

Microsoft Host Guardian Service (HGS)

INTEGRATION GUIDE



Document Information

Document Part Number	007-013769-001
Release Date	February 2019

Revision History

Revision	Date	Reason
B	February 2019	Update

Trademarks, Copyrights, and Third-Party Software

© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- > The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages

resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE	5
Scope	5
Document Conventions.....	5
Command Syntax and Typeface Conventions	6
Support Contacts	7
Customer Support Portal	7
Telephone Support	7
Email Support	7
CHAPTER 1: Introduction	8
Understanding the Microsoft HGS	8
Supported Platforms	9
Prerequisites	9
Configuring SafeNet Luna HSM	9
Provision your HSM on Demand Service	10
Microsoft HGS Setup	11
CHAPTER 2: Integrating Microsoft HGS with SafeNet HSM	12
Setting up SafeNet HSM with Microsoft HGS	12
Before You Begin.....	12
Create a Shielded VM Using an Existing VM	19

PREFACE

This document is intended to guide administrators through the steps for using a SafeNet Luna HSM or an HSM on Demand service with Microsoft Host Guardian Services (HGS) for securing the Key Protection Services (KPS) keys.

Scope

This guide provides instructions for setting up a small test lab with Microsoft HGS running with SafeNet Luna HSM and HSM on Demand service for securing the KPS keys. It demonstrates installation and configuration required for setting up Microsoft HGS while storing KPS keys on SafeNet HSM.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION! Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury

Command Syntax and Typeface Conventions

Convention	Description
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Window titles (On the Protect Document window, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document. For example: Refer to “ Error! Reference source not found. ” on page Error! Bookmark not defined.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a b c] [<a> <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a b c } { <a> <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Gemalto Customer Support](#).

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: Introduction

This guide demonstrates the installation and configuration of HGS in Windows Server 2016 using SafeNet HSM or HSM on Demand service.

This integration guide describes how to store Key Protection Service (KPS) keys on a SafeNet HSM partition. The Key Protection Service (KPS) is one of the two services that run as part of Host Guardian Service (HGS). A Hyper-V host is known as a “guarded host” once the Attestation service affirmatively validates its identity & configuration. Once affirmatively attested, the Key Protection service provides the transport key (TK) needed to unlock & run Shielded VMs.

The KPS keys stored on the HSM are backing the HGS certificates and protecting the Transport Keys.

The benefits of using an HSM with Microsoft HGS include:

- > Secure generation, storage, and protection of the KPS keys on FIPS 140-2 level 3 validated hardware.*
- > Full life cycle management of the keys.
- > HSM audit trail.**
- > Take advantage of cloud services with confidence.

*FIPS validation in progress for HSMoD services.

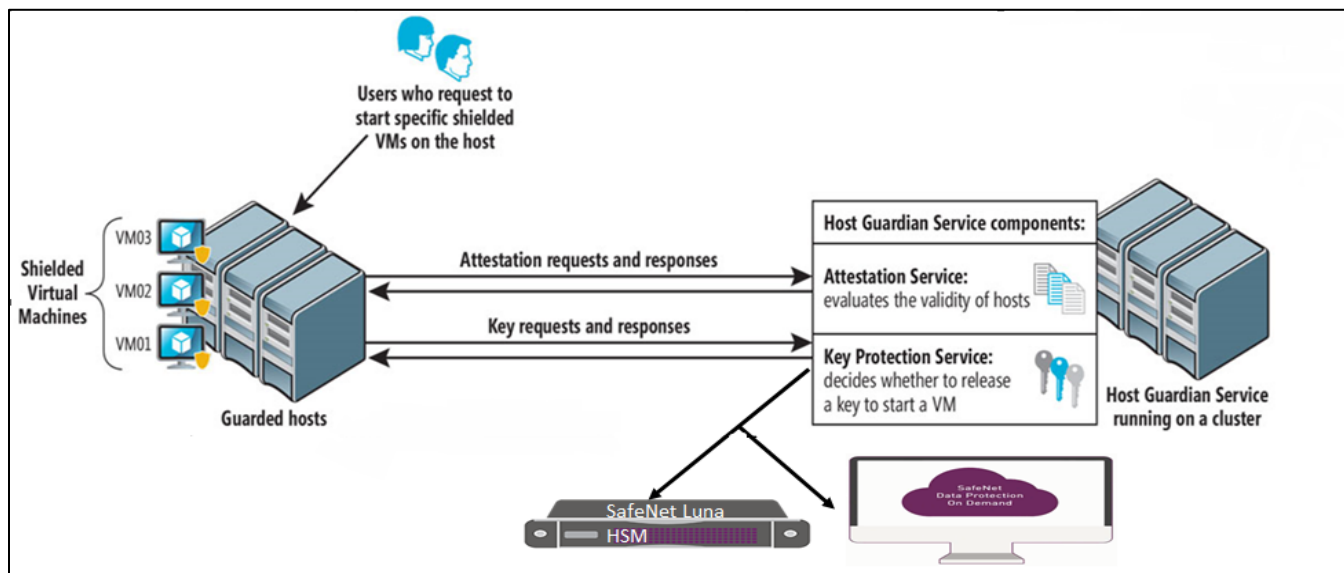
**HSMoD services do not have access to the secure audit trail.

Understanding the Microsoft HGS

The Host Guardian Service (HGS) is a server role introduced in Windows Server 2016 for configuring guarded hosts and running shielded VMs (shielded virtual machines) in Windows Server and System Center Virtual Machine Manager.

The Host Guardian Service Role specifically provides Attestation and Key Protection services that are needed to enable Hyper-V to run Shielded VMs. The Attestation services validate a Hyper-V host as a “guarded host”, which then enables the Key Protection service to provide the transport key required to unlock and subsequently run Shielded VMs.

The Host Guardian Service serves as a critical security component in protecting the transport key, and works in conjunction with other Windows Server 2016 components to ensure high security levels for Shielded VMs.



Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: It is a standalone network-attached appliance that physically and logically secure cryptographic keys and cryptographic processing. The purpose of an HSM is to protect sensitive data from being stolen by providing a highly secure operation structure. HSMs are fully contained and complete solutions for cryptographic processing, key generation, and key storage.

This integration is supported/verified with SafeNet Luna HSM on the following operating systems:

- > Windows 2016 Server Datacenter

SafeNet Data Protection on Demand (DPoD): It is a cloud-based platform that provides on-demand HSM and key management services through a simple graphical user interface. With DPoD, security is simple, cost effective, and easy to manage because there is no hardware to buy, deploy, and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain only the services that you need.

This integration is supported/verified with SafeNet DPoD on the following operating systems:

- > Windows 2016 Server Datacenter

NOTE: This Integration is supported in non-FIPS mode only.

Prerequisites

Configuring SafeNet Luna HSM

Before you get started ensure the following:

1. Ensure the HSM is setup, initialized, provisioned and ready for deployment. Refer to the *HSM product documentation* for help.
2. Create a partition on the HSM that will be later used by Microsoft HGS.

3. If using a SafeNet Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partition is:

```
# /usr/safenet/lunaclient/bin/lunacm
```

```
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```
Slot Id ->          0
Label ->           HGS
Serial Number ->   1213475834492
Model ->           LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration ->   Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
```

```
Current Slot Id: 0
```

NOTE: Follow the *SafeNet Network Luna HSM documentation* for detailed steps for creating NTLS connection, initializing the partition and various user roles.

Provision your HSM on Demand Service

This service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

To use the HSM on Demand service you need to provision your application partition, starting by initializing the following roles:

- > **Security Officer (SO)** - responsible for setting the partition policies and for creating the Crypto Officer.
- > **Crypto Officer (CO)** - responsible for creating, modifying and deleting crypto objects within the partition. The CO can use the crypto objects and create an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.
- > **Crypto User (CU)** - optional role that can use crypto objects while performing cryptographic operations.

HSM on Demand Service in Non-FIPS mode

HSMoD services operate in a FIPS and non-FIPS mode. Ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the *Mechanism List* in the *SDK Reference Guide* for more information about available FIPS and non-FIPS algorithms.

Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send the commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use slot list to determine which slot numbers are in use by which HSMoD service.

Microsoft HGS Setup

For more detail about Microsoft HGS features, Shielded VMs, guarded fabric, guarded hosts, pre-requisites and deployment please read Microsoft online documentation. The Microsoft HGS deployment guide is available at:

<https://technet.microsoft.com/en-us/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vm-top-node>

1. This guide provides steps to set up Microsoft HGS using SafeNet HSM as below: The setup comprises the following systems in a network as per the table below:

Operating System	Applications and Services	Description	Computer Name
Windows Server 2016 Datacenter Edition	Active Directory, Domain Name System (DNS)	Domain Controller for Active Directory Trust	FABRIKAD
Windows Server 2016 Datacenter Edition	Microsoft HGS	HGS Server	HGSAD
Windows Server 2016 Datacenter Edition	Hyper-V	Guarded Host to deploy shielded VMs	HYPERV1
Windows Server 2016 Datacenter Edition	Hyper-V	Tenant Host for VMs	HYPERV2

2. Create a Windows Server 2016 machine named FABRIKAD. It becomes your AD domain controller with domain name fabrikam.com.
3. Create a Windows Server 2016 machine named HGSAD. It becomes your HGS Server with domain name relecloud.com.
4. Create a Windows Server 2016 machine named HYPERV1. It becomes your Hyper-V server that joined in fabrikam domain to become the guarded host.
5. Create a Windows Server 2016 machine named HYPERV2. It becomes your Hyper-V server that is used to deploy the VM and this VM is migrated to the guarded host to demonstrate the shielded VM protected by HGS server.

Microsoft HGS supports two modes of attestation:

- > Admin-Trusted Attestation based on Active Directory
- > TPM Attestation

This guide is used to setup the HGS in Admin Trusted Attestation only. In case you need TPM Attestation, follow the Microsoft documentation for prerequisites, hardware requirements and deployment.

CHAPTER 2: Integrating Microsoft HGS with SafeNet HSM

Setting up SafeNet HSM with Microsoft HGS

HSMs provide strong physical protection of secure assets, including keys, and should be considered a best practice when deploying HGS.

Before You Begin

Before installing the Microsoft HGS on HGSAD, configure your HSM partition on the machine as guided in the Prerequisites Section.

NOTE: You need to download the SafeNet KSP that supports HGS from the Gemalto Customer Support Portal. The part number for the patched SafeNet KSP DLL is: 630-010721-001 (SW PATCH,LUNASA TO CLIENT 6.3.0 WINDOWS,KSP FOR HGS,ALPHA1).

Download and replace the SafeNetKSP.dll in HGSAD Window's System32 folder.

To set up Microsoft HGS with SafeNet HSM

1. Install Active Directory Domain Services on **FABRIKAD** and promote this server to Domain Controller.
2. Add **HYPERV1** into the **FABRIKAM** domain.
3. Log on to the **HGSAD** as a user with administrative privileges.
4. On the HGS Server run the following command in Windows PowerShell console to add the HGS Role.

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

The server will automatically restart after installing the role.

5. Log on to the **HGSAD** again as a user with administrative privileges.
6. In an elevated Windows PowerShell console, run the following commands to install the Host Guardian Service and configure its domain.

```
$adminPassword = ConvertTo-SecureString -string "temp123#" -AsPlainText -force
# Install-HgsServer -HgsDomainName 'relecloud.com' -
SafeModeAdministratorPassword $adminPassword -Restart
```

The password you specify here will only apply to the Directory Services Restore Mode password for Active Directory; it will not change the password you log in with.

7. After the computer restarts, log in as the **RELECLOUD** domain administrator using the same password you previously used as the local administrator (regardless of the password you specified in the previous step).
8. Download the SafeNet KSP patch for HGS and extract the DLL from the package.

9. Replace the SafeNetKSP.dll in the **C:\Windows\System32** folder with patched SafeNetKSP.dll.
10. Navigate to the KSP installation folder "**<Client Installation Directory>\KSP**".
11. Run the **KspConfig.exe** (KSP configuration wizard).
12. Double-click **Register Or View Security Library** on the left side of the pane.
13. Browse the library "cryptoki.dll" available in the HSM Client installation folder and click **Register**.
14. On successful registration, a message "**Success registering the security library**" displays.
15. Double-click **Register HSM Slots** on the left side of the pane.
16. Enter the Slot password. Click **Register Slot** to register the slot for Domain\User. On successful registration, a message "**The slot was successfully and securely registered**" will display.
17. Register the slot for **NT_AUTHORITY\SYSTEM** under Domain\User.
18. Open the command prompt and run the following commands to create the certificate request for signing and encryption certificates.

```
# certreq -new request.inf signreq.txt
```

```
# certreq -new request.inf encrreq.txt
```

Where the contents of the request.inf file are as follows:

```
-----
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=HGSSigning.relecloud.com"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
Exportable = FALSE
MachineKeySet = True
KeySpec = 0
ProviderName = "SafeNet Key Storage Provider"
ProviderType = 0
KeyUsage = 0xA0
RequestType = PKCS10

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
OID=1.3.6.1.5.5.7.3.2
-----
```

Replace the "**CN=HGSSigning.relecloud.com**" to "**CN=HGSEncryption.relecloud.com**" while generating the certificate request for Encryption certificate.

19. After creating the certificate request, sign the certificate request with a CA and use the following commands to import the signed certificate to the certificate store.

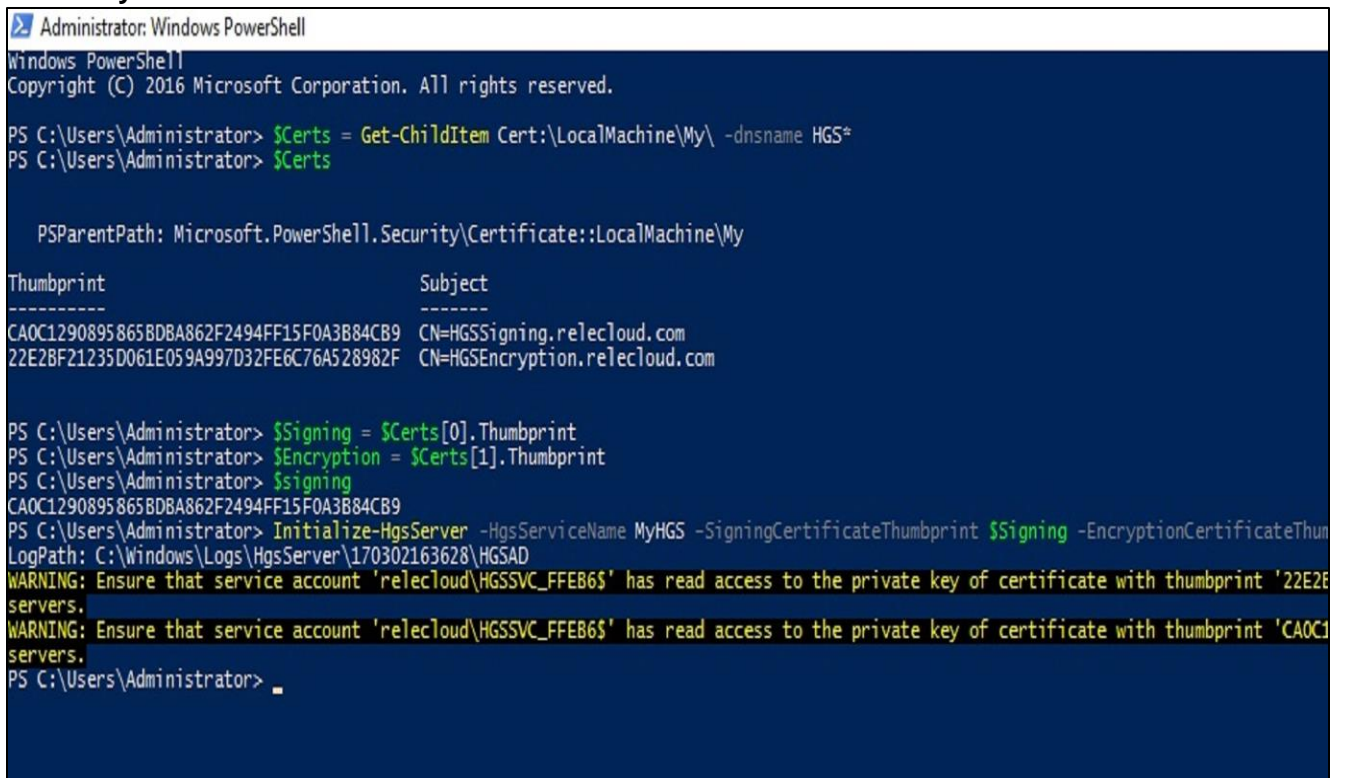
```
# certreq -accept sign.cer
# certreq -accept encrypt.cer
```

Ensure that certificate is imported successfully in the local machine's certificate store.

20. Open an elevated Windows PowerShell console, and then run the following commands to initialize the HGS server with the created encryption and signing certificates.

```
# $Certs = Get-ChildItem Cert:\LocalMachine\My\ -dnsname HGS*
# $Certs
# $Signing = $Certs[0].Thumbprint
# $Encryption = $Certs[1].Thumbprint
# Initialize-HgsServer -HgsServiceName MyHGS -SigningCertificateThumbprint
$Signing -EncryptionCertificateThumbprint $Encryption -TrustActiveDirectory -
Http -HttpPort 80
```

Where **MyHGS** is the name of HGS Service.



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

PS C:\Users\Administrator> $Certs = Get-ChildItem Cert:\LocalMachine\My\ -dnsname HGS*
PS C:\Users\Administrator> $Certs

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
CA0C1290895865BDBA862F2494FF15F0A3B84CB9  CN=HGSSigning.relecloud.com
22E2BF21235D061E059A997D32FE6C76A528982F  CN=HGSEncryption.relecloud.com

PS C:\Users\Administrator> $Signing = $Certs[0].Thumbprint
PS C:\Users\Administrator> $Encryption = $Certs[1].Thumbprint
PS C:\Users\Administrator> $Signing
CA0C1290895865BDBA862F2494FF15F0A3B84CB9
PS C:\Users\Administrator> Initialize-HgsServer -HgsServiceName MyHGS -SigningCertificateThumbprint $Signing -EncryptionCertificateThun
LogPath: C:\Windows\Logs\HgsServer\170302163628\HGSAD
WARNING: Ensure that service account 'relecloud\HGSSVC_FFEB6$' has read access to the private key of certificate with thumbprint '22E2E
servers.
WARNING: Ensure that service account 'relecloud\HGSSVC_FFEB6$' has read access to the private key of certificate with thumbprint 'CA0C1
servers.
PS C:\Users\Administrator> _
```

21. Now the GMSA user needs to register with the partition and provide the READ permissions on the keys. The GMSA User name will be displayed when HGS initialization completed. Copy the username without the domain name.

22. Run the following command from <Client Installation folder>\KSP> to enable Non-Administrative user access.

```
# kspcmd.exe n
```

This Servers Host Name is: WIN-ABHUT1L2CQG.recloud.com and the logged on user is: administrator@RECLOUD

Enable non admin user access to KSP (Y/N): y

Successfully set the non-admin user access to enabled.

- 23.** To register the GMSA user with the partition open Command Prompt and run the **kspcmd.exe** with following options and provide the partition password when prompted.

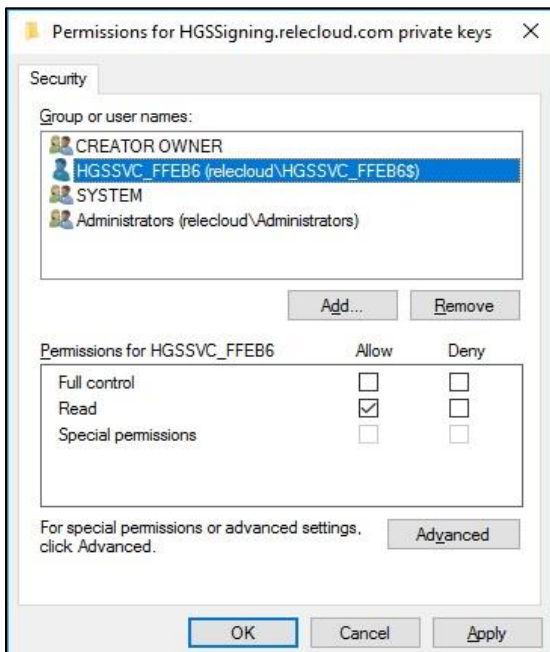
```
# kspcmd.exe password /s <slotLabel> /u <username> /d <domainName>
```

Where slotLabel = HSM Partition Name , username = GMSA User Name and domainName = HGS Domain

For example :

```
# kspcmd.exe password /s HGS /u HGS_SVCFEB6$ /d relecloud
```

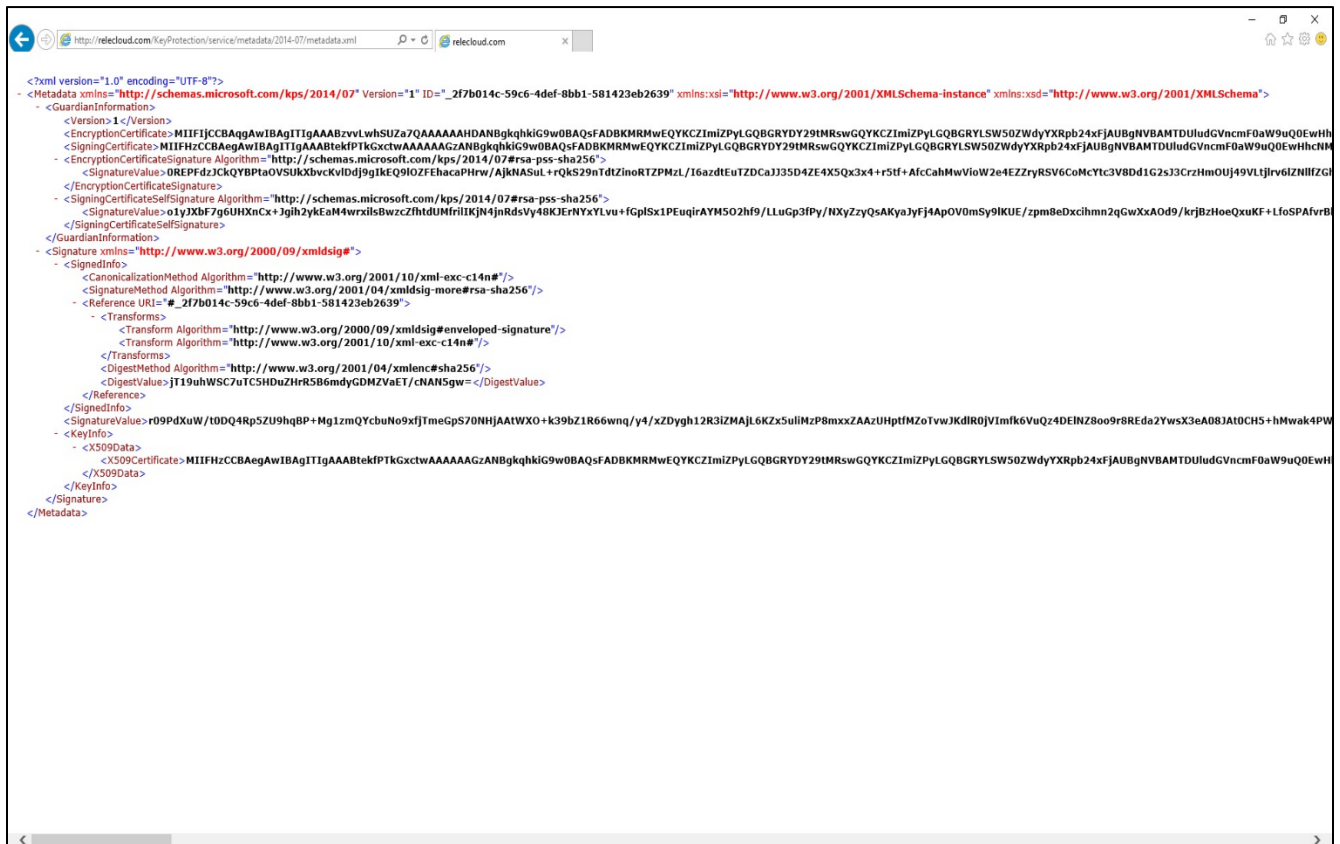
- 24.** Open the command prompt and type **certlm.msc** and press Enter.
- 25.** Expand **Certificates - Local Computer**. click **Personal -> Certificates**.
- 26.** Right click on the signing certificate. Click **All Tasks -> Manage Private Keys...**
- 27.** Click on **Add** button, Click **Object Types...** and select **Service Accounts** after that click **OK** button.
- 28.** Type HGSSVC in the **Enter the object name to select** text box and click **Check Names** button. It will display the GMSA user name. Click **OK**.
- 29.** Select GMSA user in **Group or user names** and select **Read** check box after that click **OK**.



- 30.** Repeat the same steps for the Encryption certificate to provide the Read permission to GMSA user.

31. Now open the Internet Browser and access the metadata. If the metadata is accessible then you have successfully initialized the Key Protection service using certificates backed by the HSM.

<http://relecloud.com/KeyProtection/service/metadata/2014-07/metadata.xml>



Admin-trusted attestation only - configuring DNS forwarding and domain trust

Use the following steps to set up necessary DNS forwarding from the HGS domain to the FABRIKAM domain, and to establish a one-way forest trust to the FABRIKAM domain. These steps allow the HGS to locate the FABRIKAM domain's domain controllers and validate group membership of the Hyper-V hosts.

1. To configure a DNS forwarder that allows HGS to resolve resources located in the fabric (host) domain, run the following command in an elevated PowerShell session.

```
# Add-DnsServerConditionalForwarderZone -Name "fabrikam.com" -ReplicationScope "Forest" -MasterServers <DNSserverAddress>
```

Replace `fabrikam.com` with the name of the fabric domain and type the IP addresses of DNS servers in the fabric domain.

2. To create a one-way forest trust from the HGS domain to the **FABRIKAM** domain, run the following command in an elevated PowerShell session:

```
# netdom trust relecloud.com /domain:fabrikam.com /userD:fabrikam.com\Administrator /passwordD:<password> /add
```

Replace `relecloud.com` with the name of the HGS domain and `fabrikam.com` with the name of the fabric domain. Provide the password for an admin of the fabric domain.

3. Log on to the **FABRIKAM** domain as an administrative privileges.

4. Open the PowerShell and add the relecloud domain.

```
# Add-DnsServerConditionalForwarderZone -Name "relecloud.com" -ReplicationScope
"Forest" -MasterServers <DNSserverAddress>
```

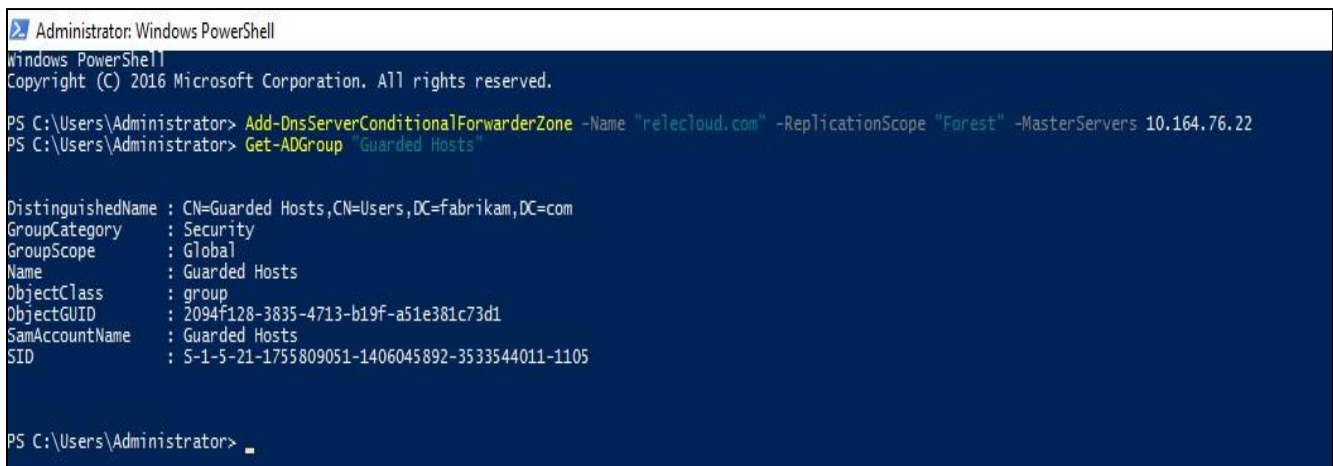
5. Log on to the **FABRIKAD** as a domain administrator and create a Global Security group "**Guarded Hosts**" in the Active Directory.

6. Add the **HYPERV1** into the created group "**Guarded Hosts**".

7. Restart the **HYPERV1** machine to enable the security policies.

8. On **FABRIKAD**, use Get-ADGroup to obtain the security identifier (SID) of the security group and provide it to the HGS administrator.

```
# Get-ADGroup "Guarded Hosts"
```



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

PS C:\Users\Administrator> Add-DnsServerConditionalForwarderZone -Name "relecloud.com" -ReplicationScope "Forest" -MasterServers 10.164.76.22
PS C:\Users\Administrator> Get-ADGroup "Guarded Hosts"

DistinguishedName : CN=Guarded Hosts,CN=Users,DC=fabrikam,DC=com
GroupCategory     : Security
GroupScope       : Global
Name             : Guarded Hosts
ObjectClass      : group
ObjectGUID       : 2094f128-3835-4713-b19f-a51e381c73d1
SamAccountName   : Guarded Hosts
SID              : S-1-5-21-1755809051-1406045892-3533544011-1105

PS C:\Users\Administrator> _
```

9. Log on to the **HGSAD** as a domain administrator and open the PowerShell and run the command to add HGS Attestation group.

```
# Add-HgsAttestationHostGroup -Name "Guarded Hosts" -Identifier "S-1-5-21-
1755809051-1406045892-3533544011-1105"
```

10. Now log on to the **HYPERV1** as domain administrator.

11. If the required role is not already installed. Install the Hyper-V role and Host Guardian Hyper-V Support feature, install them with the following command:

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

12. Configure the host's Key Protection and Attestation URLs on **HYPERV1**. Use the Fully Qualified Domain Name (FQDN) of your HGS cluster to get the HGS Cluster ask the HGS administrator to run the **Get-HgsServer** cmdlet on the HGS server to retrieve the URLs.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-HgsServer

Name                Value
----                -
AttestationOperationMode AD
AttestationUrl      {http://myhgs.relecloud.com/Attestation}
KeyProtectionUrl    {http://myhgs.relecloud.com/KeyProtection}

PS C:\Users\Administrator> _

```

13. On **HYPERV1**, configure the Key Protection and Attestation URLs by executing the following command in an elevated Windows PowerShell console.

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

14. Run the **Get-HgsClientConfiguration** cmdlet to see the status. Ensure that **IsHostGuarded** is **True** and **AttestationStatus** is **Passed**.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator.FABRIKAM> Get-HgsClientConfiguration

IsHostGuarded      : True
Mode                : HostGuardianService
KeyProtectionServerUrl : http://myhgs.relecloud.com/KeyProtection
AttestationServerUrl  : http://myhgs.relecloud.com/Attestation
AttestationOperationMode : ActiveDirectory
AttestationStatus    : Passed
AttestationSubstatus : NoInformation

PS C:\Users\Administrator.FABRIKAM> _

```

15. Log on to the **HGSAD** as a domain administrator.

16. Run the following command on PowerShell to confirm the status of HGS Diagnostic.

```
# Get-HgsTrace -RunDiagnostics
```

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-HgsTrace -RunDiagnostics
Overall Result: Warning
HGSAD: Warning
Certificates: Warning
KPS Certificate Permissions: Warning
>>> There was an error retrieving the permissions for the certificate with the subject "CN=HGSEncryption.relecloud.com" and thumbprint "E310469A294080BEC07C79FCE69C228CC2C6C96": The private key container for the certificate with thumbprint
>>> CN=HGSEncryption.relecloud.com could not be found. This could be caused by using a different key storage provider or even a hardware security module.
>>> There was an error retrieving the permissions for the certificate with the subject "CN=HGSSigning.relecloud.com" and thumbprint "6585D12DE8C06C7D404AA56E3888FECCFA9E009": The private key container for the certificate with thumbprint
>>> CN=HGSSigning.relecloud.com could not be found. This could be caused by using a different key storage provider or even a hardware security module.

Traces have been stored at "C:\Users\Administrator\AppData\Local\Temp\2\HgsDiagnostics-20170309-110533".

PS C:\Users\Administrator> _

```

A warning message indicates that there is an error receiving the permissions for the certificate. This error is expected for certificates backed by an HSM.

The Microsoft HGS integration with SafeNet HSM is complete. The next section demonstrates that the HGS service is working by creating a shielded VM using an existing VM.

Create a Shielded VM Using an Existing VM

This section demonstrates a scenario to create a shielded VM on a guarded host using an existing VM. This simulates a tenant taking an existing, unprotected VM and shielding it, and then moving it to a guarded host. You therefore require a running VM on a host which is not the guarded host. For clarity, the host machine which is not the guarded host will be referred to as the tenant host below.

A shielded VM can only run on a trusted guarded host. The trust is established by the adding the HGS guardian (retrieved from the HGS server) to the Key Protector which is then used to shield the VM. That way, the shielded VM can only be started after the guarded host successfully attests against the HGS server. For other scenarios, refer to the Microsoft documentation for Shielded VM using HGS.

1. Log on to the **HYPERV1** or any machine that can reach the HGS Server. The first step is to get the HGS guardian metadata from the HGS server, and use it to create the Key protector. To do this, run the following PowerShell command on a guarded host.

```
# Invoke-WebRequest
http://myhgs.relecloud.com/KeyProtection/service/metadata/2014-07/metadata.xml
-OutFile C:\HGSGuardian.xml
```

2. Copy the file **C:\HGSGuardian.xml** to the tenant host. i.e. **HYPERV2** which is not the guarded host.

Shield the VM

Each shielded VM has a Key Protector which contains one owner guardian, and one or more HGS guardians. The steps below illustrate the process of getting the guardians and creating the Key Protector in order to shield the VM.

1. Log on to the **HYPERV2** as administrative privileges. Run the following cmdlets on a tenant host.

```
# $VMName = 'SVM'
```

Where **SVM** is the VM name which to be shielded.

2. Turn off the VM first. You can only shield a VM when it is powered off.

```
# Stop-VM -VMName $VMName
```

3. Create an owner self-signed certificate.

```
# $Owner = New-HgsGuardian -Name 'Owner' -GenerateCertificates
```

4. Import the HGS guardian.

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

5. Create a Key Protector, which defines which fabric is allowed to run this shielded VM.

```
# $KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -
AllowUntrustedRoot
```

6. Enable shielding on the VM.

```
# Set-VMKeyProtector -VMName $VMName -KeyProtector $KP.RawData
```

7. Set the security policy of the VM to be shielded.

```
# Set-VMSecurityPolicy -VMName $VMName -Shielded $true
```

8. Enable vTPM on the VM.

```
# Enable-VMTPM -VMName $VMName
```

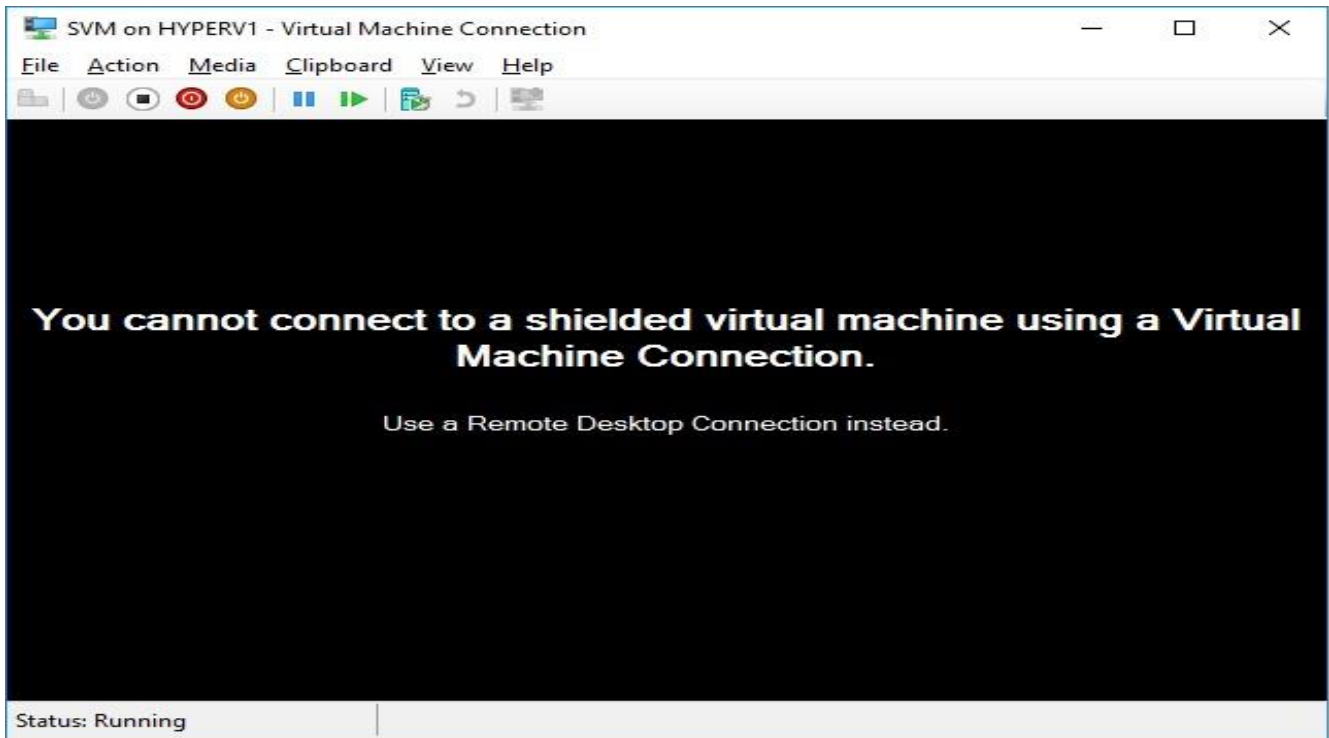
Typically you can run this command on the Guarded Host, to get the IP Address. After exporting the VM, you need to start the VM and note its IP address, because after the VM is encrypted, only remote connections are allowed.

To complete the process of shielding a VM, perform the following steps:

1. Shut down the shielded VM on tenant host.
2. Export the VM from the tenant host.
3. Copy the exported file to the guarded host and import it.
4. Start the VM on the guarded host.

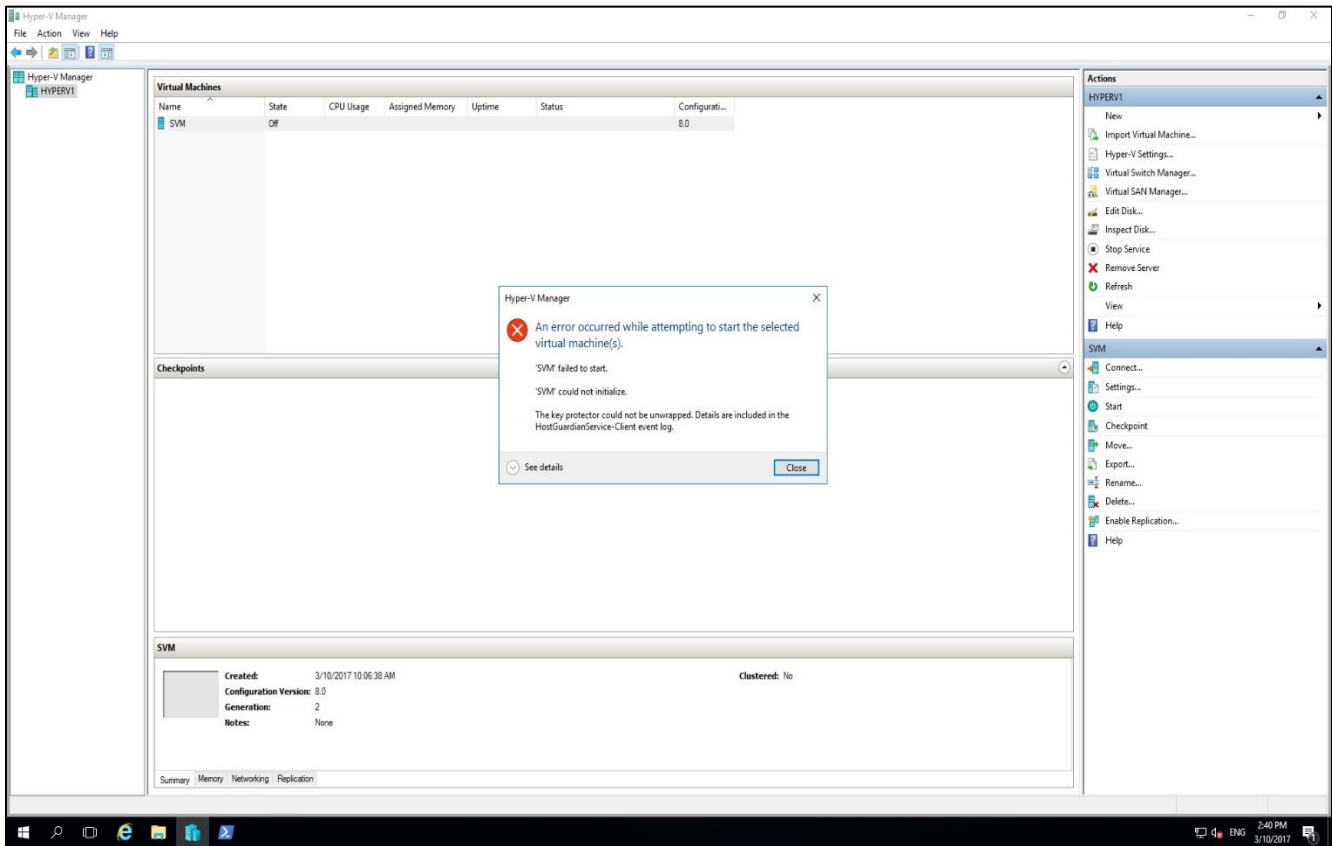
Test that HSM is protecting shielded VM

At this point, if you attempt to connect to the VM using Hyper-V Administrator, the connection fails and a message displays indicating that you must connect remotely.



If the VM is shielded then it can be started only after the attestation from HGS Server and when KPS releases the key required to start the VM. So, if we stop the HGS Server or stop the HSM client connection, KPS would not be able to release the key which is needed to start the VM.

If you suspend the HSM client connection, and try to start the shielded VM, it fails to start because the Host Guardian Service does not have access to keys stored on HSM, which are needed to decrypt the VM.



This completes the demonstration of a Shielded VM, shielded by an HGS Server that uses the SafeNet HSM to protect the KPS Signing and Encryption keys.