Deploying Shielded Virtual Machines – Part1

michaelfirsov.wordpress.com/deploying-shielded-virtual-machines-part1

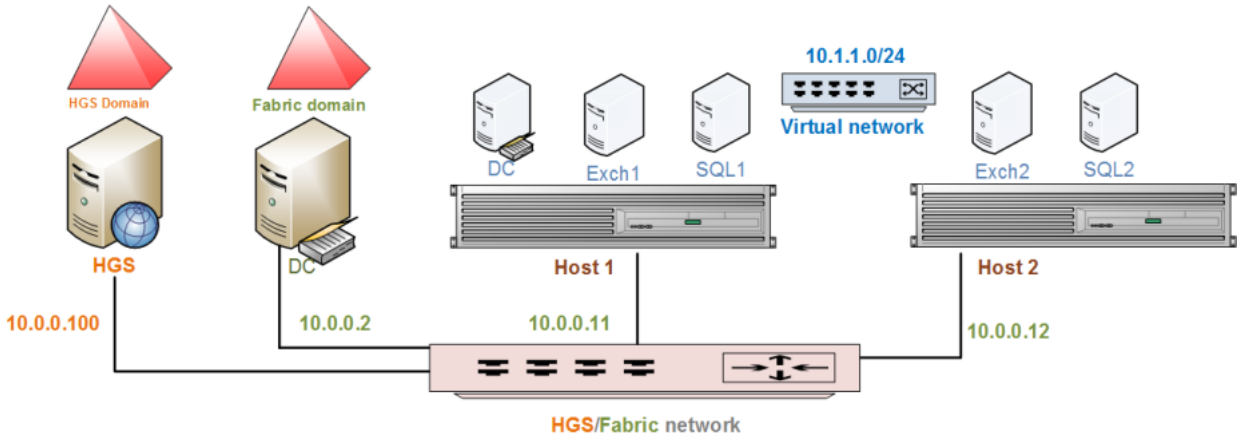
May 31, 2018

Windows Server 2016 incorporates many new security features and a new type of virtual machines – *shielded virtual machines* – is definitely one of the most important ones. As you may already know there are two types of shielded VMs: **shielded** VMs and **encryption supported** VMs. *Shielded* virtual machines are the most restricted VMs: the only way the owner can interact with them is by means of RDP – no other ways such as PS or Hyper-V manager is not supported. *Encryption Supported* VMs do allow the hyper-v administrators to connect to virtual machines – you can find more information on the matter here and here.

In this blog post series I'd like to show how we can protect virtual machines from stealing – I think it is the most actual security-related question for the organizations where you do NOT need to protect virtual machines from fabric admins – in other words where the administrators are fully trusted and the only security concern is the possibility that some virtual machine can be stolen along with the host itself. In this case it'll be suffice to deploy HGS service with Active Directory attestation mode. Let's see how this can be done.

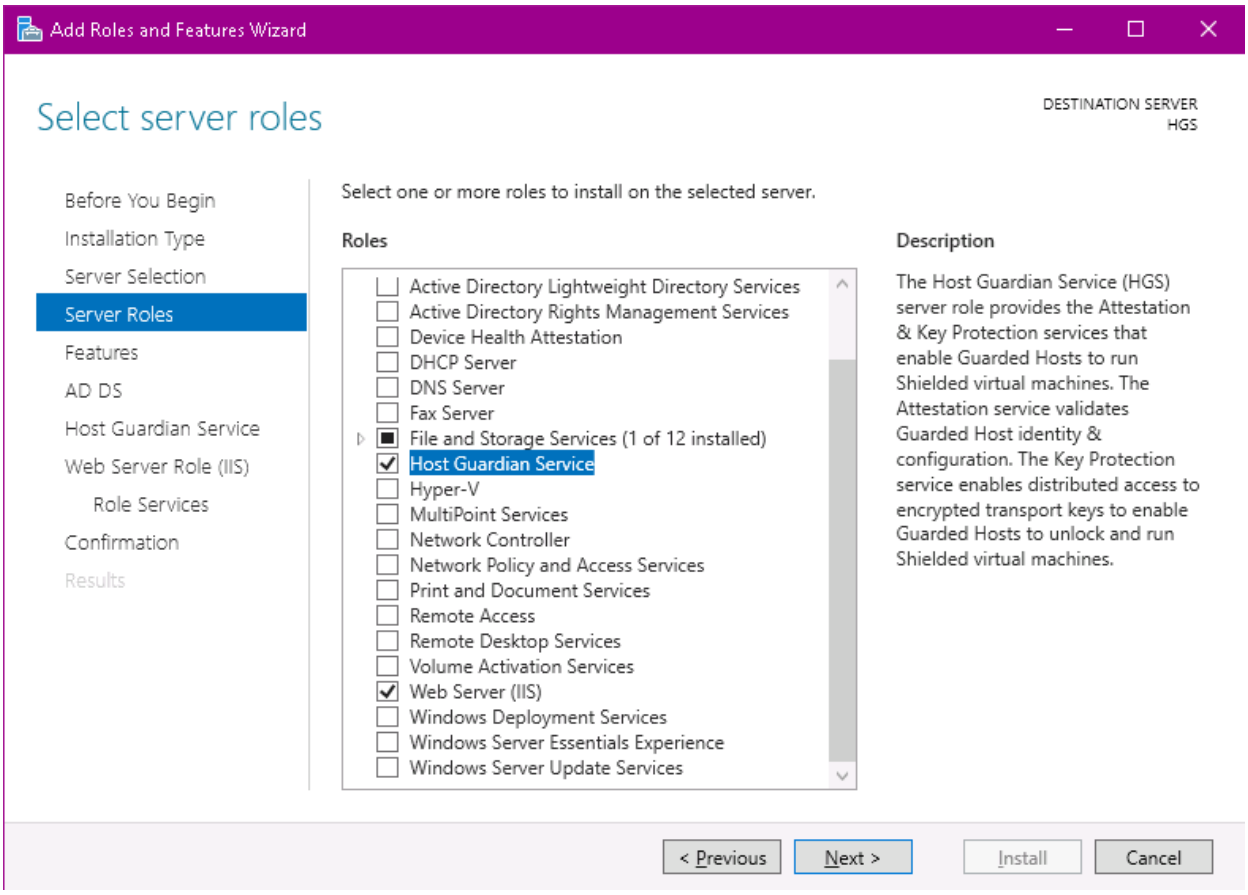
Part 1: Deploying HGS service

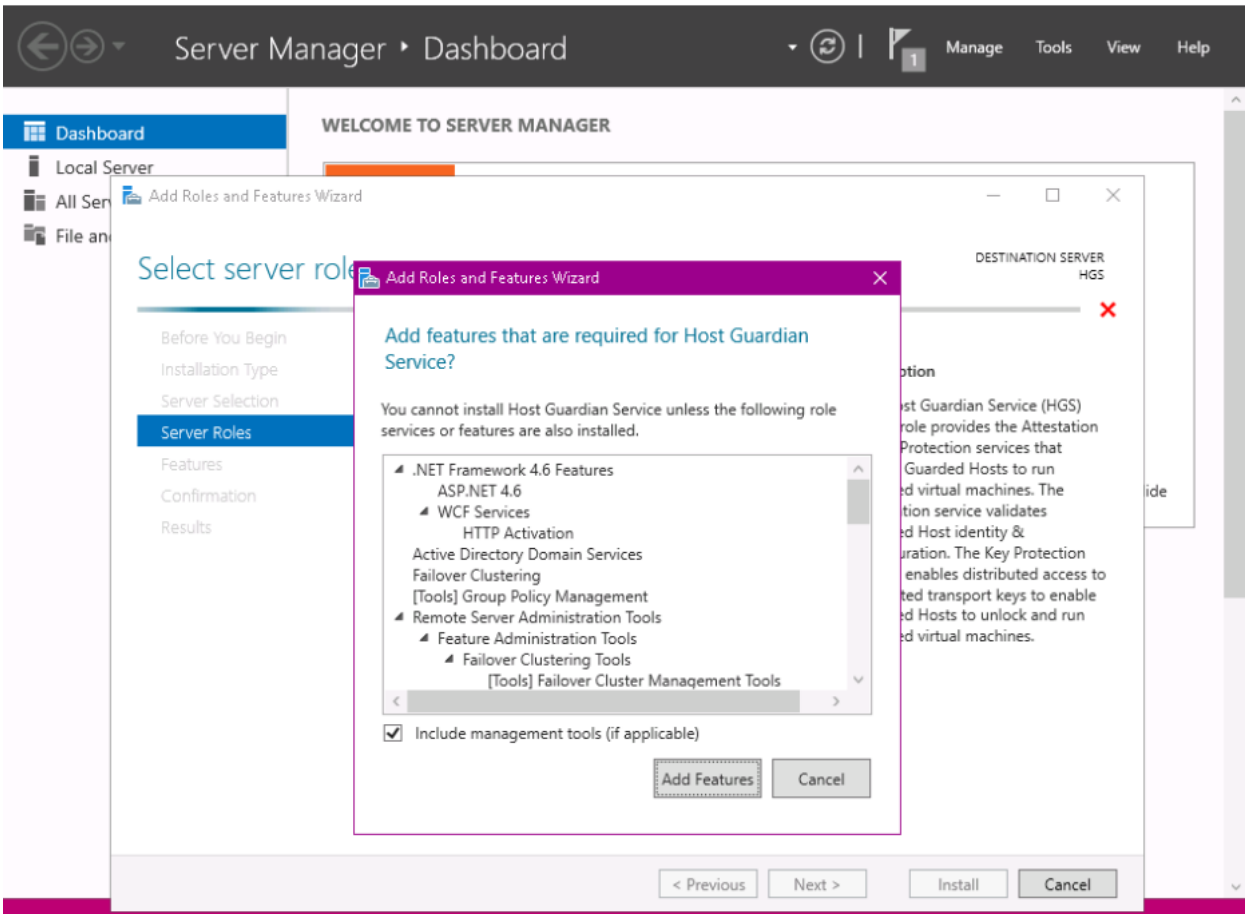
Here's the schematic of my testing network:



I'll start deploying shielded virtual machines from installing and configuring HGS cluster. MS recommends create a three-node cluster but for the purpose of this test the cluster will consist of the single node named **HGS** (the name of the cluster will be **HGScloud**).

First of all I add the Host Guardian Service to the newly installed Windows Server 2016 Datacenter (Standard edition may be used as well – please see Review prerequisites for the Host Guardian Service for the additional information).





Advertisements

Report this adPrivacy

Please pay attention to the outcomes of the HGS Service installation:

Add Roles and Features Wizard

Host Guardian Service

DESTINATION SERVER
HGS

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- Host Guardian Service
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

The Host Guardian Service (HGS) server role provides the Attestation & Key Protection services that enable Guarded Hosts to run Shielded virtual machines. The Attestation service validates Guarded Host identity & configuration. The Key Protection service enables distributed access to encrypted transport keys to enable Guarded Hosts to unlock and run Shielded virtual machines.

Things to Note:

- To install and initialize the Host Guardian Service server role, the account you use must be a member of the local Administrators group on the server.
- To help ensure that Shielded virtual machines can run on Guarded Hosts in the event of a server outage, install a minimum of three instances of the Host Guardian Service server role.
- After installing & initializing the Host Guardian Service server role, the Active Directory Domain Services (AD DS) server role is automatically installed, and the server is promoted to a domain controller in a private AD DS forest.
- After installing & initializing the Host Guardian Service server role, the server automatically becomes a failover cluster member.
- After installing & initializing the Host Guardian Service server role, the server is automatically configured with a "Just Enough Administration" profile and registered with pre-defined Active Directory user groups.

< Previous | Next > | Install | Cancel

Add Roles and Features Wizard

Web Server Role (IIS)

DESTINATION SERVER
HGS

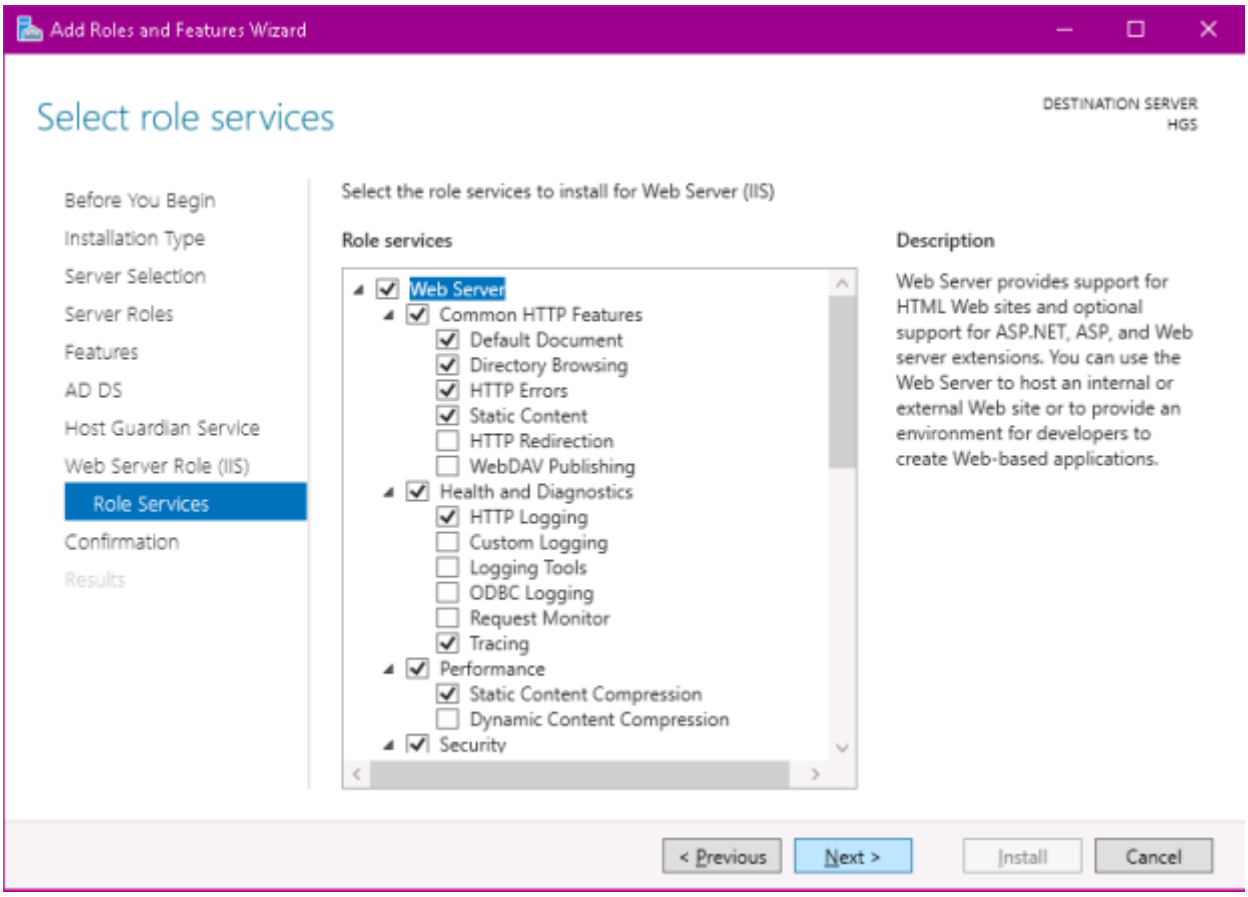
- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- Host Guardian Service
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

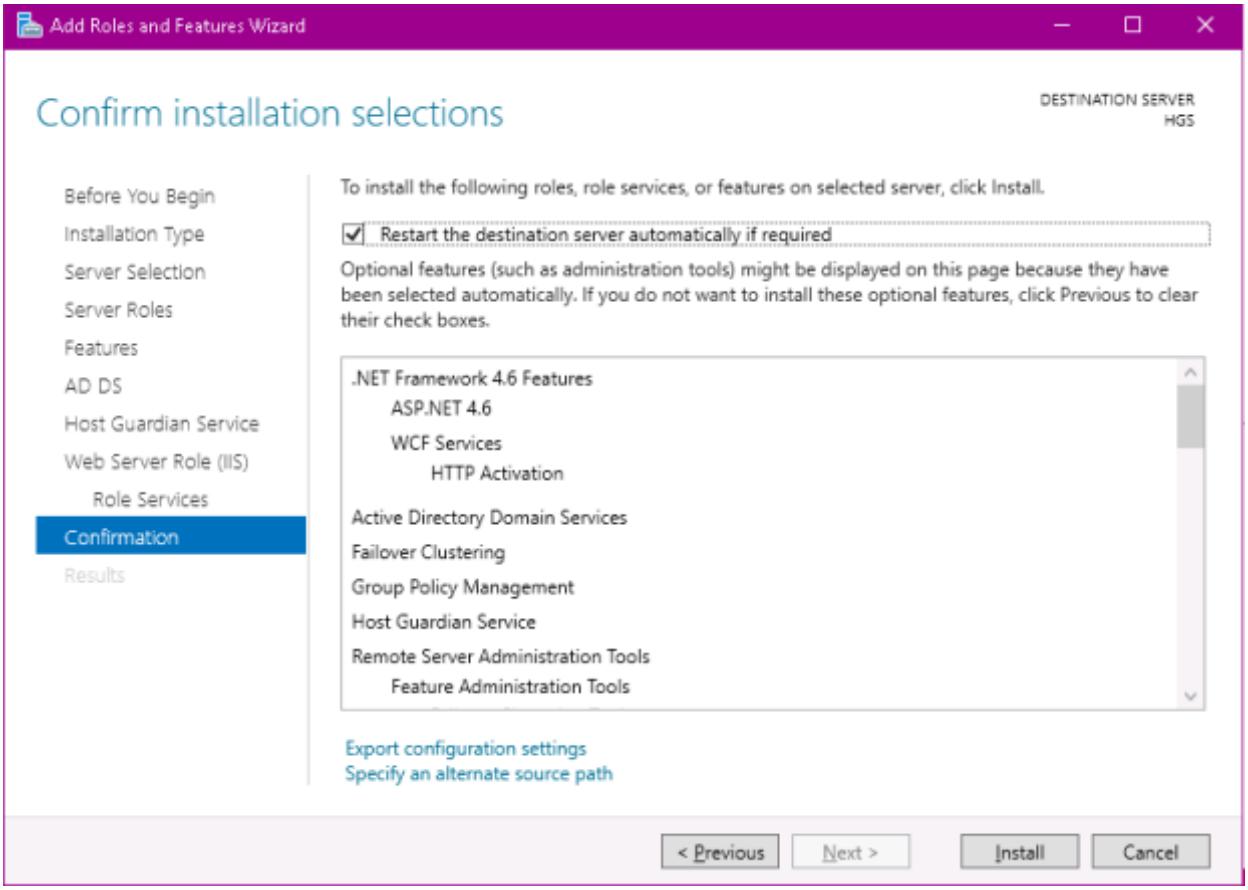
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

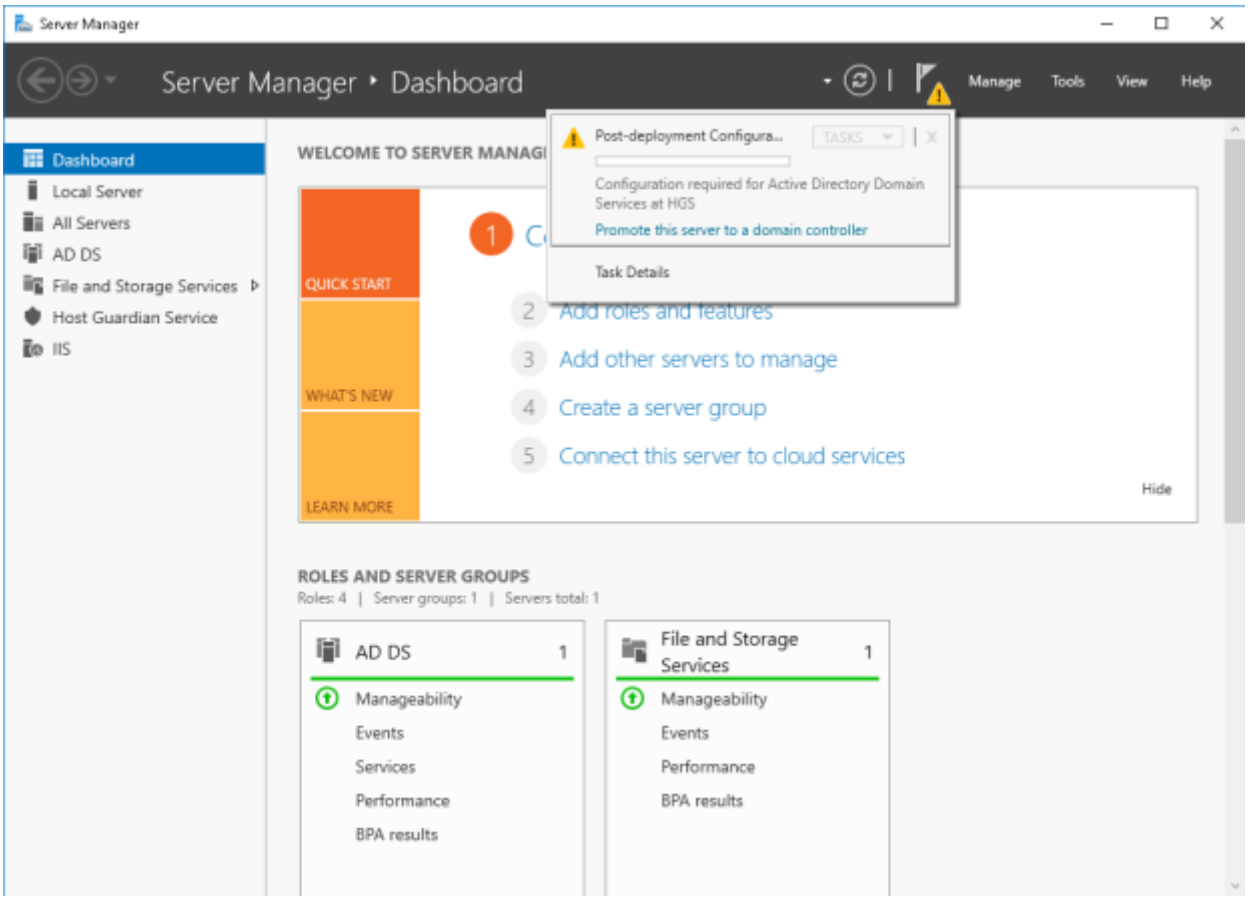
More information about Web Server IIS

< Previous | Next > | Install | Cancel



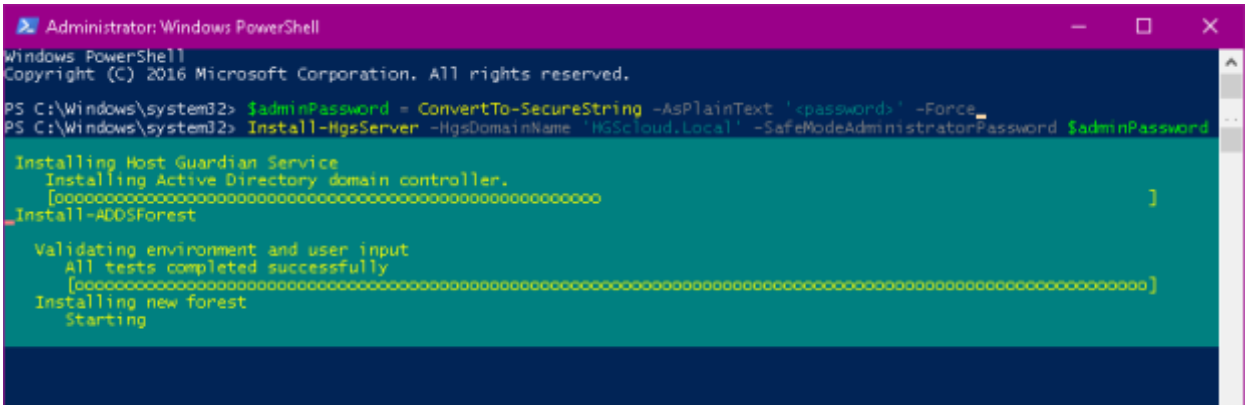


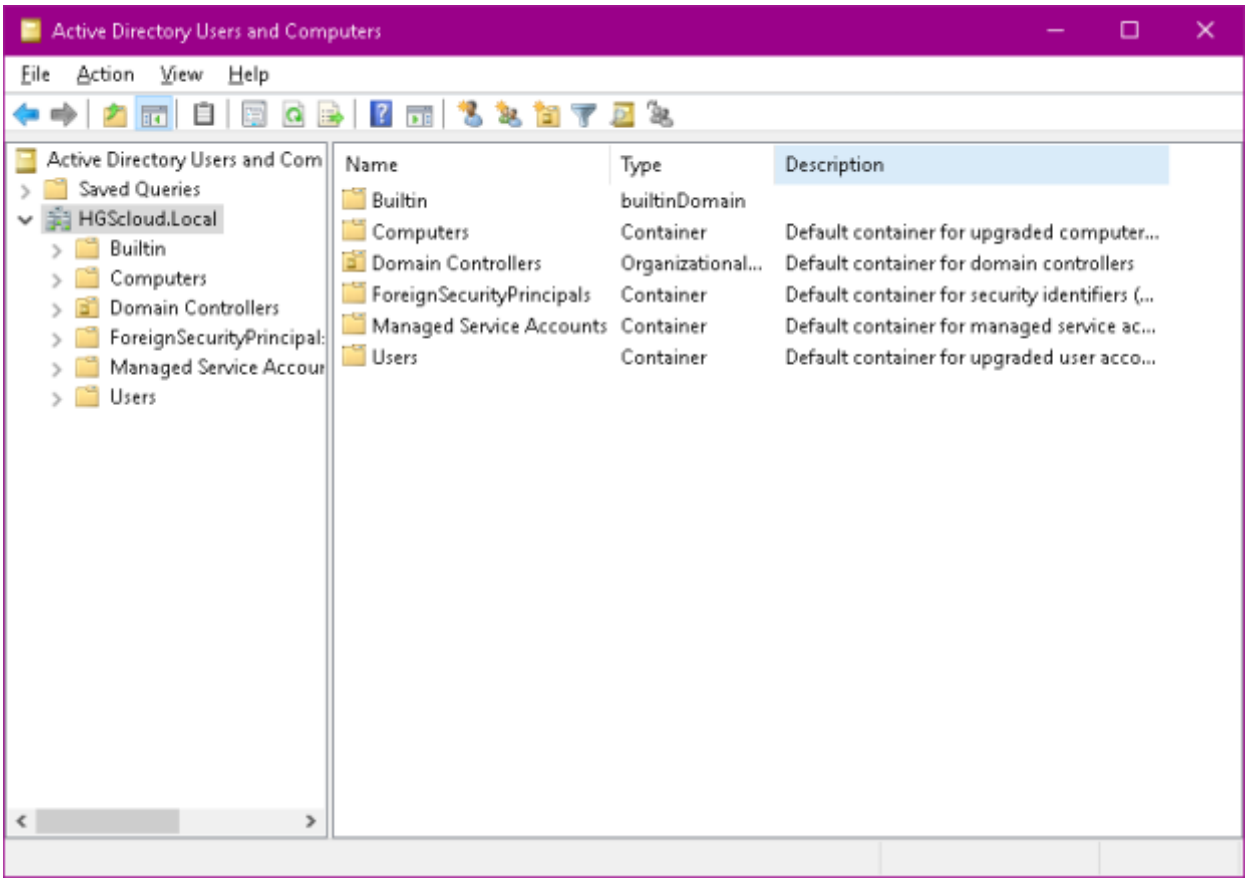
After restarting, the Server Manager offers to promote this server to a domain controller…



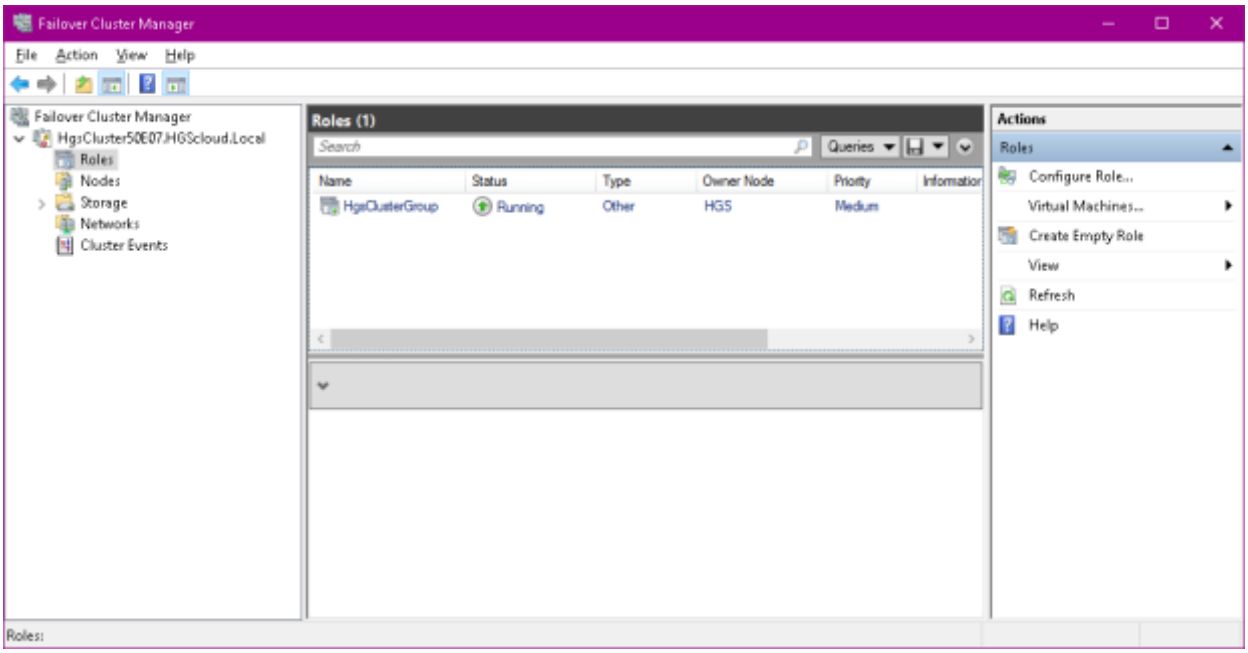
…but all other subsequent configuration steps will be done in MS PS and the second step is to install HGS Service (the name of the new Active Directory domain will be HGScloud.Local):

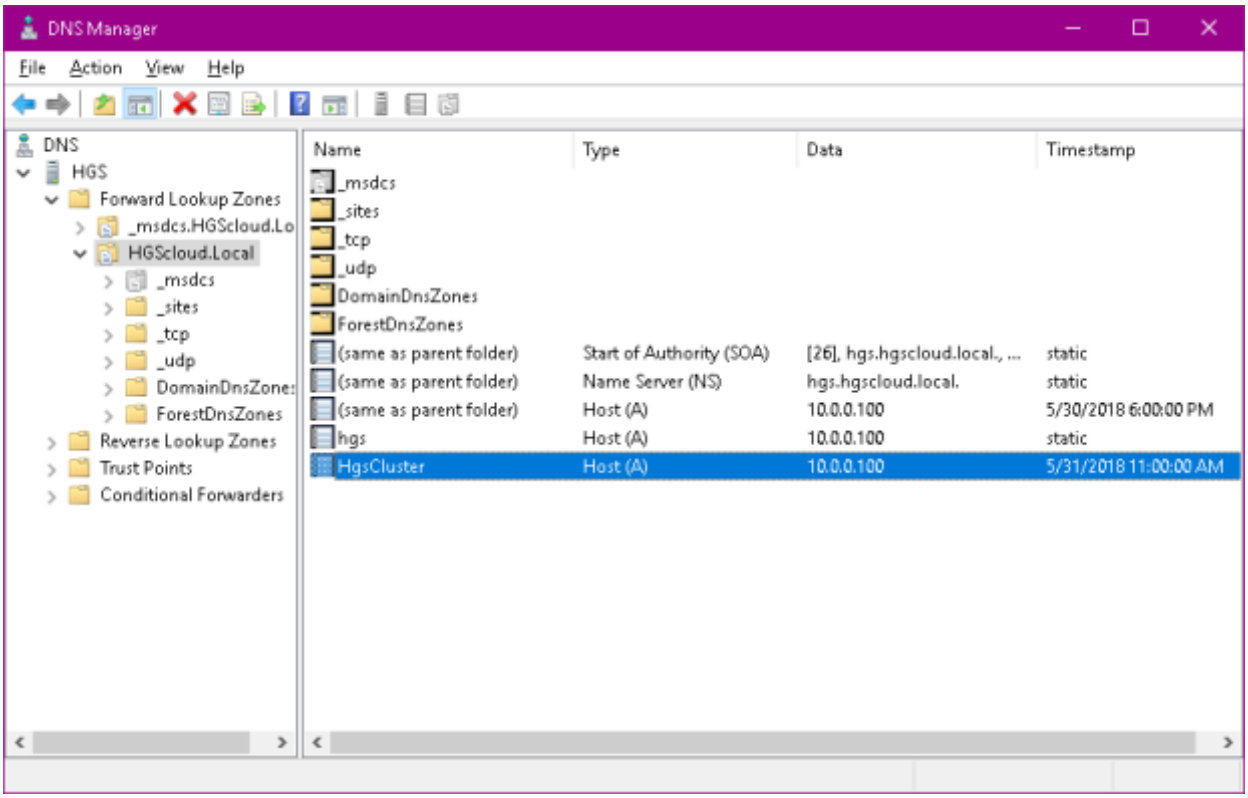
$adminPassword = ConvertTo-SecureString -AsPlainText ‘<password>’ -Force
Install-HgsServer -HgsDomainName ‘HGScloud.Local.com’ -SafeModeAdministratorPassword $adminPassword -Restart





Advertisements
Report this adPrivacy

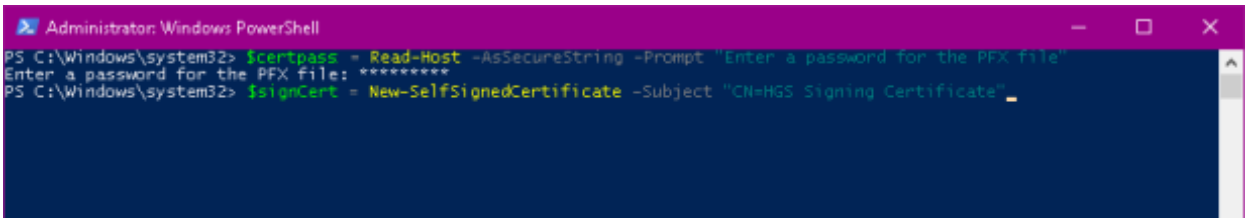




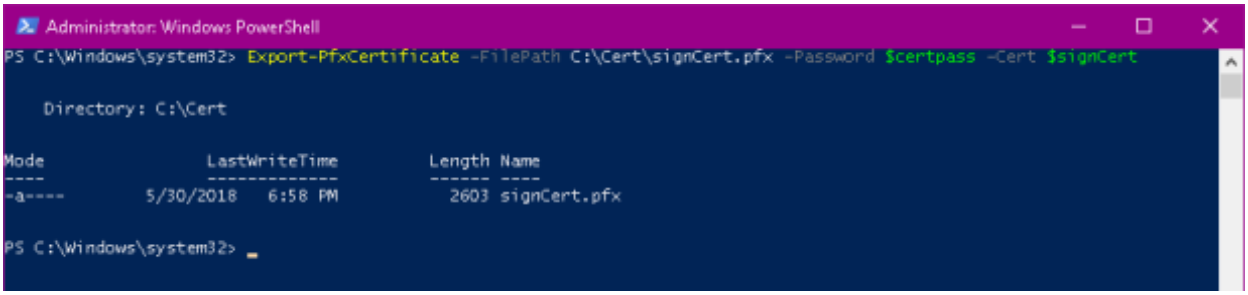
The next step is to create a couple of certificates that will be used by HGS Service for key signing and encryption – I'll make use of self-signed certificates as it'll be enough for this installation (and probably not only for test installations!):

$certpassword = Read-Host -AsSecureString -Prompt "Enter a password for the PFX file"

$signCert = New-SelfSignedCertificate -Subject "CN=HGS Signing Certificate"

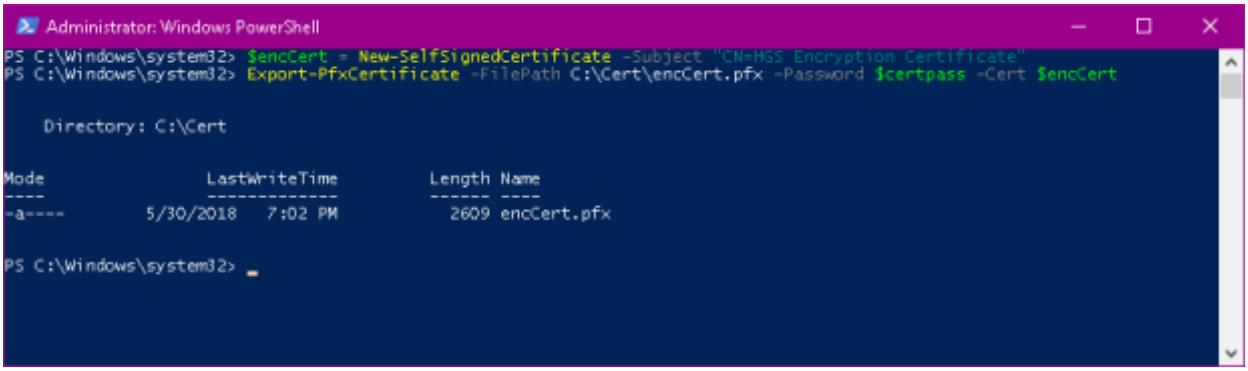


Export-PfxCertificate -FilePath .\signCert.pfx -Password $certpass -Cert $signCert

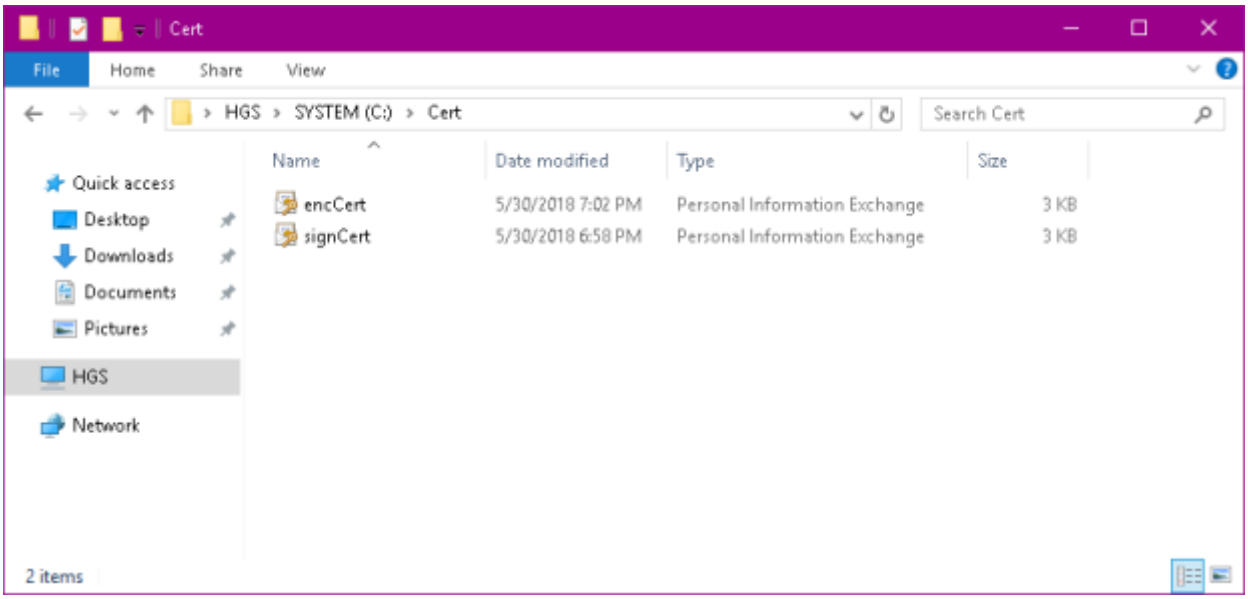


$encCert = New-SelfSignedCertificate -Subject "CN=HGS Encryption Certificate"

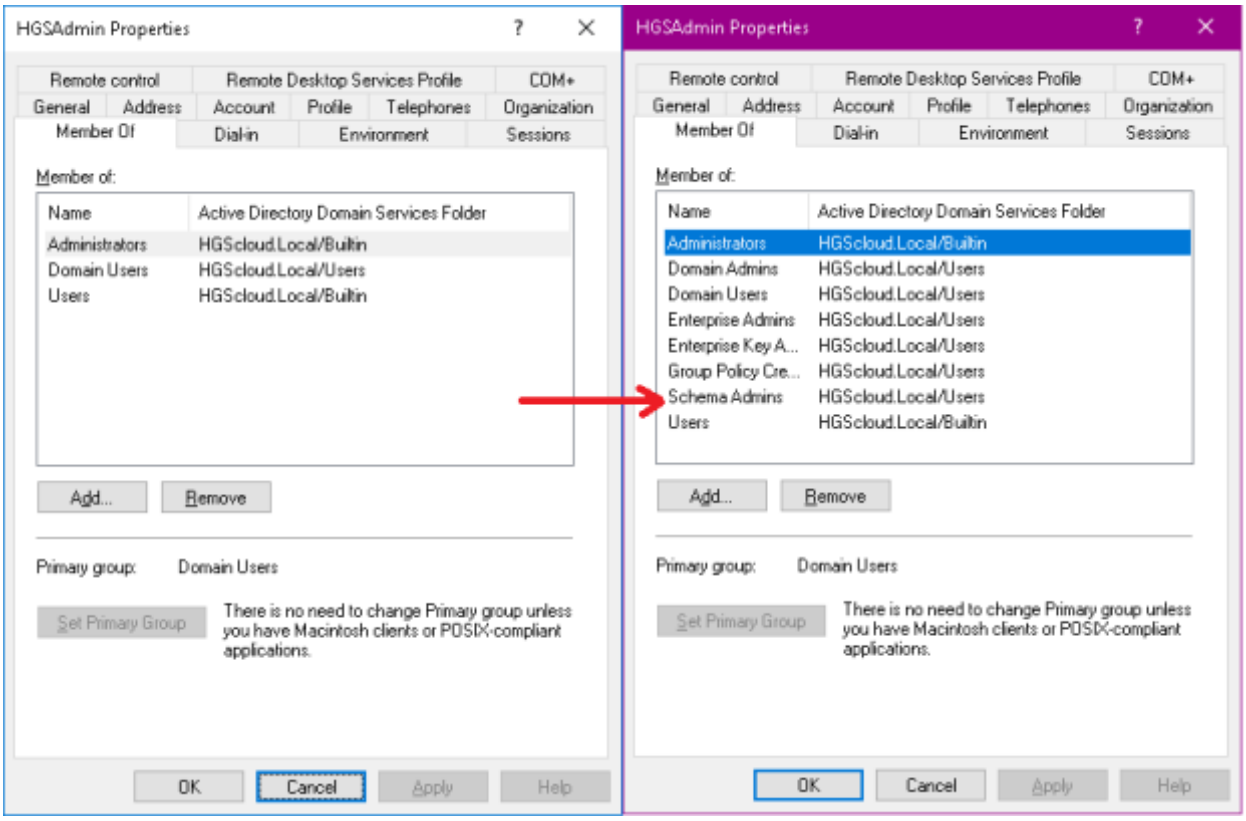
Export-PfxCertificate -FilePath .\encCert.pfx -Password $certpass -Cert $encCert



Here are the certificates:



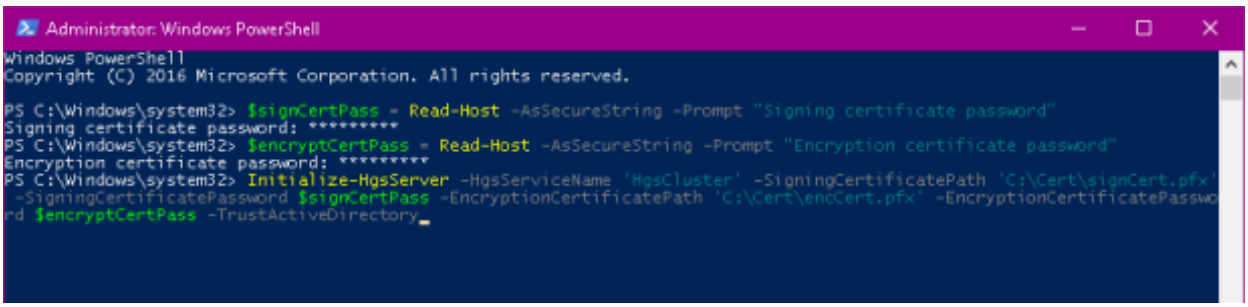
Now that the service is installed and the certificates are in place it's time to initialize the hgs server. As I was logged on to HGS server as hgsadmin user account which was NOT the default administrator account I had to add that account to the Schema Admins default group (as well as to other administrative groups) – my first attempt had ended with Access Denied error because HGSadmin was the member of only the Administrators and Domain Admin groups. After adding it to all other administrative groups (especially to the Schema Admins) the initialization has completed successfully:

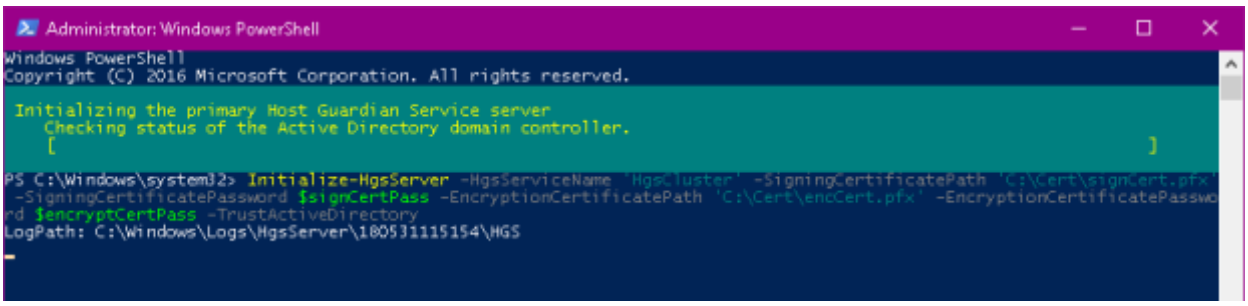


Advertisements
Report this adPrivacy
$signCertPass = Read-Host -AsSecureString -Prompt “Signing certificate password”

$encryptCertPass = Read-Host -AsSecureString -Prompt “Encryption certificate password”

Initialize-HgsServer -HgsServiceName ‘HgsCluster’ -SigningCertificatePath ‘C:\Cert\signCert.pfx’ -SigningCertificatePassword $signCertPass -EncryptionCertificatePath ‘C:\Cert\encCert.pfx’ -EncryptionCertificatePassword $encryptCertPass -TrustActiveDirectory

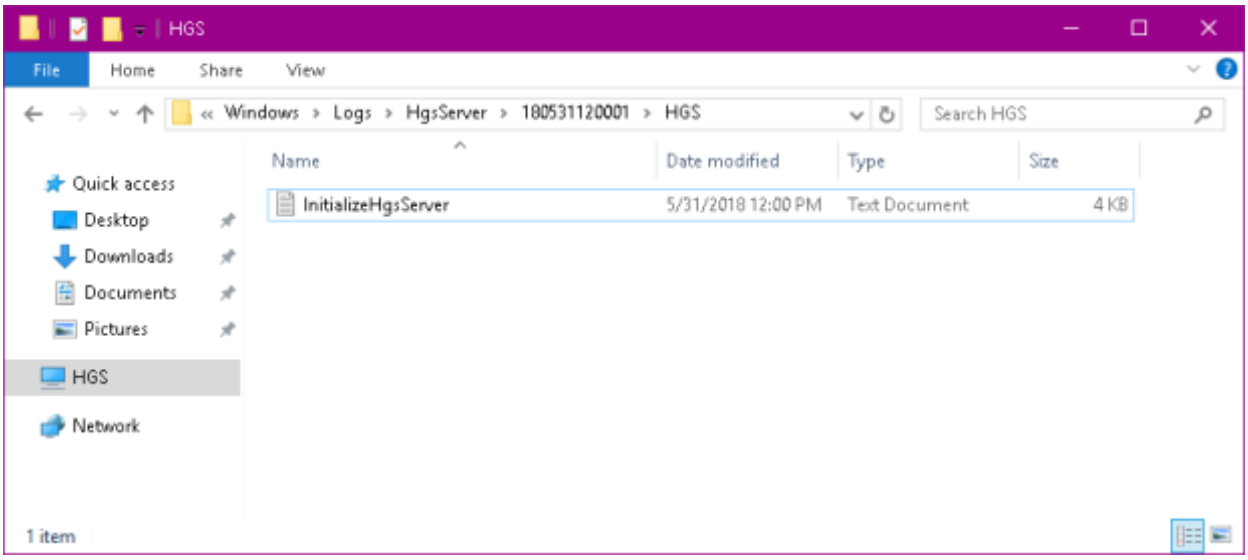


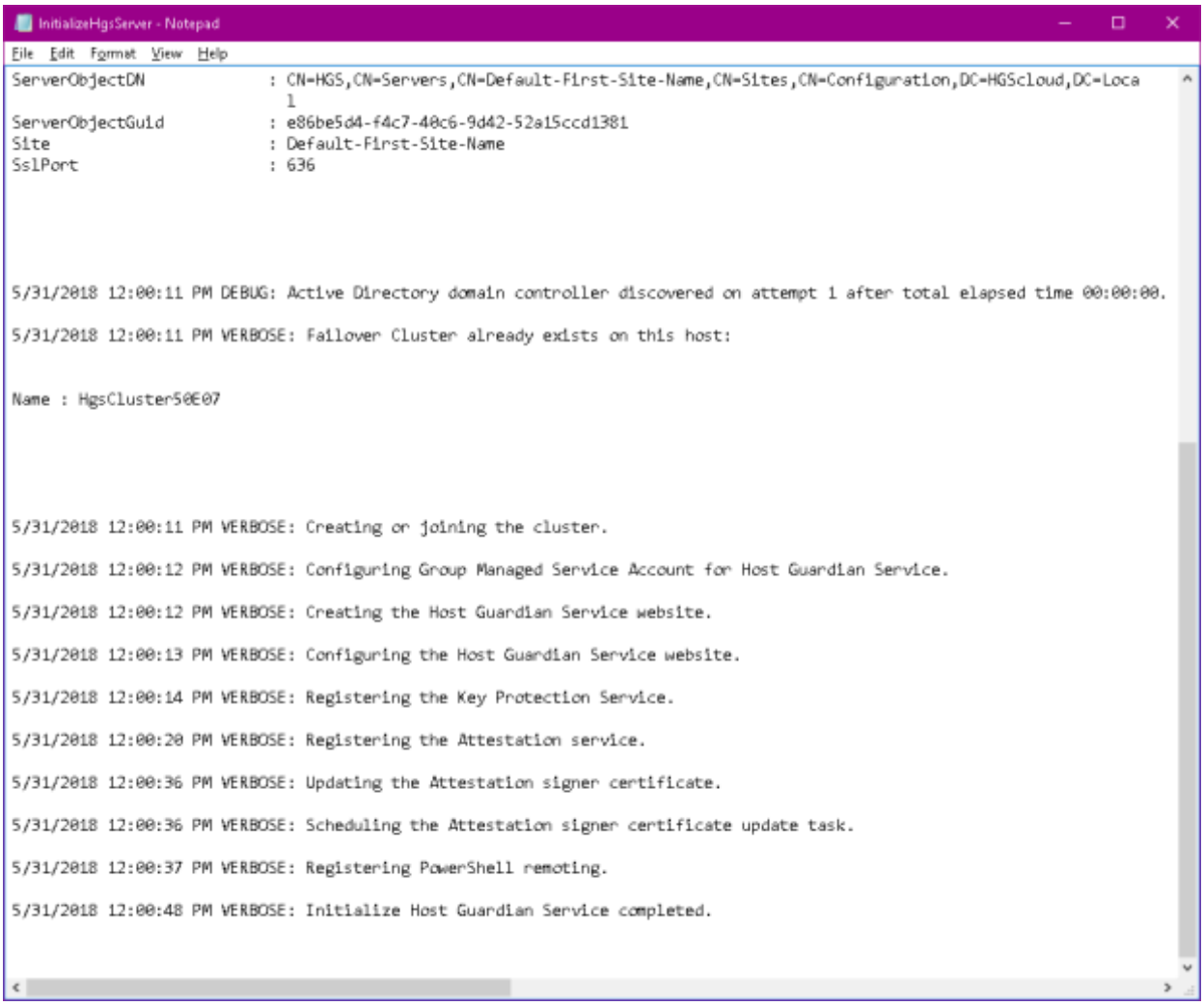


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $signCertPass = Read-Host -AsSecureString -Prompt "Signing certificate password"
Signing certificate password: ********
PS C:\Windows\system32> $encryptCertPass = Read-Host -AsSecureString -Prompt "Encryption certificate password"
Encryption certificate password: ********
PS C:\Windows\system32> Initialize-HgsServer -HgsServiceName 'HgsCluster' -SigningCertificatePath 'C:\Cert\signCert.pfx'
 -SigningCertificatePassword $signCertPass -EncryptionCertificatePath 'C:\Cert\encCert.pfx' -EncryptionCertificatePasswo
rd $encryptCertPass -TrustActiveDirectory
LogPath: C:\Windows\Logs\HgsServer\180531120001\HGS
PS C:\Windows\system32>
```

I think it would be pertinent to read the log created in the folder C:\Windows\Logs\HgsServer\180531120001\HGS as written above:





InitializeHgsServer - Notepad

File Edit Format View Help

```
ServerObjectDN              : CN=HGS,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=HGScloud,DC=Loca
                              l
ServerObjectGuid            : e86be5d4-f4c7-40c6-9d42-52a15ccd1381
Site                        : Default-First-Site-Name
SslPort                     : 636




5/31/2018 12:00:11 PM DEBUG: Active Directory domain controller discovered on attempt 1 after total elapsed time 00:00:00.

5/31/2018 12:00:11 PM VERBOSE: Failover Cluster already exists on this host:


Name : HgsCluster50E07




5/31/2018 12:00:11 PM VERBOSE: Creating or joining the cluster.

5/31/2018 12:00:12 PM VERBOSE: Configuring Group Managed Service Account for Host Guardian Service.

5/31/2018 12:00:12 PM VERBOSE: Creating the Host Guardian Service website.

5/31/2018 12:00:13 PM VERBOSE: Configuring the Host Guardian Service website.

5/31/2018 12:00:14 PM VERBOSE: Registering the Key Protection Service.

5/31/2018 12:00:20 PM VERBOSE: Registering the Attestation service.

5/31/2018 12:00:36 PM VERBOSE: Updating the Attestation signer certificate.

5/31/2018 12:00:36 PM VERBOSE: Scheduling the Attestation signer certificate update task.

5/31/2018 12:00:37 PM VERBOSE: Registering PowerShell remoting.

5/31/2018 12:00:48 PM VERBOSE: Initialize Host Guardian Service completed.
```

The deployment of the HGS service is complete. In Part2 of this series we'll move on to configuring guarded hosts.