**Step 1: Components required for setting up a Shielded VM environment**

**2 HGS Cluster Nodes – (Hgslab.local)**

**HGS1 – 192.168.1.50**

**HGS2 – 192.168.1.51**

**1 DC – Pikachu.Local –192.168.1.1**

**2 Guarded Hosts Cluster**

**Compute1 – 192.168.1.2**

**Compute2 -192.168.1.3**

Diagram

Description automatically generated with medium confidence

Graphical user interface, diagram, text, application, Teams

Description automatically generated

**Step 2: Configuring HGS Node**

Enable Host Guardian Service role by opening windows PowerShell in a elevated mode and run the following command.

Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart

Install HGS Domain in its own forest by running the below command.

$SafeModeAdministratorPassword= ConvertTo-SecureString -AsPlainText '<password>' -Force

Note : Replace <Password> with HGS machine password.

Install-HgsServer -HgsDomainName ‘HGSLab.Local' -SafeModeAdministratorPassword $SafeModeAdministratorPassword -Restart

Note : Replace ‘HGSLab.local’ with a FQDN of your choice.

After machine reboot, log in with the domain account with the same password which you have used for the local account.

**Step 3: Initialize HGS Node**

For initializing HGS Node, administrator need to have a valid SSL certificate. For a lab environment, we can use self-signed certificate. But for production use, has to purchase SSL certificate from digital certificate Vendors.

#you can create CA in Bastion forest <https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-obtain-certs#request-certificates-from-your-certificate-authority>

$CertificatePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force

Note : Replace <Password> with HGS machine password.

$certificatePassword = ConvertTo-SecureString -AsPlainText -String "LS1setup!" -Force

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

Export-PfxCertificate -FilePath $env:temp\signCert.pfx -Password $certificatePassword -Cert $signCert

Remove-Item $signCert.PSPath

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

Export-PfxCertificate -FilePath $env:temp\encCert.pfx -Password $certificatePassword -Cert $encCert

Remove-Item $encCert.PSPath

Then, must initialize the HGS Node,

Initialize-HgsServer -HgsServiceName ‘MyHGS’ -SigningCertificatePath "C:\signCert.pfx" -SigningCertificatePassword $certificatePassword -EncryptionCertificatePath " C:\encCert.pfx" -EncryptionCertificatePassword $certificatePassword -TrustTpm -hgsversion V1

Set the DNS forwarder on the fabric DC so other nodes can find the new domain

<https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-configuring-fabric-dns>

Add-DnsServerConditionalForwarderZone -Name HGSLab.local -ReplicationScope Forest -MasterServers 192.168.1.50

Here Guarded domain fqdn is HGSLab.local with IP 192.168.1.50

To add the HGSLab.local to the trusted group, run the below command.

netdom trust HGSLab.local /domain: HGSLab.local /userD: HGSLab.local\Administrator /passwordD:<PASSWORD> /add

Note : Replace “<PASSWORD>” with appropriate credential details.

That’s it, you all done with HGS Server configuration, now connect to your Guarded domain controller.

**Step 4: Guarded Host configuration**

TPM-trusted attestation

Guarded hosts using TPM mode must meet the following prerequisites:

Hardware: One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

Hosts must have:

IOMMU and Second Level Address Translation (SLAT)

TPM 2.0

UEFI 2.3.1 or later

Configured to boot using UEFI (not BIOS or "legacy" mode)

Secure boot enabled

Operating system: Windows Server 2016 Datacenter edition or later

 Important

Make sure you install the [latest cumulative update](https://support.microsoft.com/help/4000825/windows-10-and-windows-server-2016-update-history).

Role and features: Hyper-V role and the Host Guardian Hyper-V Support feature. The Host Guardian Hyper-V Support feature is only available on Datacenter editions of Windows Server.

Add the Guarded Host into Pikachu.Local domain.

Install Host Guardian Feature on Guarded Hosts by using below Powershell.

Install-WindowsFeature HostGuardian -IncludeManagementTools

**Also generate attestation artifacts (CI policy, TPM EK, and TPM baseline)**

TPM mode uses a TPM identifier (also called a platform identifier or endorsement key [EKpub]) to begin determining whether a particular host is authorized as "guarded." This mode of attestation uses Secure Boot and code integrity measurements to ensure that a given Hyper-V host is in a healthy state and is running only trusted code. In order for attestation to understand what is and is not healthy, you must capture the following artifacts:

TPM identifier (EKpub)

This information is unique to each Hyper-V host

TPM baseline (boot measurements)

This is applicable to all Hyper-V hosts that run on the same class of hardware

Code integrity policy (an allowlist of allowed binaries)

This is applicable to all Hyper-V hosts that share common hardware and software

We recommend that you capture the baseline and CI policy from a "reference host" that is representative of each unique class of Hyper-V hardware configuration within your datacenter. Beginning with Windows Server version 1709, sample CI policies are included at C:\Windows\schemas\CodeIntegrity\ExamplePolicies.

<https://docs.microsoft.com/en-us/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-tpm-trusted-attestation-capturing-hardware>

Endorsement key for each guarded host needs to be added on HGS Sever, But only one copy of the baseline and CI policy, since they should be identical on both hosts

Add-HgsAttestationTpmHost -Path C:\attestationdata\TPM\_EK\_COMPUTE1.xml -Force

Add-HgsAttestationTpmHost -Path C:\attestationdata\TPM\_EK\_Compute2.xml -Force

Add TPM Baseline of a Guarded Host on HGS Server

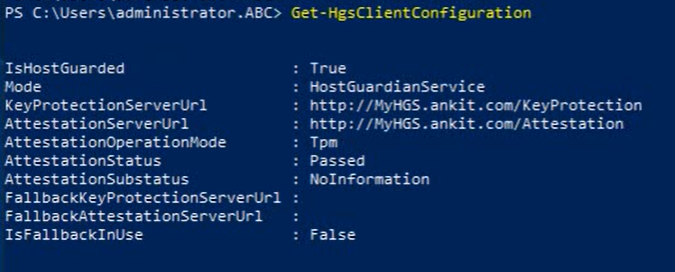
Add-HgsAttestationTpmPolicy -Path C:\attestationdata\TPM\_Baseline\_COMPUTE1.xml -Name "Hyper-V TPM Baseline1"

Add CI Policy of Guarded Host on HGS Server

Add-HgsAttestationCIPolicy -Path C:\attestationdata\CI\_POLICY\_AUDIT.bin -Name "AllowMicrosoft-AUDIT-CI1"

Once added we can check the host configuration by running below command.

Get-HgsClientConfiguration



Get-HgsTrace -RunDiagnostics -Detailed