DELL EMC

TPM 2.0 AND SHIELDED VIRTUAL MACHINES

ABSTRACT

Cloud security is one of the trending areas due to high adoption rates by small and huge businesses alike. Security of the virtual layer is very important from the customer's perspective as all the private data is hosted over virtual machines. This paper is aimed at describing the role of TPM 2.0 chip in guaranteeing the best security features to the VMs hosted in a third party environment in collaboration with the Hyper-V Shielded VM security feature introduced by Microsoft.

May, 2017

SHUBHRA RANA

VINAY PATKAR

TABLE OF CONTENTS

EXECUTIVE SUMMARY

When business units decide to move their infrastructure to the cloud, one of the biggest challenges that they face is data security. Physical host security can be guaranteed with the many security measures introduced recently, while the virtualized environment is slightly more difficult to secure. This is because the access to the virtualized environment is controlled by physical host administrators, which leaves them with a lot of chances to tamper with the data being hosted on the VMs. The need is to provide the VM owners with adequate security assurances by the service providers.

The Shielded VM feature by Microsoft is a promising breakthrough in providing requisite security controls at the virtualization level. This white paper elaborates on how shielded VM deployment can be done in the production environment by using a Microsoft tool called SC-VMM, which simplifies virtual machine provisioning and management.

Introduction

Today, more and more businesses are moving towards adoption and usage of Cloud Computing. Few of the important advantages of cloud computing are high availability, disaster recovery management, reduced downtime, and tremendous budget savings in terms of hardware provisioning and maintenance. When cloud computing came into existence, there were many risks associated, security of data being one of the primary ones. In the forthcoming years, the cloud providers and technical wizards around the world came up with stringent security mechanisms to make cloud services more and more secure. Few of the noticeable enhancements in this regard are homomorphic encryption, elliptic curve cryptography, steganography, data obfuscation, advanced access control and identity management.

However, most of the security mechanisms adopted were aimed at the physical host security, whereas it is in the public/private or hybrid cloud environments that the virtual machines hold most of the tenant's data. As cloud computing involves deploying the data and the associated process in a third party environment on a virtual layer, security of the virtualization layer becomes paramount. In this context, the concept of shielded VMs introduced by Microsoft is a breakthrough advancement in hardening the Hyper-V virtualization layer.

Shielded VMs: What are they ?

Shielded VMs are secure 2nd generation VMs that are designed to run on a specific set of hosts (called guarded hosts) that conform to specific standards such as UEFI and Secure Boot. Host Guardian Service (HGS), which is an external agency, is assigned with the task of validating whether the host on which the VM is being launched is a guarded host or not. The server or the cluster hosting the HGS service conducts this validation by using two key components called Attestation and Key Protection services.

- The Attestation service ensures that the host on which the VMs are run has all the valid security measures enabled and is entitled to run the VMs.
- The Key Protection service handles the locking and unlocking of the vTPM (Virtual TPM) associated with each module.

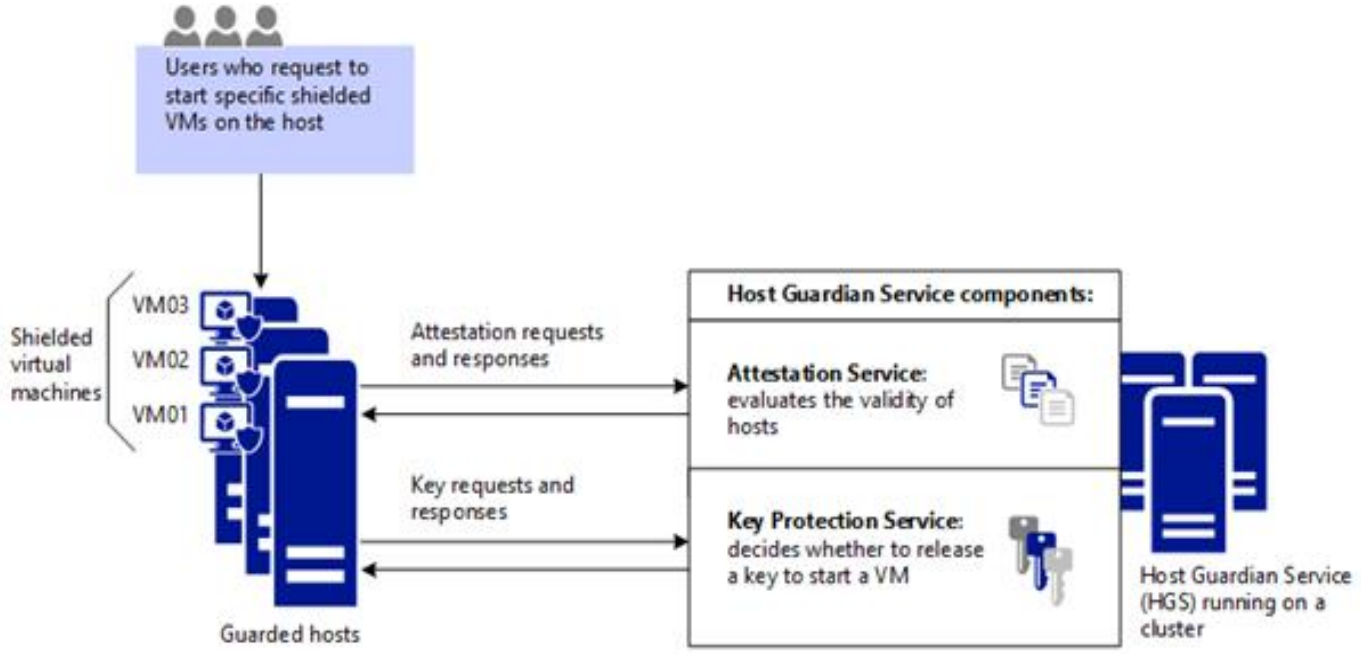

Figure 1. Shielded VM Environment

Source: https://technet.microsoft.com/en-us/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

Microsoft offers two different methods for attestation:

1. **Active Directory based attestation:** This attestation mechanism is based on the Active Directory group membership concept, and hence it is easy to configure in the existing data center scenarios where TPM 2.0 hardware components are not available. Though relatively easy to configure, it lacks the stringent security provisions as compared to the hardware based attestation mechanism.
2. **Hardware based attestation:** Hardware based attestation provides the highest security assurance and requires TPM 1.2 or 2.0 for Hyper-V Hosts. Though TPM 1.2 can be used, the recommendation is to use TPM 2.0. The guarded hosts are marked safe based on the TPM (Hardware) identity, pre-boot measurements and code integrity policies which collectively validate that only secure code is running on the physical hosts when the hosts are powered ON. The Host Hardware and firmware must include TPM 2.0 and UEFI 2.3.1(or later) with secure boot enabled.

Shielded VMs provide the following security assurances:

- Encrypted virtual hard disks ensure that there is no unauthorized access to the underlying data. Only the attested hosts can launch a shielded virtual machine. The concept of having a virtualized instance of TPM (vTPM) which is independent of physical hardware (i.e. physical TPM) ensures that the stringent security measures are applicable even during VM migration across hosts.
- Shielded VMs prevent code injection and any insecure code execution and hence safeguard against malware injection attacks.
- Even VM console connections and PowerShell Direct are blocked for Shielded VMs.

Note: Microsoft provides encryption supported VMs which supports Hyper-V console access and PowerShell Direct, thus providing greater flexibility to the VM owners. This is meant for scenarios where the Hyper-V owners are trusted by the VM owners (tenants).

The whole solution of shielded VM is designed to protect the tenant's data from being attacked by malicious or rogue administrators in a cloud environment.

Role of TPM

TPM plays a significant role in terms of securing platforms in hardware based attestation. In this mode of attestation, trust relationship between Hyper-V hosts and HGS server is established by using TPM and not Active Directory. The role of TPM in attestation is described below:

- Each Hyper-V host's identity is expressed with HGS by using a unique key called EK_{pub} or the public endorsement key found in the TPM chip. To get this key, run the PowerShell cmdlet Get-PlatformIdentifier on each Hyper-V host. To make a host as guarded host, add this key to HGS server by running the Add-HgsAttestationTpmHost cmdlet.
- To verify if the Hyper-V host is healthy, TPM uses the following:
    - Baseline policy – Contains measurements that describe the binaries that can be loaded by the Operating System during system boot.
    - Code-integrity (CI) policy – Contains whitelist binaries (drivers and tools) that are allowed to run on the Hyper-V host.

The steps to extract the baseline and code-integrity policies from each or one of the Hyper-V hosts TPM are outlined below:

1. Extract baseline policy from each Hyper-V host by using the Get-HgsAttestationBaselinePolicy cmdlet--for example:

    ```
    Get-HgsAttestationBaselinePolicy –Path 'c: \host.tcglog'
    ```

2. Add the baseline policy from each Hyper-V host to the HGS server by using the Add-HgsAttestationTpmPolicy cmdlet--for example:

    ```
    Add-HgsAttestationTpmPolicy –Path 'c: \host.tcglog' –Name 'HostTPMPolicy'
    ```

3. Use the New-CIPolicy cmdlet to generate code-integrity policy for each Hyper-V host [Can be done on one host also and applied across several hosts] and convert it into the format that is recognized or used by HGS by using ConvertFrom-CIPolicy--for example:

    ```
    New-CIPolicy –Level FilePublisher –Fallback Hash –FilePath 'CodeIntegrity.xml'

    ConvertFrom-CIPolicy –XmlFilePath 'CodeIntegrity.xml' –BinaryFilePath 'CodeIntegrity.p7b'
    ```

4. Use the Add-HgsAttestationCiPolicy cmdlet to add the code-integrity policy to HGS.

    ```
    Add-HgsAttestationCIPolicy -Path 'C: \CodeIntegrity.p7b' -Name 'HostCIPolicy'
    ```

When Hyper-V hosts attest with HGS, each host sends its EKpub to be authorized to host the shielded VMs. Baseline measurements contained within tcglog (Trustworthy Computing Group logs) are sent to the HGS server by each Hyper-V host. Tcglog contains a list of individually-measured binaries and the manner in which they are loaded. The Attestation process continues if HGS finds a match for tcglog to its database of known healthy baselines.

Next HGS uses a series of measurements contained within the tcglog to determine what values should the host's TPM have. HGS contacts the Hyper-V hosts to check whether the PCR values match with what it has computed. If they match, then attestation continues.

Lastly, the Hyper-V hosts send the hash value of its CI policies to HGS to compare with its database of known good CI-policies. If it matches with the HGS database, then attestation is complete and a certificate of health is sent back to the Hyper-V host which entitles the respective hosts to request the keys from HGS key protection service.

With TPM 2.0, the HGS service provides the following additional functionalities:

- A key that identifies the host (with EK_{pub}) and checks if the host is trustworthy (determined by baseline and CI policy measures)
- Cryptographically verified list of binaries
- Host's CI policy

TPM 1.2 vs TPM 2.0

TPM 2.0 chips have been given higher priority over TPM 1.2 for hardware based attestation for the following reasons:

- TPM 2.0 provides a wide range of secure algorithms unlike TPM 1.2 algorithms that provide limited crypto:
  - One hash algorithm (SHA1 + HMAC)
  - One asymmetric algorithm – RSA (ENC, SIG and DAA) has shown signs of weakness
- With TPM 2.0, the manufacturer can add any algorithms with TCG IDs.
- With respect to functions, TPM 2.0 provides three separate domains, and each domain has its own resources and controls:
  - Security – Functions that protect the security of the OS/application user by *ownerAuth*, storage hierarchy, hierarchy enable (*shEnable*)
  - Platform – Functions that protect the integrity of the platform/firmware BIOS/UEFI services by *platformAuth*, platform hierarchy, *phEnable*
  - Privacy – Functions that expose the identity of the platform/user by using resources and controls *endorsementAuth*, endorsement hierarchy, *ehEnable*.

The advantage provided by the same is that each domain (platform/OS/User) can execute separate ownership compared to TPM 1.2 where the ownership is controlled by the OS only. Hence TPM 2.0 presents a more secure and flexible architecture compared to TPM 1.2.

The following table outlines the key security features and requirements for both the attestation methods:

	AD BASED ATTESTATION	**HARDWARE BASED ATTESTATION**
Hyper-V host and Hardware	Windows Server 2016 Data center	• Windows Server 2016 Data center • UEFI 2.3.1 rev. C or later • Secure boot / measure boot • TPM v2 **Note:** TPM 2.0 mandatory for hardware based attestation
Attestation and protection to run a shielded VM	Hyper-V VM must be a member of the designated / trusted AD group	• UEFI firmware with secure, measure boot support • Hosts Operating System and drivers • Encrypted disk with secure, TPM based key-release • Encrypted live migration • Host's code-integrity policy

TPM 2.0 provides a wider and more secure set of algorithms (such as elliptic curve cryptography, SHA-256, etc.) for the internal functionalities of TPM. Moreover, the TPM 2.0 chip architecture supports three different ownership hierarchies as compared to a single owner entity model supported in TPM 1.2. Hence, TPM 2.0 provides a more flexible architecture where the end users can modify and use different cryptographic algorithms as deemed fit for their applications. For more details, please see the link [5].

Dell supported platforms for TPM 1.2 and 2.0

Dell EMC is happy to announce the certified list of Power Edge Servers that support TPM 1.2 and TPM 2.0. All the listed platforms have achieved the "*Hardware Assurance*" logo. Go to the below link for supported platforms for "*Hardware Assurance*" feature and how to enable TPM in Dell EMC Power Edge Servers.

http://en.community.dell.com/techcenter/b/techcenter/archive/2016/11/10/dell-poweredge-servers-certified-for-windows-server-2016.

Shielded VM: Configuration and Management

Shielded VMs can be configured and managed in several ways as given below:

- Native PowerShell method
- Using SCVMM
- Using Azure Portal
- OpenStack method

Even if the customer has existing VMs in their infrastructure, they can be converted to shielded VMs. Following are the steps required in setting up the environment by using SCVMM:

1. Guarded Host Creation
2. Shielded VM deployment or Shielding of Existing VMs

Guarded Hosts are the ones that support shielded VMs. Perform the following steps to Tadd and provision the guarded host by using VMM:

1. Specify the HGS and related settings as shown in Figure 2.

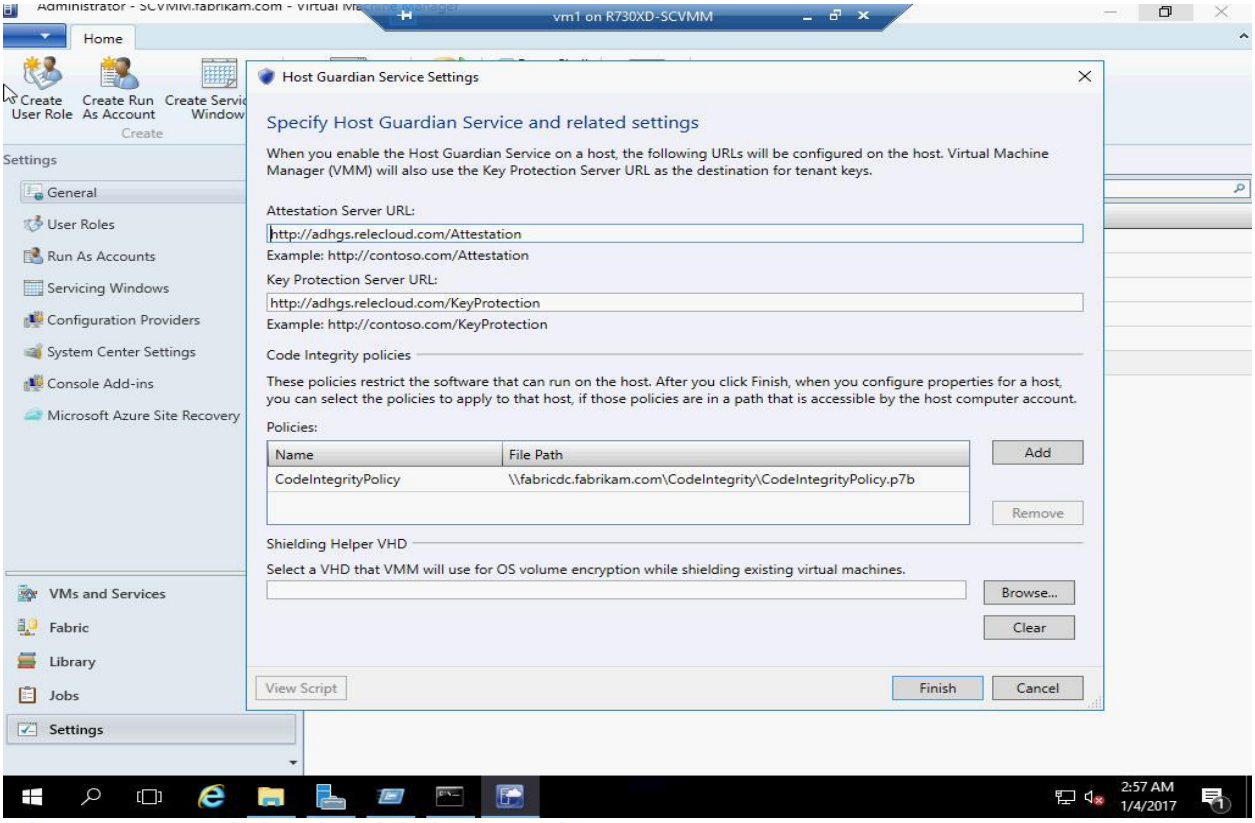

Figure 2. Specifying the Global HGS settings

2. On the VMM, configure the HGS related settings with the Attestation Server URL and the Key Protection Server URL. These URLs will be used by the guarded hosts to communicate with the HGS node to have the attestation and key protection service functionality provided.

3. Specify the Code Integrity Policy that should be used as the standard for the guarded hosts.

Once the related settings are configured on the SCVMM, the hosting service provider is able to routinely review the health status of the guarded hosts.

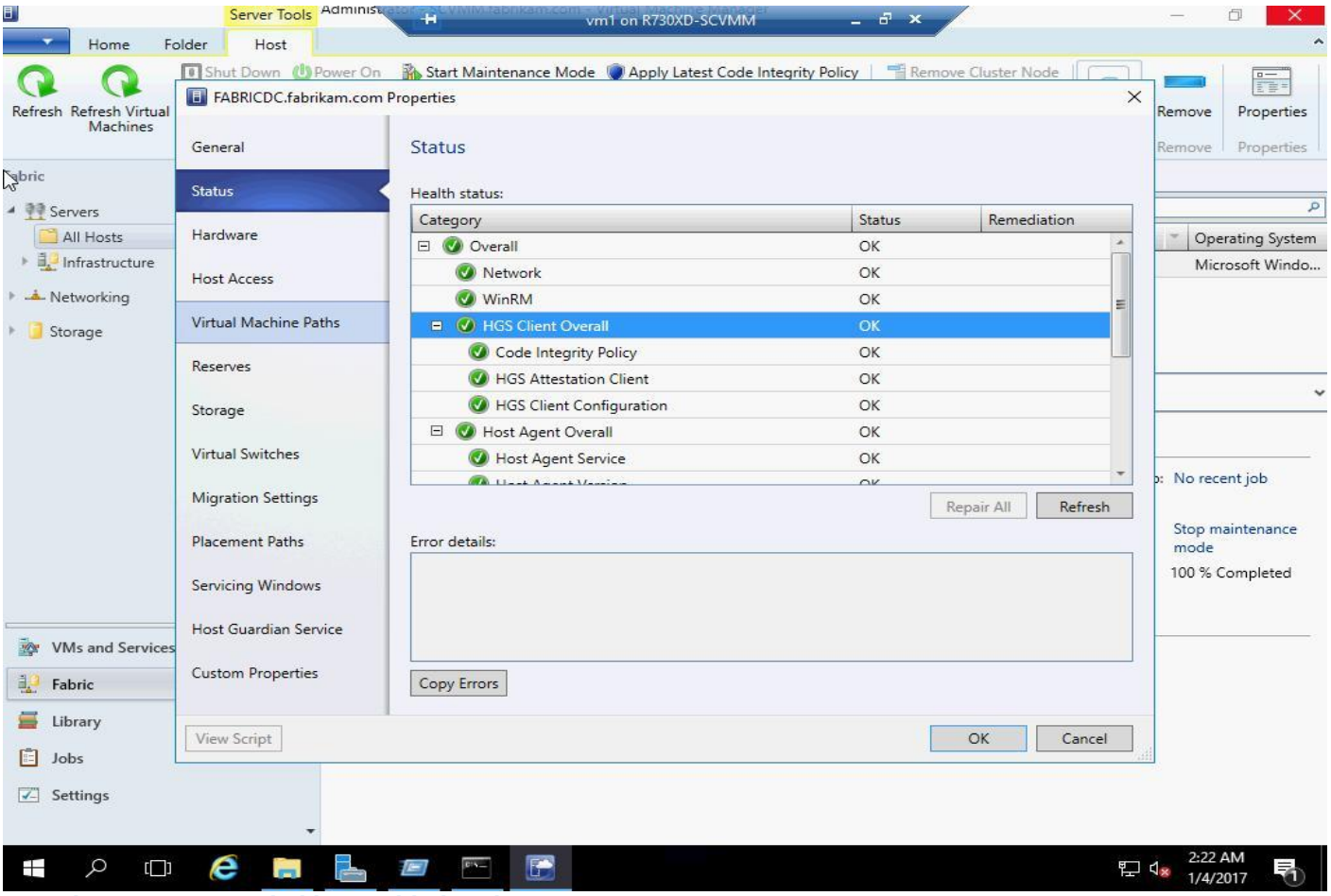

Figure 3. Guarded host added to the setup

Conclusion

Securing the virtual layer is very important when it comes to cloud based environment. Shielded VMs, a unique security offering by Microsoft, is a very promising breakthrough in the world of virtualization security. This feature from Windows Server 2016 has brought new hopes to hosting providers who can, in turn, provide better security guarantees to customers who have hosted virtual machines in their environment and hence, attract more customers. Hosting Service Providers can make use of Virtual Machine Manager to provision and monitor the shielded VMs. Adoption of the shielded VM feature in the open source world (already initiated in OpenStack) is another way to boost the cloud adoption rates.

References

- https://technet.microsoft.com/en-us/windows-server-docs/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms
- Arthur, Will, David Challener, and Kenneth J Goldman. A Practical Guide to TPM 2.0 using the Trusted Module in the New Age of Security. 1st ed. Print.
- http://www.alex-ionescu.com/blackhat2015.pdf
- https://cloudbase.it/hyperv-shielded-vms-part-1/
- http://en.community.dell.com/techcenter/enterprise-client/w/wiki/11849.tpm-1-2-vs-2-0-features