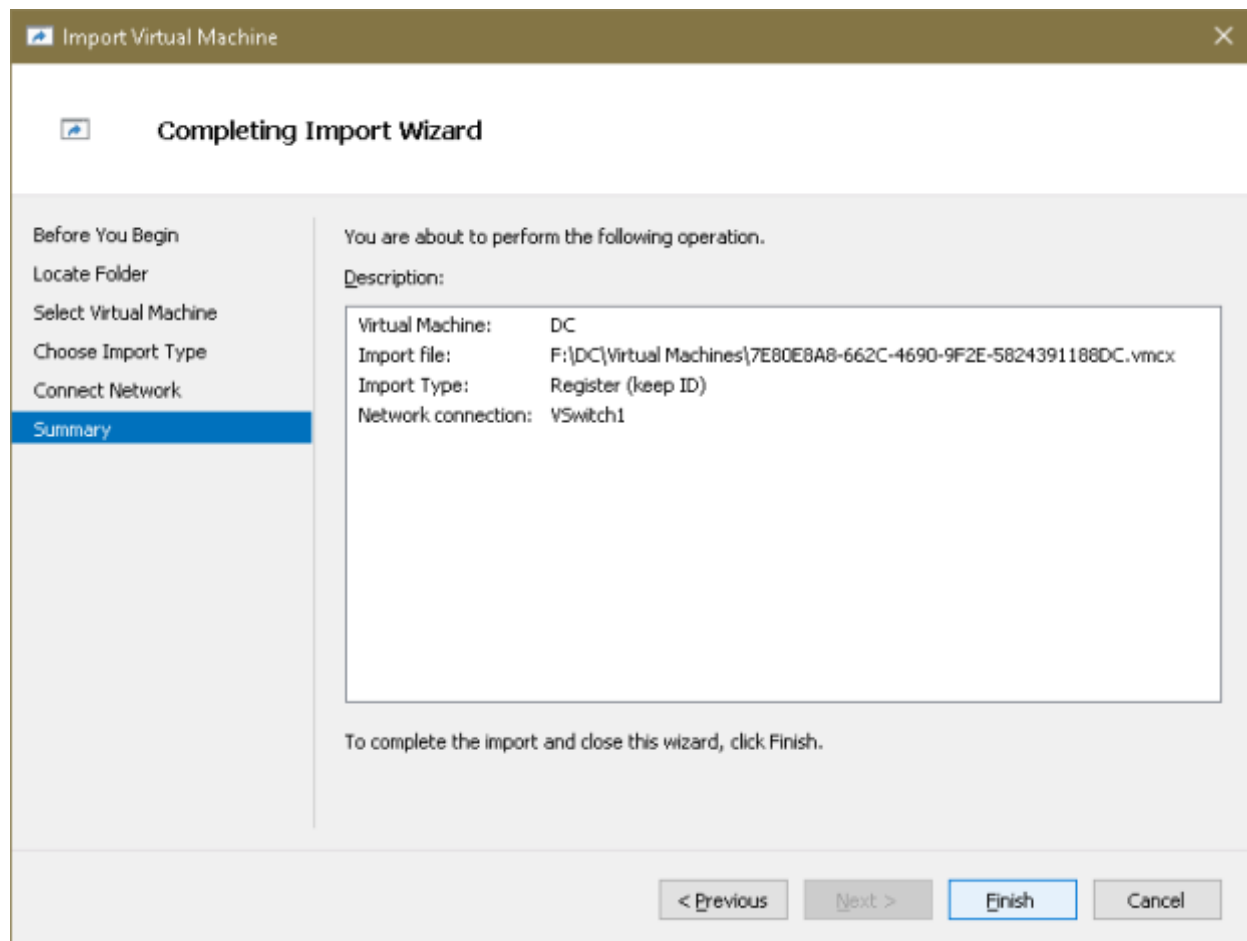
Next >

Finish

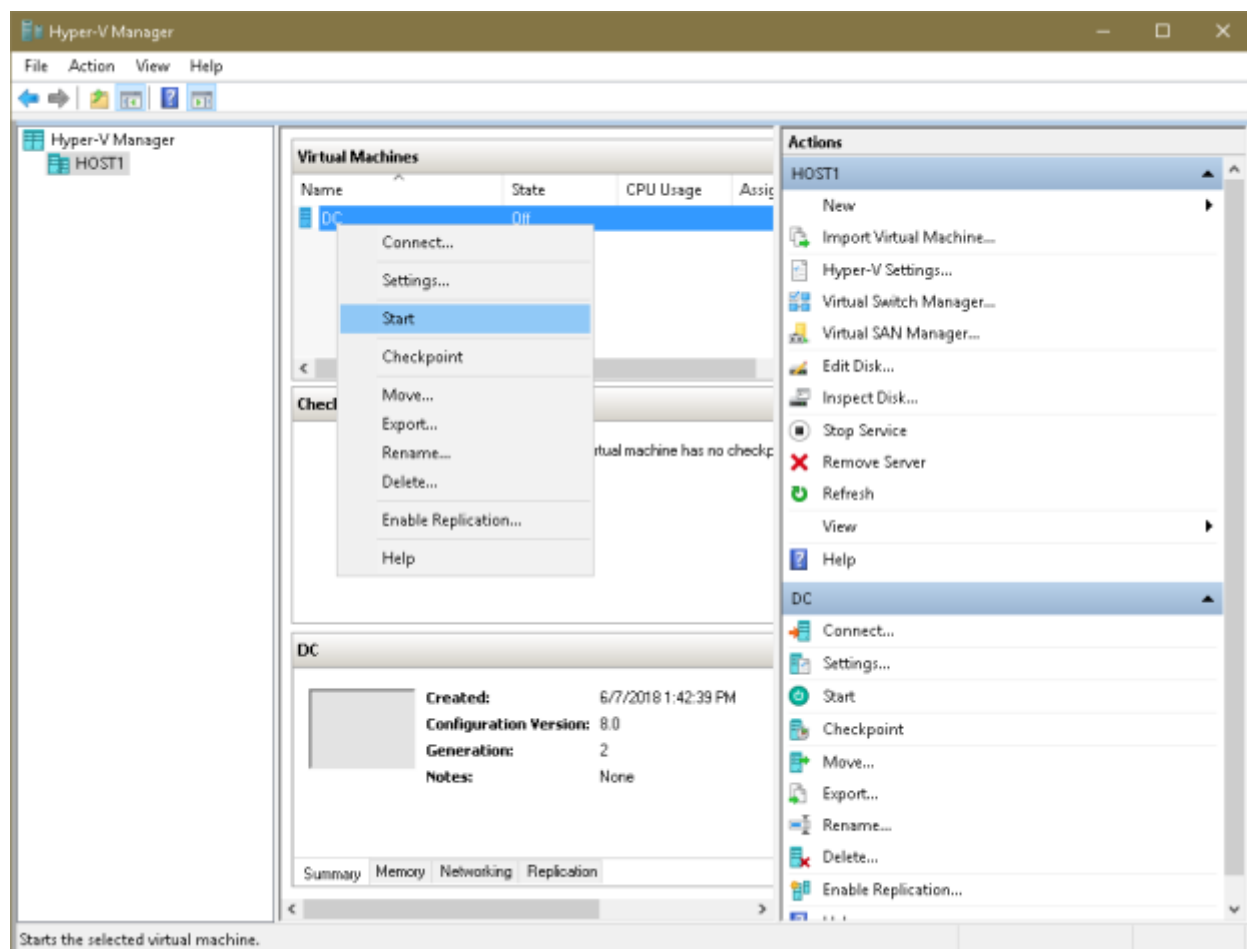
Cancel

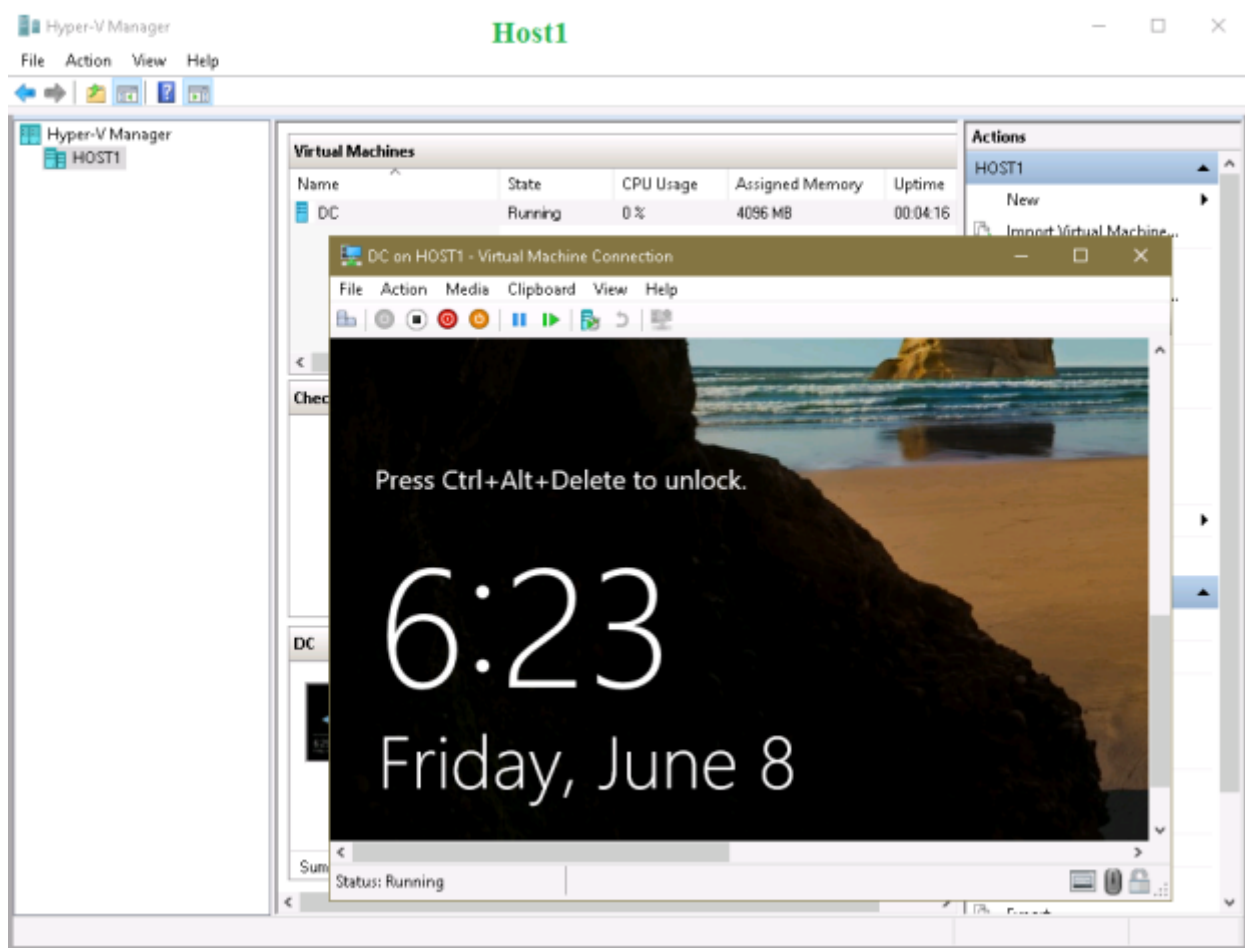


As Host1 doesn't have the virtual switch that was used at the time of DC creation I must select the one available on this host.



Now let's test the shielded (encryption supported!) virtual machine:

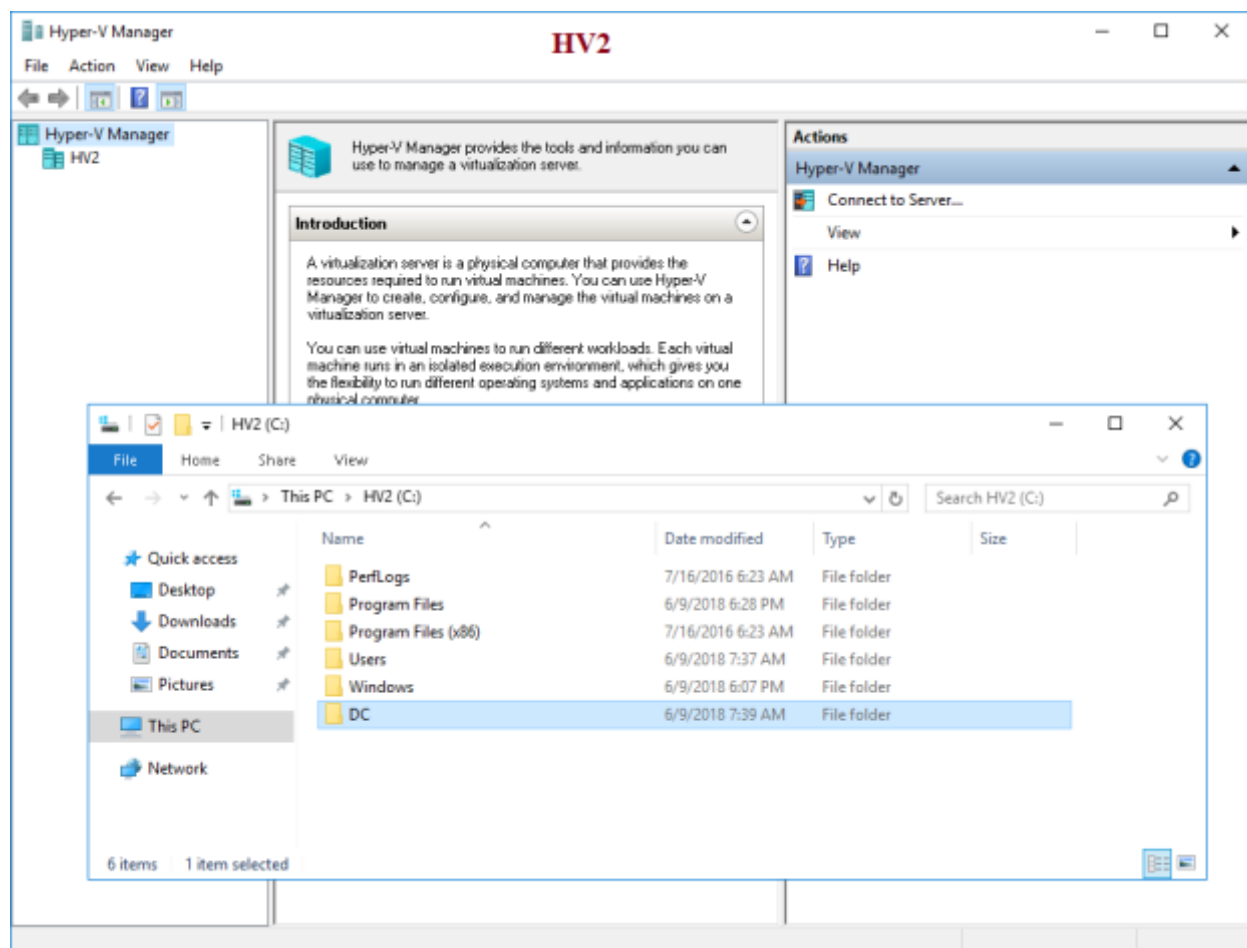
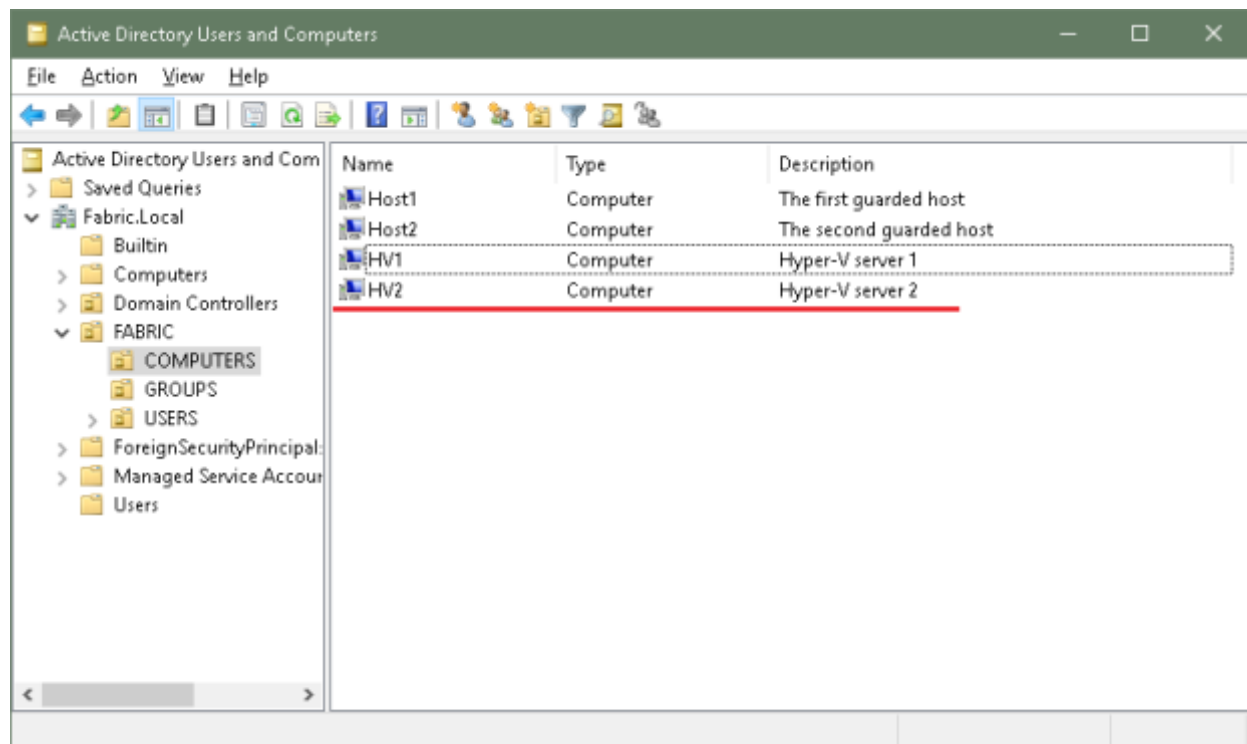


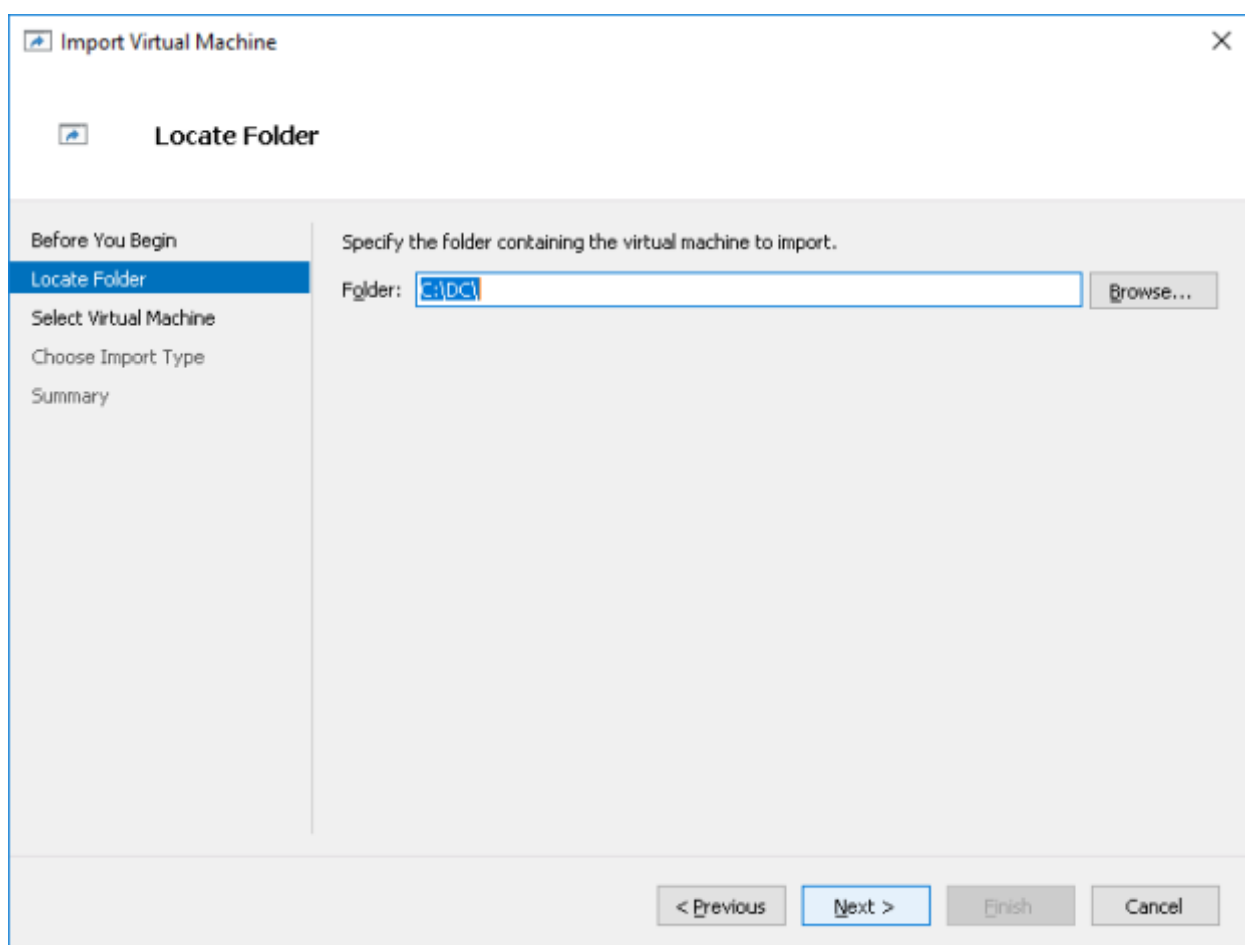
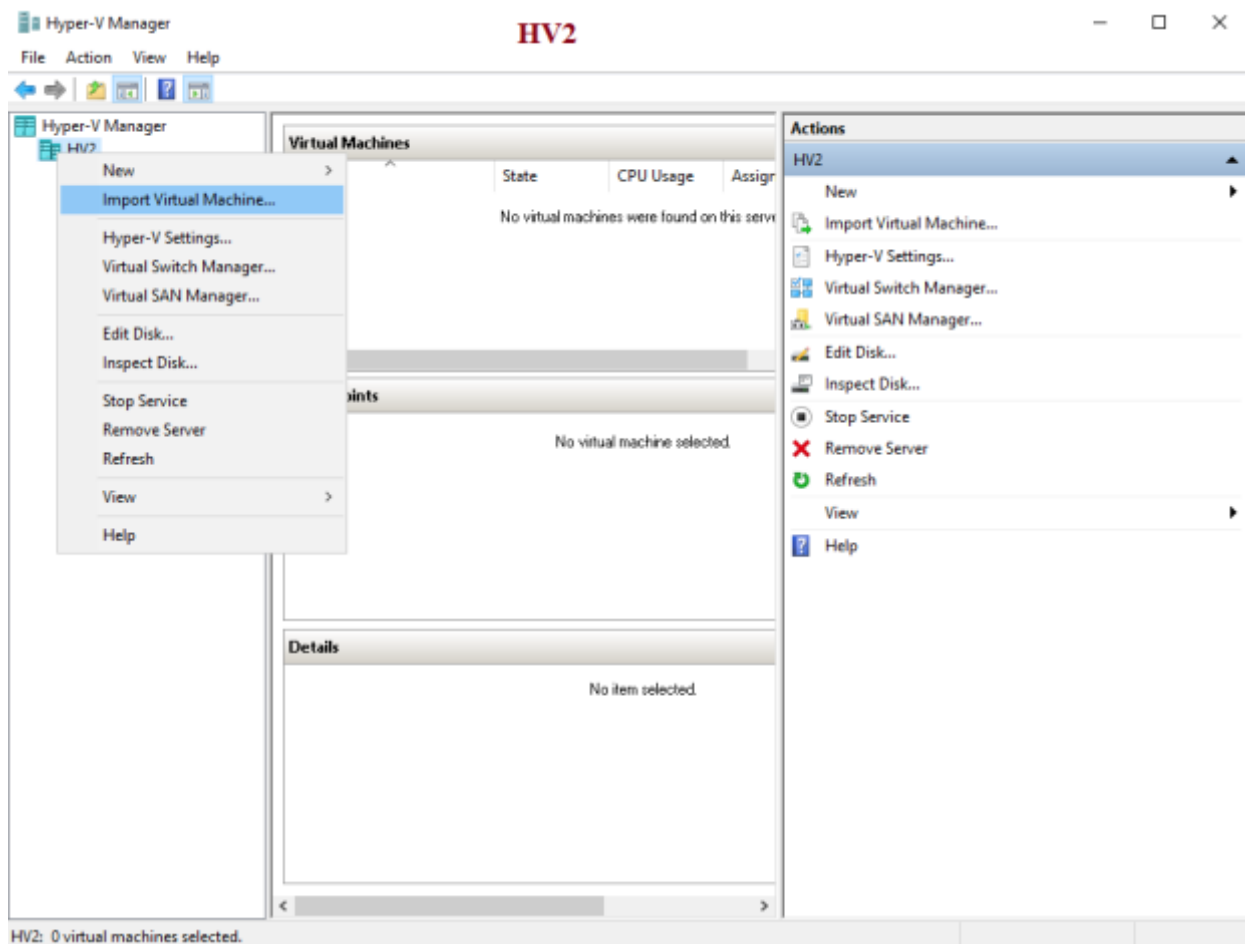


As you see the fabric administrator does have the ability to connect to the DC vm using Hyper-V Manager – if I had applied the `$Shielded = $true` policy this would not be possible.

To make sure the DC vm is fully secured we can enable Bitlocker using the virtual TPM which was enabled in step 7 – I'll skip this step as Bitlocker will not have any impact on the guarded hosts' ability to run or not to run shielded VMs.

Now I'll try to import the DC virtual machine to another Hyper-V host – HV2 – which is not part of the guarded fabric and make sure the DC vm will not start:





Import Virtual Machine

Select Virtual Machine

Before You Begin

Locate Folder

Select Virtual Machine

Choose Import Type

Summary

Select the virtual machine to import:

Name	Date Created
DC	6/7/2018 3:42:39 AM

< Previous

Next >

Finish

Cancel

Import Virtual Machine

Choose Import Type

Before You Begin

Locate Folder

Select Virtual Machine

Choose Import Type

Summary

Choose the type of import to perform:

☒ Register the virtual machine in-place (use the existing unique ID)

☐ Restore the virtual machine (use the existing unique ID)

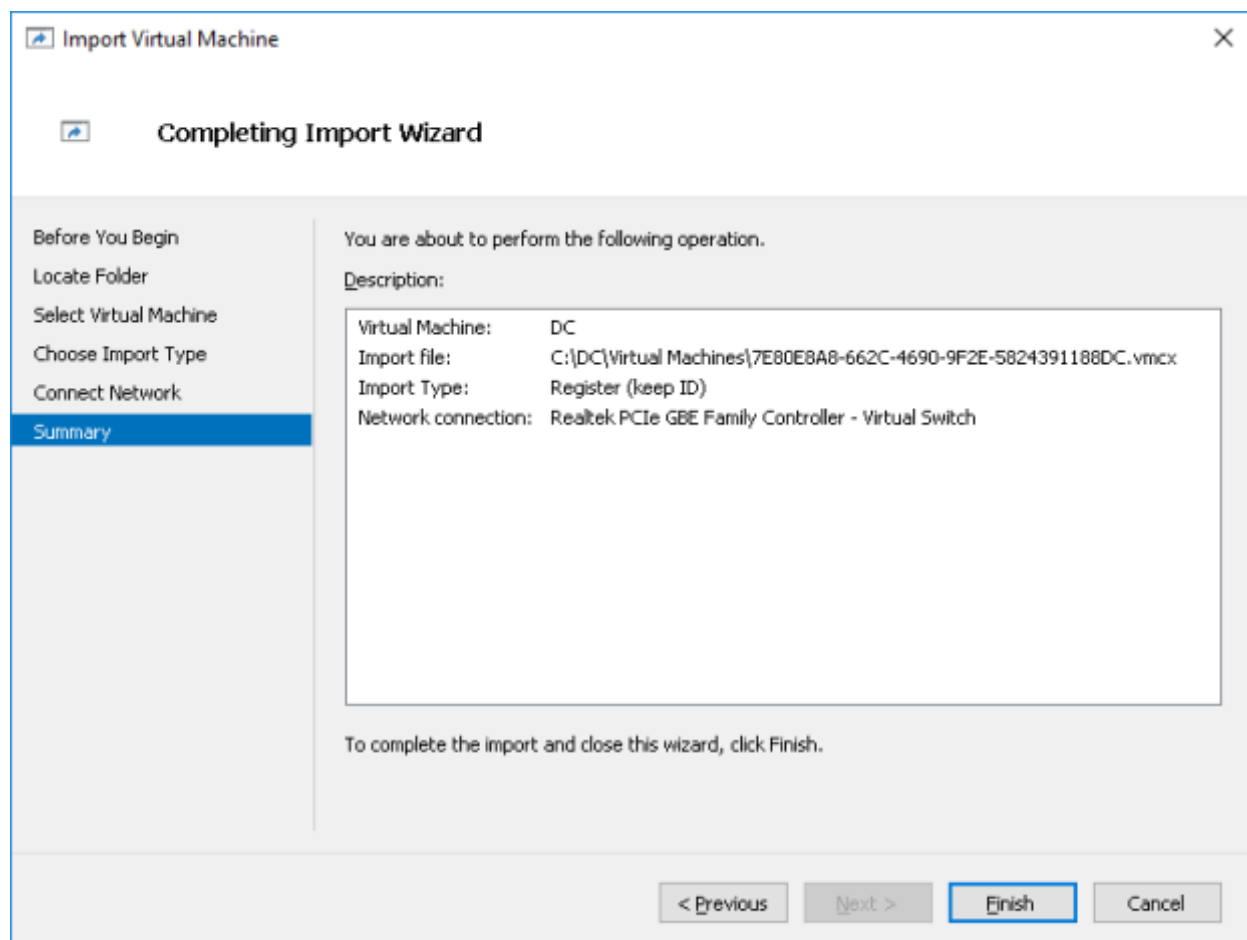
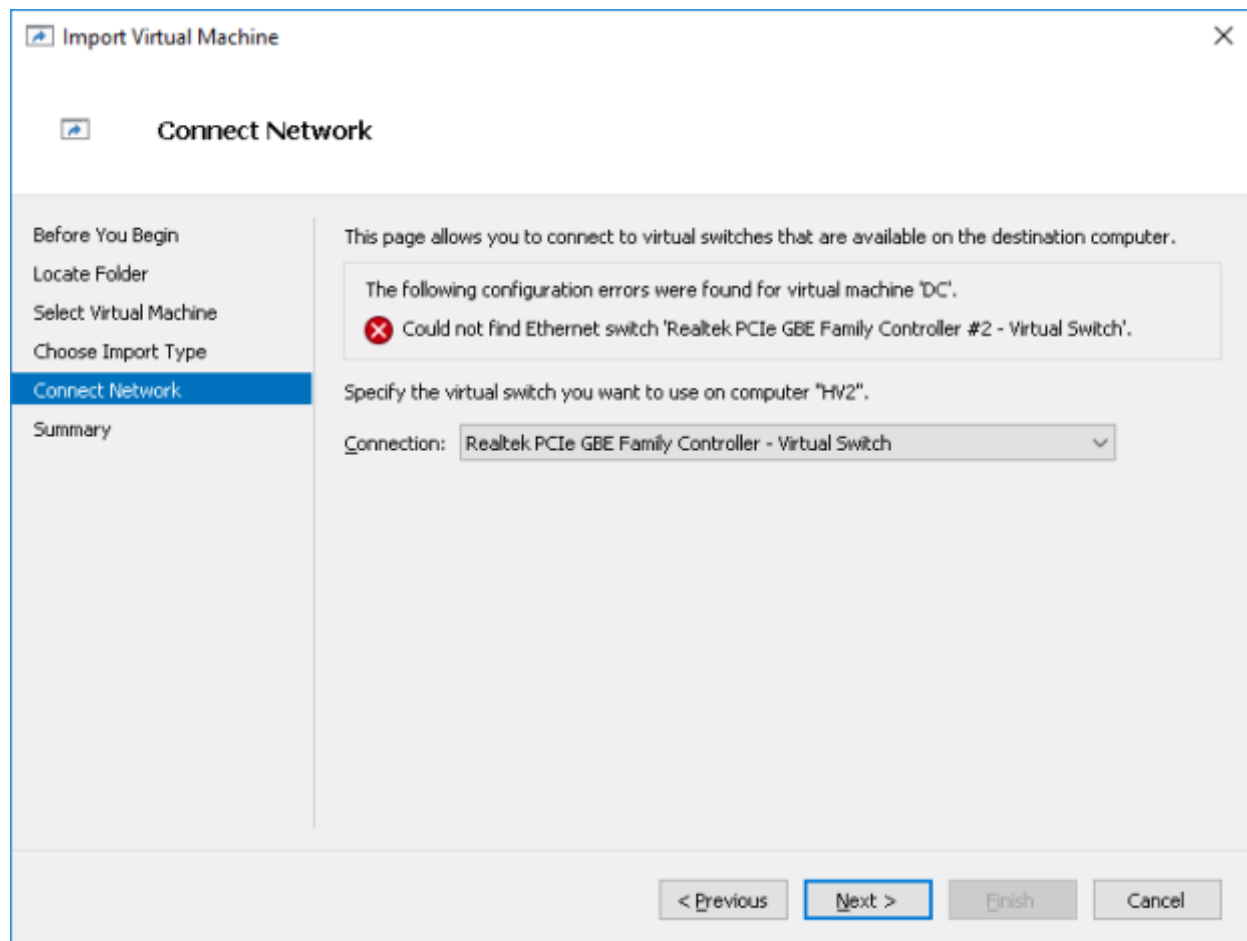
☐ Copy the virtual machine (create a new unique ID)

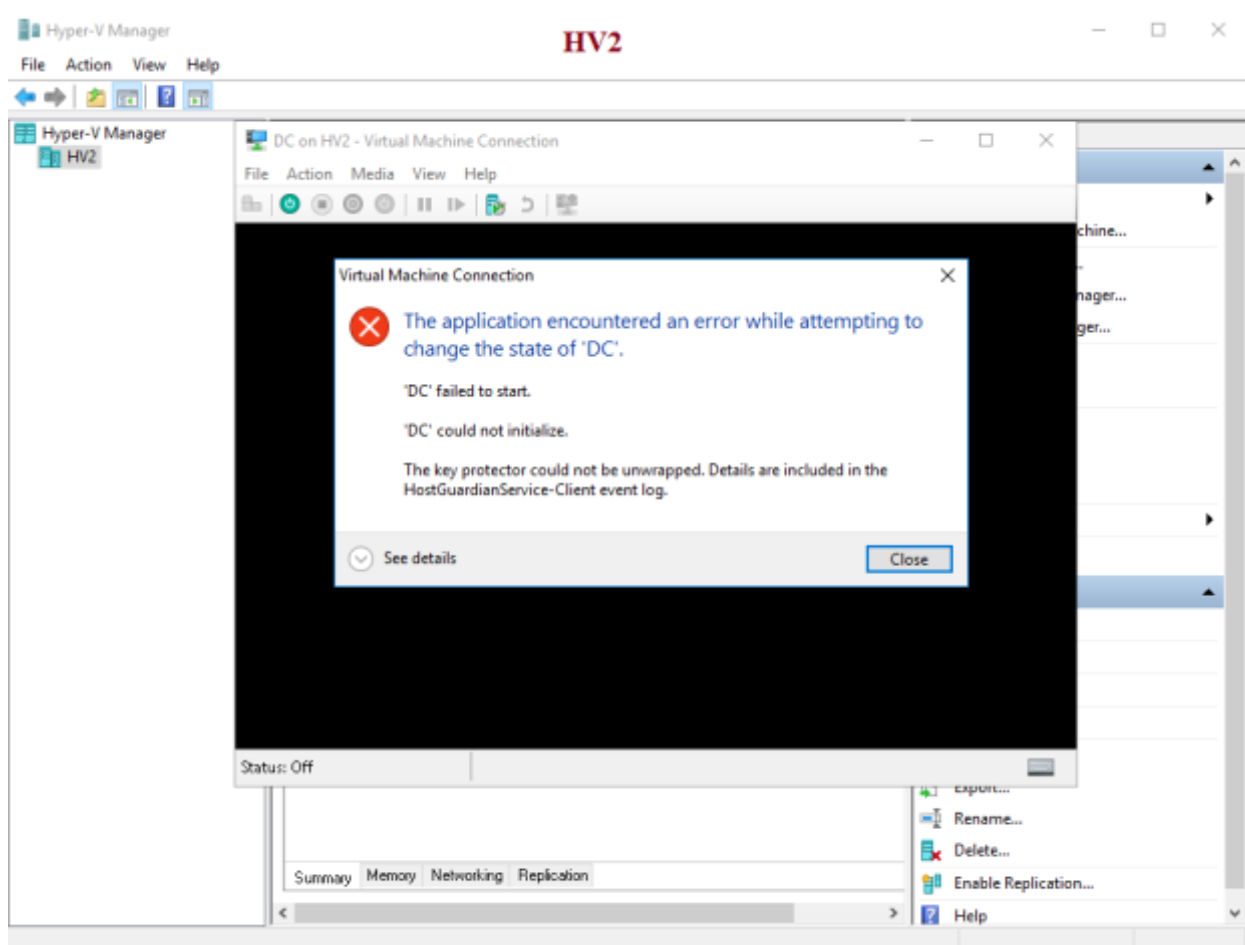
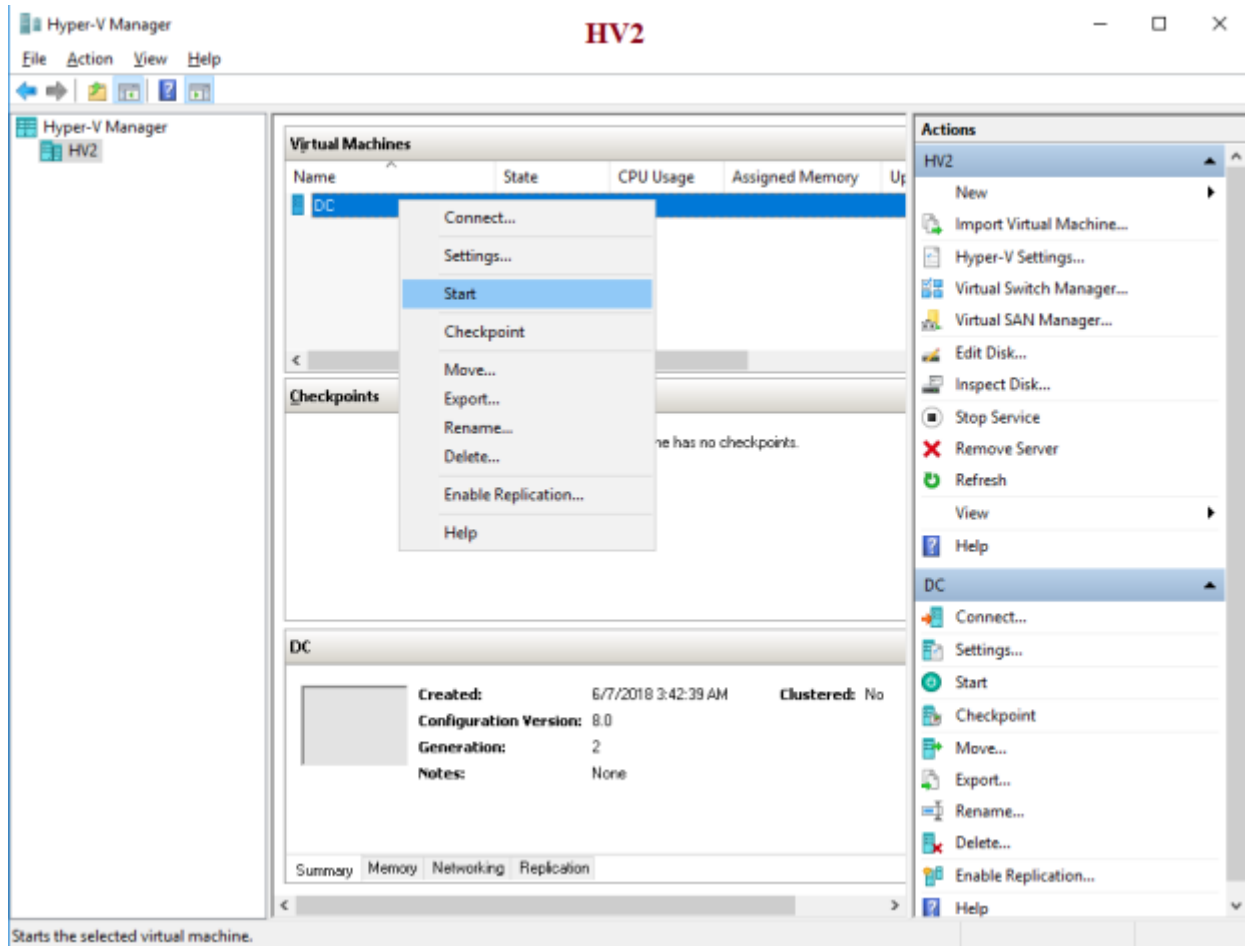
< Previous

Next >

Finish

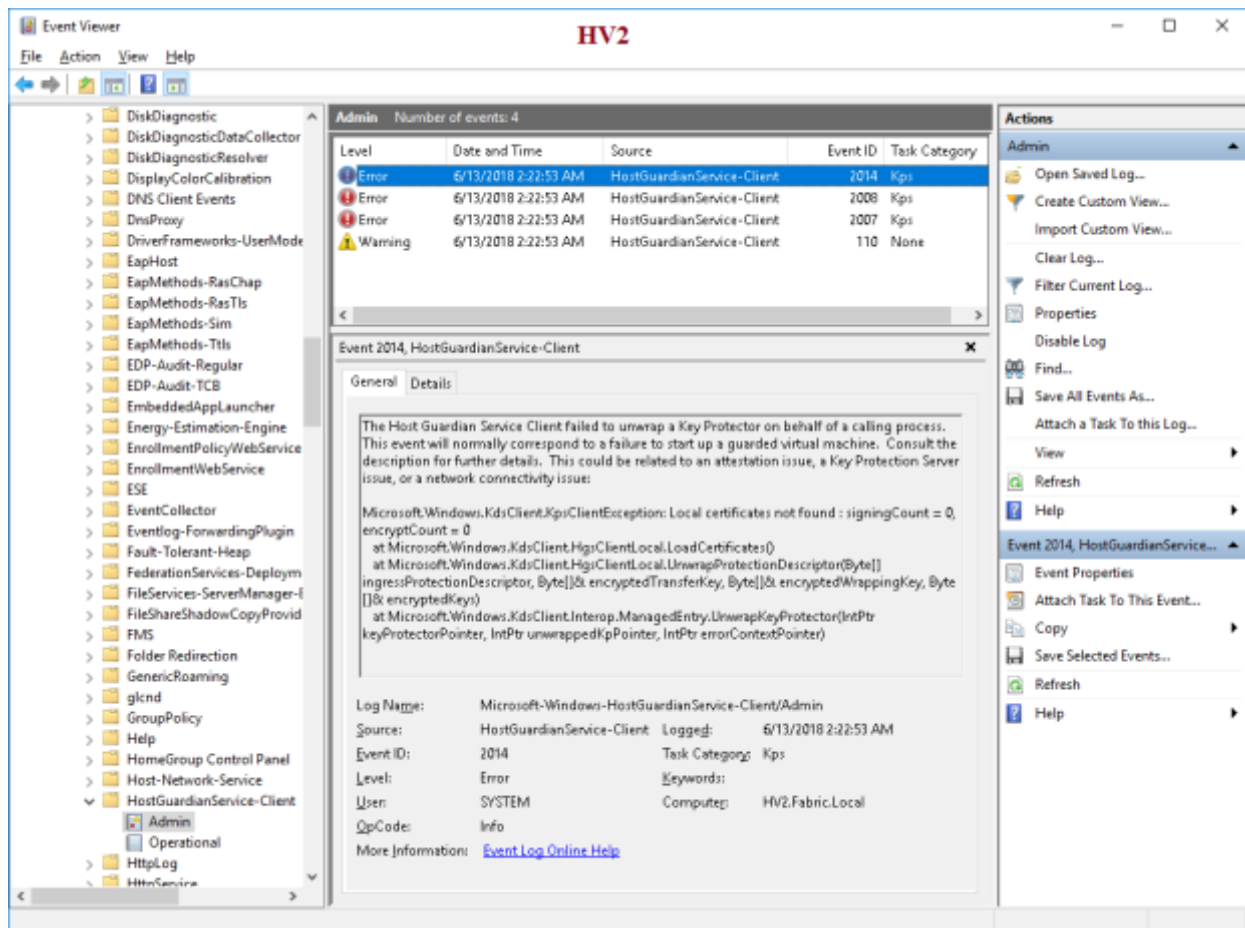
Cancel



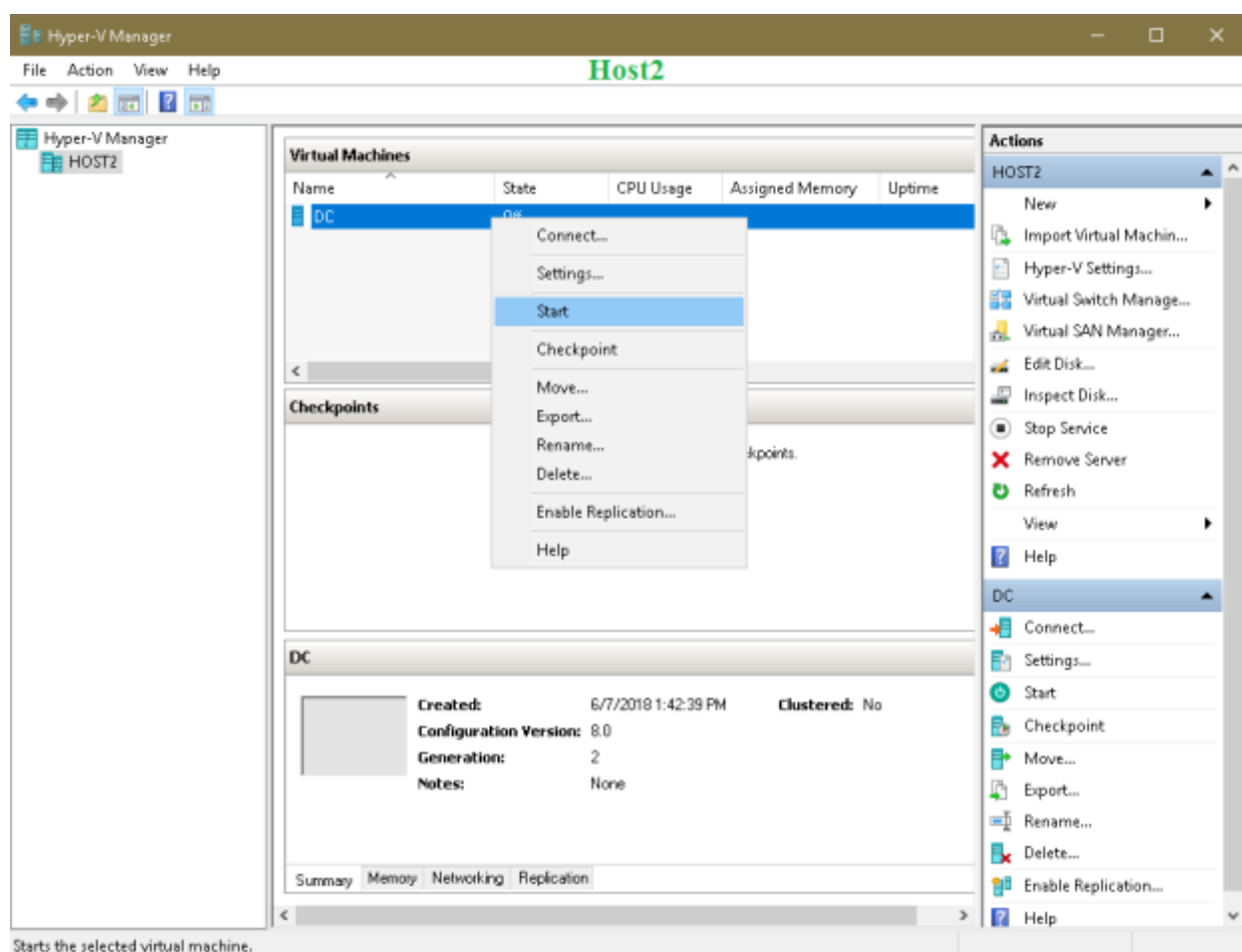
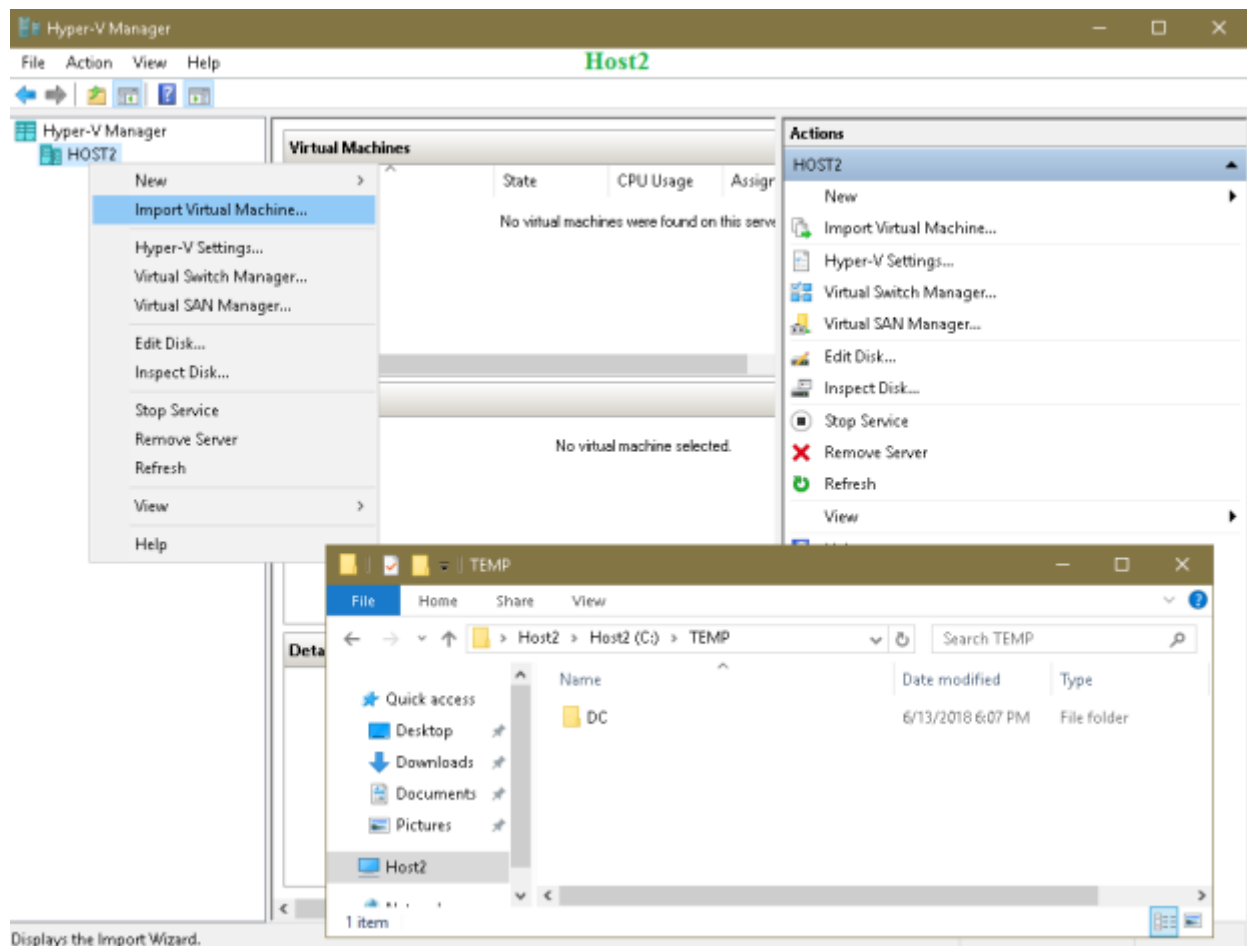


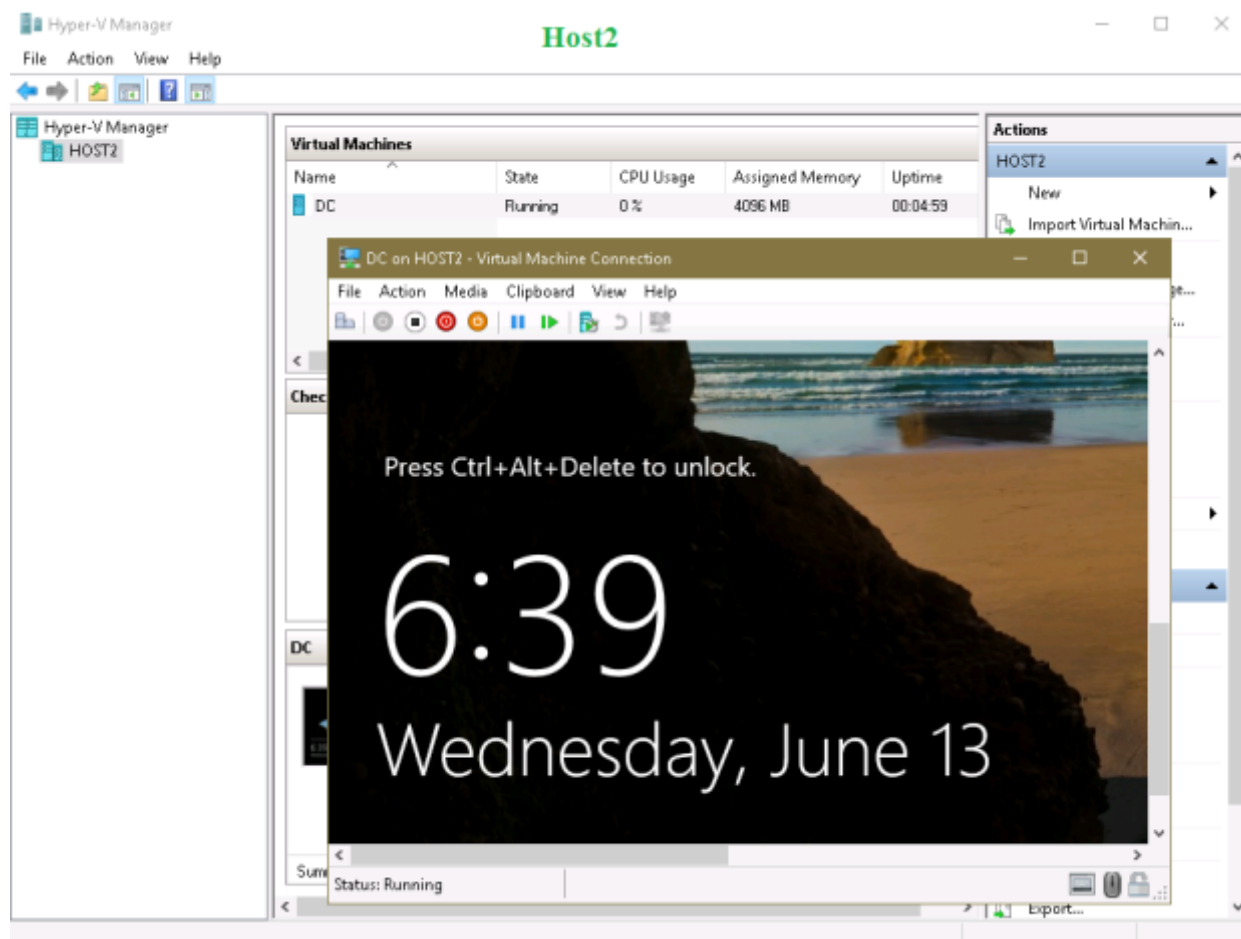
As you see the DC's key protector can not be unencrypted because HV2 host is not allowed to connect to the HGS service – only Host1 and Host2 are permitted to run the DC vm because they are the members of the GUARDED_HOSTS group and it is the only group that has been registered on HGS server using Add-HgsAttestationHostGroup cmdlet.

In this situation the following events gets registered in the **HostGuardianService-Client** event log:



And the last test: suppose I want to move the DC vm to the other guarded host – Host2. After configuring Host2 as described in [part2](#) and importing the virtual machine I'll try to start the DC vm on Host2:





Summary:

In this blog post series we've seen how the new type of virtual machines – the guarded virtual machines – can be used in the Encryption-Supported scenario.