Microsoft

Securing Windows Server 2016

Exam Ref 70-744

Timothy L. Warner
Craig Zacker

Microsoft

Exam Ref 70-744 Securing Windows Server 2016

Timothy Warner
Craig Zacker

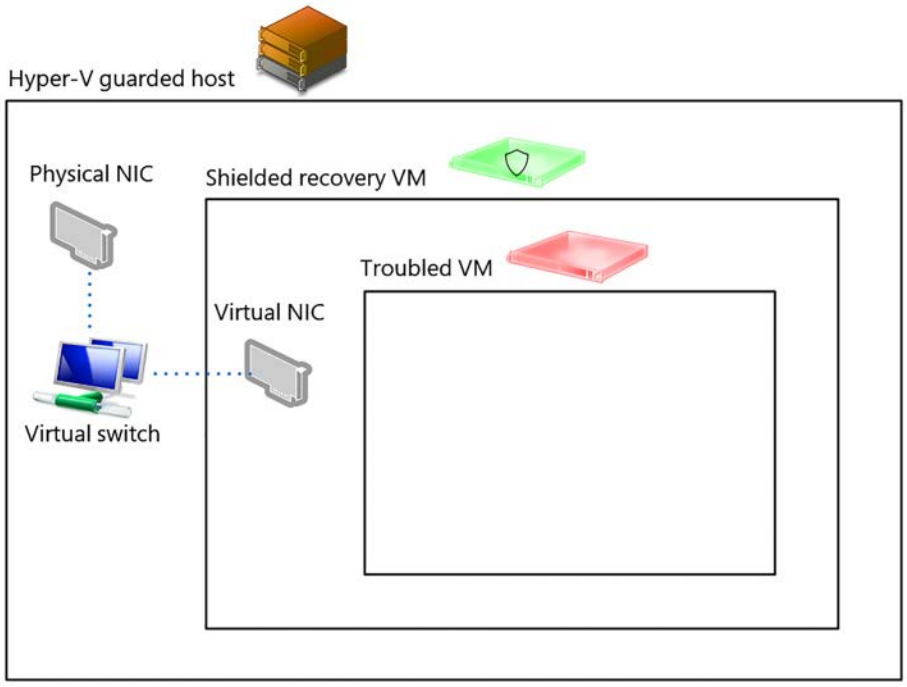

FIGURE 2-12 Conceptual diagram of shielded VM recovery

In Figure 2-12, we start from the perspective of a Hyper-V hardware host that's connected to an Internal Hyper-V switch. We create a dedicated, shielded recovery VM that has nested virtualization enabled. Incidentally, you can enable nested virtualization on a VM by running the following PowerShell command from the host:

```
Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
```

It's important for you to know that you must disable dynamic memory on the virtual machine, and that you need to allocate enough host RAM to cover any nested VMs you plan to run on the virtual Hyper-V host.

NOTE **OTHER USES FOR NESTED VIRTUALIZATION**

Nested virtualization refers to the capacity of a virtual machine to become a virtualization host itself. This is a feature that customers asked Microsoft about for many years, and it's great that we finally have it in Windows Server 2016.

With host hardware being so powerful nowadays, it makes sense to deploy virtualized Hyper-V hosts Going further, shared storage has become much more affordable in Windows Server 2016, so it's almost trivial to deploy highly available virtual machines that themselves spring from the nested virtualization scenario. Finally, in today's age of rapid application development and continuous integration, developers appreciate being able to deploy "second level" VM pods from "first level" VMs to which they have access.

The recovery process

Okay. So we've created a shielded recovery VM (with nested virtualization enabled) that's also connected to the aforementioned internal Hyper-V switch. Part of this scenario involves the understanding that the workload admins and fabric admins need to work cooperatively to enact this solution, and that the fabric admins don't get to tap into the troubled VM.

The fabric admin is responsible for deploying the recovery VM and exporting the troubled VM's VHDX file(s).

The workload admin then RDPs into the recovery VM and imports the troubled VM as a nested virtual machine.The workload admin then uses PowerShell to change the nested shielded VM's security policy to encryption-supported.

The workload admin then establishes a VM Connect console session from the recovery VM to the nested, troubled VM and fix whatever problems where present.

Finally, the fabric admin restores the previously troubled VM to the fabric and deletes the recovery VM.

Chapter summary

- The Host Guardian Service (HGS) is a new role in Windows System 2016 that allows for the creation and management of shielded virtual machines.
- The need for HGS and shielded VMs is based in the separation of duties between workload (VM) administrators and fabric (Hyper-V host) administrators and least-privilege security.
- HGS is deployed exclusively with PowerShell; Microsoft recommends at least three nodes per HGS cluster to support high availability.
- HGS and shielded VMs rely upon various hardware and software features (physical and virtual TPM, UEFI, Secure Boot, Hardware Security Module (HSM), and more.
- HGS has two main functions: attestation that a guarded host is healthy, and key transfer to lock and unlock shielded virtual machines.
- Local console access is blocked for shielded virtual machines, making pre-shielding VM configuration crucial to allow for remote management.
- Shielded VMs offer strong protection against fabric (host) administrators as well as compromised Hyper-V host servers themselves.
- Shielded VM deployment is inextricably tied to the presence and availability of a Host Guardian Service (HGS) cluster.
- The strong protections offered by shielded VMs have one potential downfall—no host console access could lead to connectivity and availability problems if the shielded VM isn't correctly configured.
- Encryption-supported VMs represent an approach that combines some of the shielded VM protections but preserves console access. However, this protection method involves trusting your fabric admins.

Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answer to this thought experiment in the next section.

You are a datacenter administrator for Contoso Solutions, a managed service provider (MSP) located in Buffalo, NY. Your newest client, Woodgrove Bank, has strict regulatory requirements that limit access to their servers only to their own full-time information technology staff.

You installed four hardware Hyper-V hosts in a secure server rack for Woodgrove Bank; each host contains five virtual machines. All server hardware includes a TPM v2.0 chip and UEFI firmware and runs Windows Server 2016 Datacenter Edition with the full GUI.

You've outlined the new Hyper-V security features offered by Windows Server 2016. In reply, Woodgrove IT personnel have the following questions for you:

1. If we accidentally mess up RDP or WinRM access to our workload VMs, we need another way to access them. How can we accomplish this goal?
2. Woodgrove plans to virtualize more of its infrastructure over the coming years, and we need a way to automate (or at least make easier) shielded VM deployment. What's possible?
3. What are the pros and cons of TPM-trusted vs. admin-trusted attestation?

Thought experiment answers

This section contains the solution to the thought experiment.

1. Shielded VM recovery is very much a "version 1.0" technology as of this writing. We really have only one solution: to implement the "repair garage" scheme as we discussed earlier in the chapter. By this method, fabric admins would be allowed temporary access to the VMs to unlock them. Then, presumably Woodgrove staff would connect to the workload VMs, reconfigure, and then allow the fabric admin to re-lock the shielded VMs.

   Configuring the VMs as encryption-supported would enable console access, but this option gives fabric administrators the ability to access the workload VM data permanently.
2. Microsoft discourages the approach of "grandfathering" existing, unshielded VMs into shielded state because this is a violation of the "clean source" principal. In other words, the best practice is to deploy new VMs in a guarded state to ensure integrity throughout the VM's lifetime.
3. That said, both System Center 2016 Virtual Machine Manager and Azure Stack both include in-box features that make it easier to store shielded VM templates. The big question for Woodgrove is who does the shielded VM deployment work; remember

that SCVMM and Azure Stack are fabric management tools, and would be more suited for Contoso Solutions' use rather than for Woodgrove workload administrators.

TPM-trusted attestation provides a much stronger set of protections for virtual machines running in a guarded fabric. Technically, we can use virtual TPM functionality in Hyper-V virtual machines even in the absence of a server physical TPM, but Woodgrove is fortunate enough to have host hardware that allows for TPM-trusted attestation.

Recall that in the TPM-trusted attestation scenario, we capture the startup and runtime environment of each guarded host. This means we need to perform the extra work of capturing a "golden image" of each host's state and deploying a Code Integrity (CI) policy that whitelists the code that can run.

If Woodgrove's security requirements are this strict, then AD-trusted attestation is a much easier implementation approach. However, the only thing we're attesting in this scenario is that a guarded host belongs to the appropriate AD security group. If the HGS cluster domain were to be compromised, then this defeats the entire attestation method and trust path.

CHAPTER 3

Secure a network infrastructure

Karl is the IT director of a local law firm. He doesn't believe in enabling Windows Firewall on any of his infrastructure servers. "It's just too much hassle," Karl explained. "We have a strong hardware firewall at our network perimeter. Inside the firewall we believe we have a trusted fabric, so we turn off the Windows Firewall on all server and desktop systems to facilitate remote management."

Don't be like Karl. Windows Firewall is a software, host-based firewall that is every bit as present in Windows Server 2016 as it is in every previous server operating system since Windows Server 2003.

By restricting the network traffic that is allowed to reach your servers, you reduce those servers' attack surface. Ideally, your servers should never even respond to port or service probes. In other words, your servers should be "ghosts" on your network and respond only to legitimate connection requests by authorized parties.

In this chapter, we explain how to configure Windows Firewall in Windows Server 2016. We also cover Microsoft's vision to bring Azure's software-defined networking (SDN) stack to your on-premises network. Finally, we dig into Server Message Block (SMB) and Internet Protocol Security (IPSec) and discover how to provide confidentiality, integrity, and authentication to selected network traffic flows.

Skills in this chapter:

- Configure Windows Firewall
- Implement a Software Defined Distributed Firewall
- Secure network traffic

Skill 3.1: Configure Windows Firewall

A firewall is hardware or software that protects a host by screening inbound (and, potentially, outbound) network traffic. Windows Firewall is the host-based software firewall that's been part of Windows Server since Windows Server 2003.

This section covers how to:

- Configure Windows Firewall with Advanced Security
- Configure network location profiles and deploy profile rules using Group Policy
- Configure connection security rules using Group Policy, the GUI management console, or Windows PowerShell
- Configure Windows Firewall to allow or deny applications, scopes, ports, and users using Group Policy, the GUI management console, or Windows PowerShell
- Configure authenticated firewall exceptions
- Import and export setting

Configure Windows Firewall with Advanced Security

Although this 70-744 exam topic gets directly to the "meat and potatoes" by indicating the Windows Firewall with Advanced Security MMC console, we think it's appropriate for us to review all the ways we can interact with Windows Firewall on Windows Server 2016 systems.

From an elevated Windows PowerShell console, try the following commands:

- **firewall.cpl** This opens the Windows Firewall Control Panel
- **wf.msc** This command opens the Windows Firewall with Advanced Security MMC console.
- **netsh advfirewall firewall** This command employs the legacy netsh command-line program to allow you to manage Windows Firewall programmatically
- **ShowControlPanelItem -Name 'Windows Firewall'** This PowerShell statement opens the Windows Firewall Control Panel

The Windows Firewall Control Panel

Open the "standard" Windows Firewall Control Panel either by using the Control Panel interface or by invoking one of the previously listed commands. Figure 3-1 showcases the interface.