

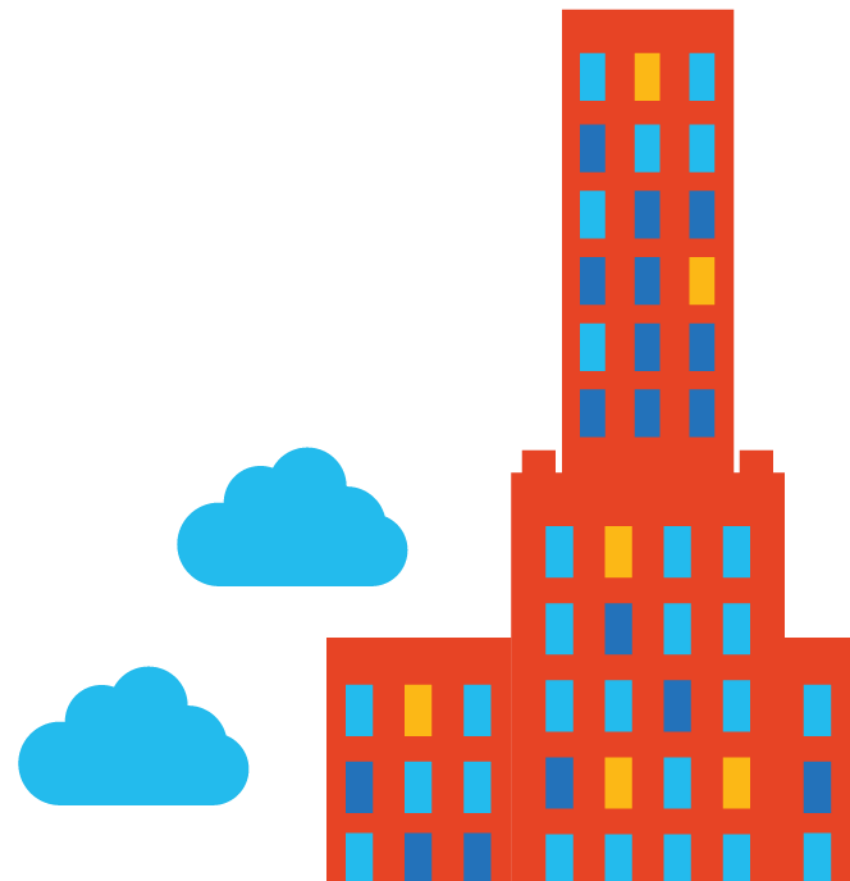
现代化企业数据中心

Windows Server 2016

Windows Server 2016 虚拟化技术

议程

- 安全与隔离
- 高可用
- 升级
- 高效运维原力



安全与隔离

不断进化的安全威胁

越来越多的组织遭受破坏和影响

1

更多的安全事件

2

更大的动机

3

更大的风险

Cyberattacks on the rise against US corporations

New York Times [2014]

1

Espionage malware infects rafts of governments, industries around the world

Ars Technica [2014]

1

Cybercrime costs US economy up to \$140 billion annually, report says

Los Angeles Times [2014]

2

How hackers allegedly stole "unlimited" amounts of cash from banks in just a few hours

Ars Technica [2014]

2

The biggest cyberthreat to companies could come from the inside

Cnet [2015]

3

Malware burrows deep into computer BIOS to escape AV

The Register [September 2014]

3

Forget carjacking, soon it will be carhacking

The Sydney Morning Herald [2014]

3

中央风险: 管理员特权

钓鱼攻击

窃取管理凭据

内部攻击

... 每个上述的攻击都试图寻找和利用特权用户账户

1. 我们大家都知道管理员掌握了王国的钥匙；我们已经给他们这样的特权数十年了
2. 但是上述管理员特权很容易因为社会工程，商业贿赂，胁迫或私人关系置换等受损

结论: 我们需要改变我们认知安全的方式

我们需要采用“假定违约” – 并不是悲观认定而是出于谨慎的原则

问题

违约即将或已经发生了

缺少安全分析人力

无法认定违背行为的影响

无法针对违背行为作出适当反应

新的方法

限制或阻止来自传播违背行为

检测到违背行为

对违背行为作出反应



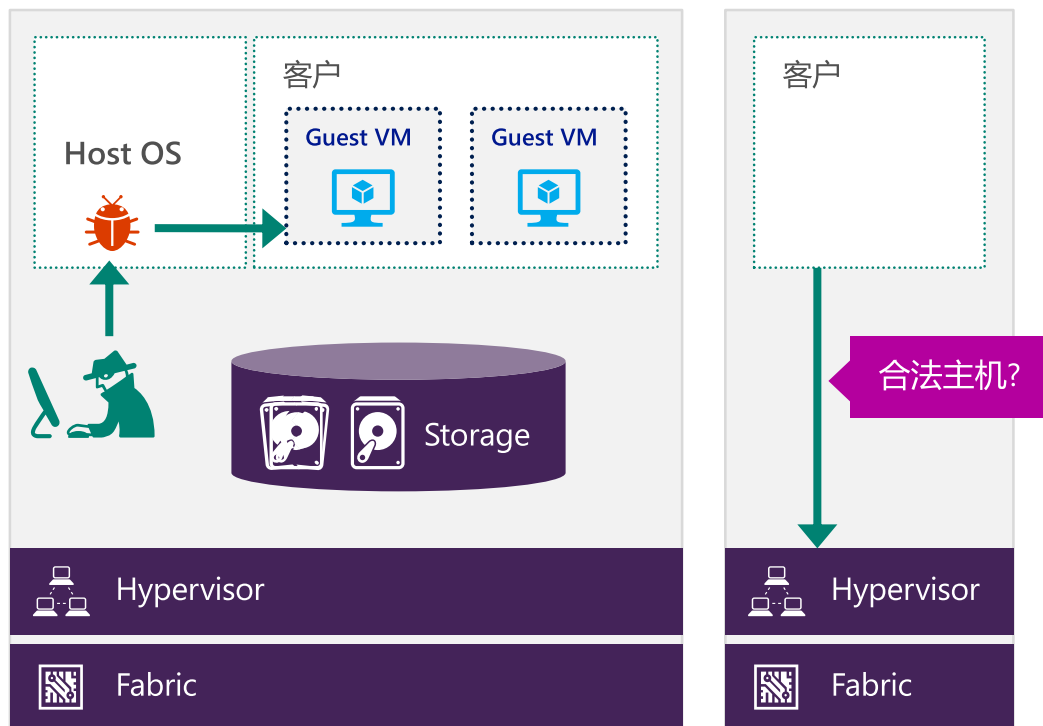
保护虚拟机

保护高价值的虚拟机的挑战

任何劫获或感染的主机管理员都可以获得客户虚拟机

没有硬件级别的验证几乎无法验证哪些主机是合法的

租户的虚拟机在没有加密的情况下非常冗余受到暴露到网络和存储端的攻击



保护虚拟机

微软的方法

通过基于主机的技术来分离主机
管理员与来宾操作系统

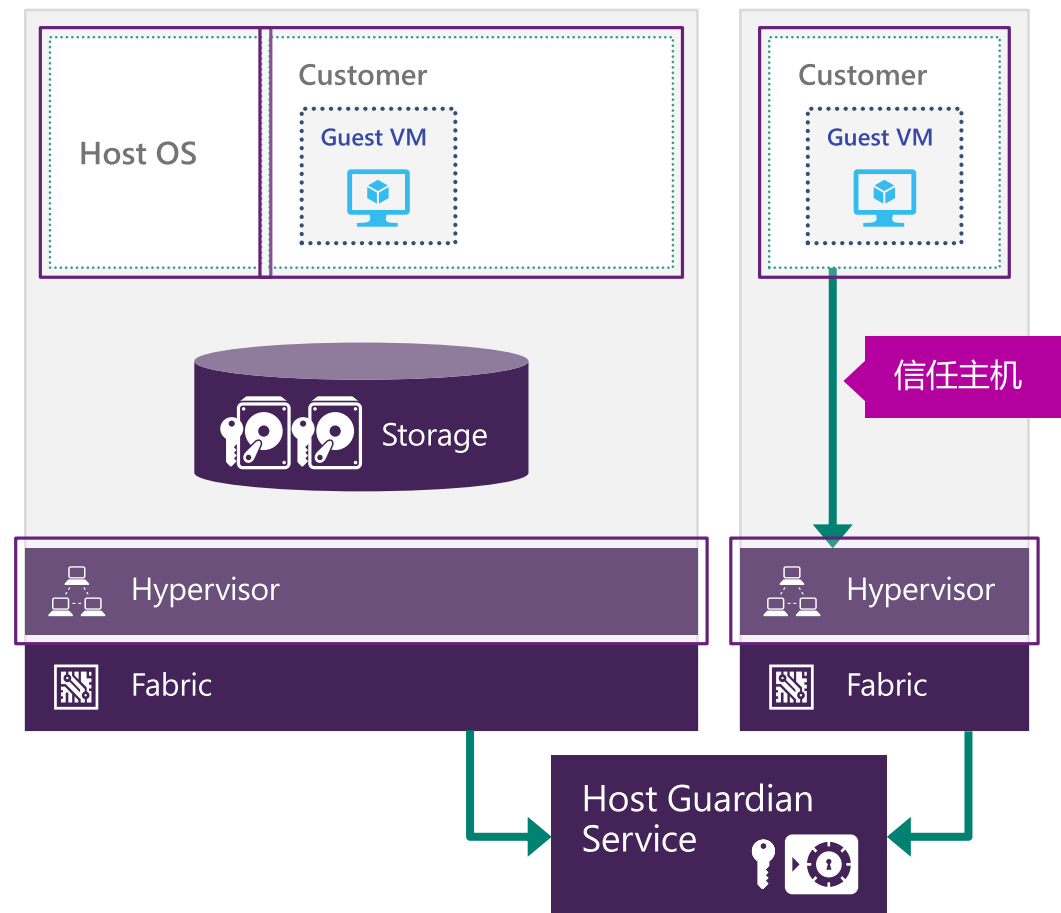
Virtual Secure Mode
从主机端保护进程与内存的访问

守护服务fabric用于识别合法主机
并证明其合法性来运行受保护的租
户虚拟机

Host Guardian Service
让受保护的虚拟机运行在经过
合法性验证的fabric主机中

Virtualized trusted platform 模块
(vTPM) 用于加密虚拟机

Shielded VM
Bitlocker加密保护虚拟机



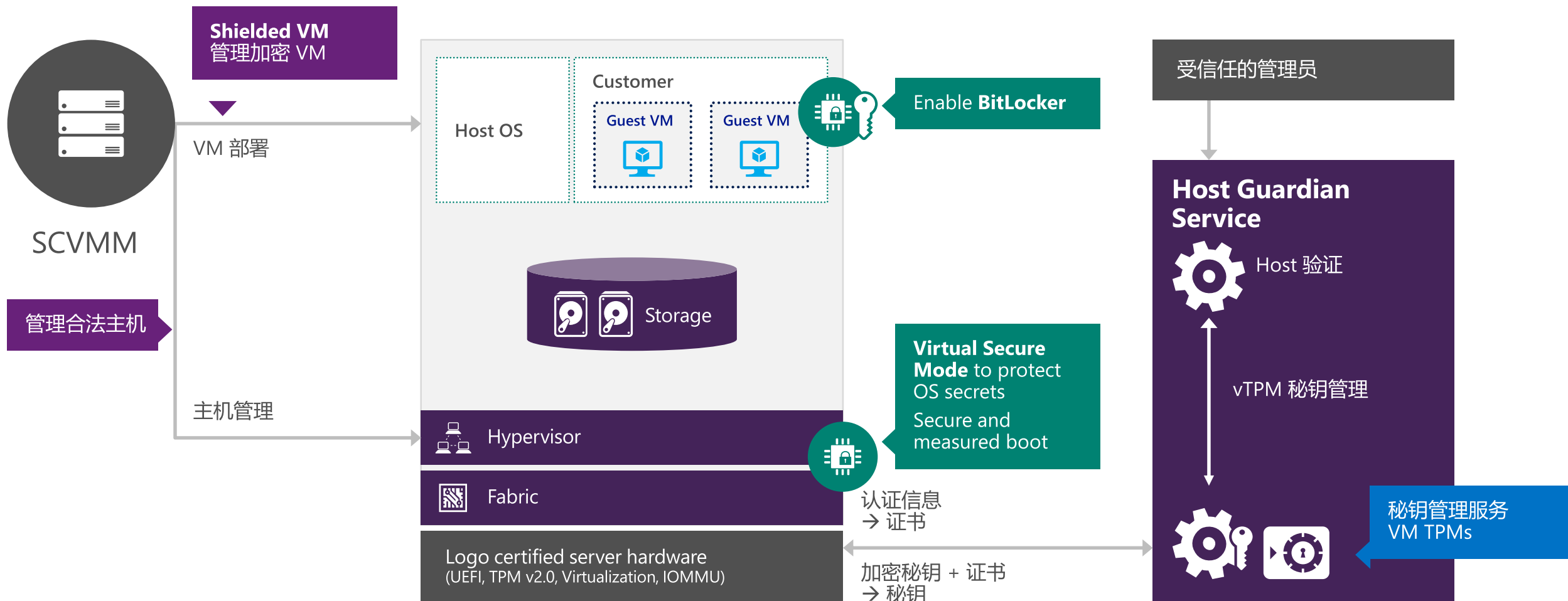
那么啥是‘屏蔽虚拟机’咩？

“受保护的虚拟机中的数据和状态不受数据中心管理员或者恶意软件的检查，窃取和篡改¹。”

¹ *fabric admins, storage admins, server admins, network admins*

保护虚拟机

与Windows Server 和 System Center工作方式



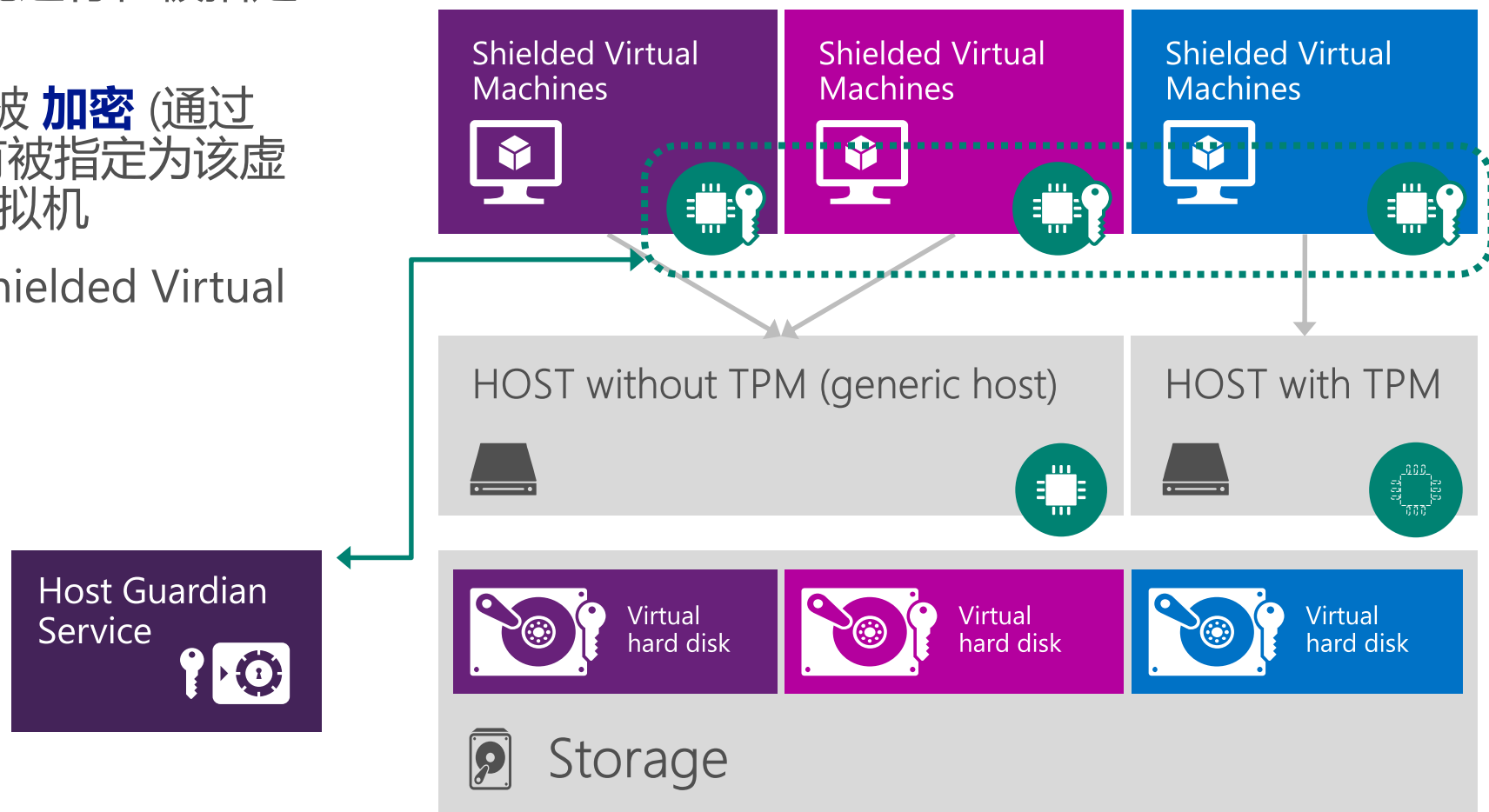
保护虚拟机

屏蔽虚拟机Shielded Virtual Machines

Shielded Virtual Machines 只能运行在被指定为该虚拟机的所有者的Fabric中

Shielded Virtual Machines 需要被 **加密** (通过 **BitLocker** 有其他) 用于保证只有被指定为该虚拟机的所有者才可以运行这个虚拟机

可以**转换正在运行的虚拟机** 为Shielded Virtual Machine



Shielded VMs: 安全保障目标

通过静态/动态数据加密保护

虚拟 vTPM 用于虚拟机的磁盘加密 (e.g. BitLocker)

在线迁移和虚拟机状态均进行加密

管理锁定

主机管理员无法访问虚拟机 Host administrators cannot access guest VM secrets (e.g. 无法看到磁盘和视频)

主机管理员无法运行任意的内核模式代码

健康认证

虚拟机负载只能运行于“健康状态”主机上

认证模式: 相互排斥

可信硬件认证

(基于TPM硬件)

复杂安装和设置

- 将每个Hyper-V主机的 TPM (EKpub) 注册到守护服务
- 每个硬件的SKU建立不同的CI代码完整性策略基线
- 部署HSM并使用 HSM-backed 证书

需要新的 Hyper-V 主机硬件

- 需要支持 TPM v2.0 和 UEFI 2.3.1

更高级别的保障

- 可信任根在硬件级别
- 通过代码完整性策略合规用于发布密密钥 (认证)
- Fabric管理员不受信任

... 主要面向云供应商

可信管理

(基于活动目录)

简化的部署和配置

- 安装活动目录信任加注册组
- 通过添加活动目录组对运行屏蔽虚拟机的Hyper-V主机进行授权

现有的硬件应该可以满足需求

应用场景

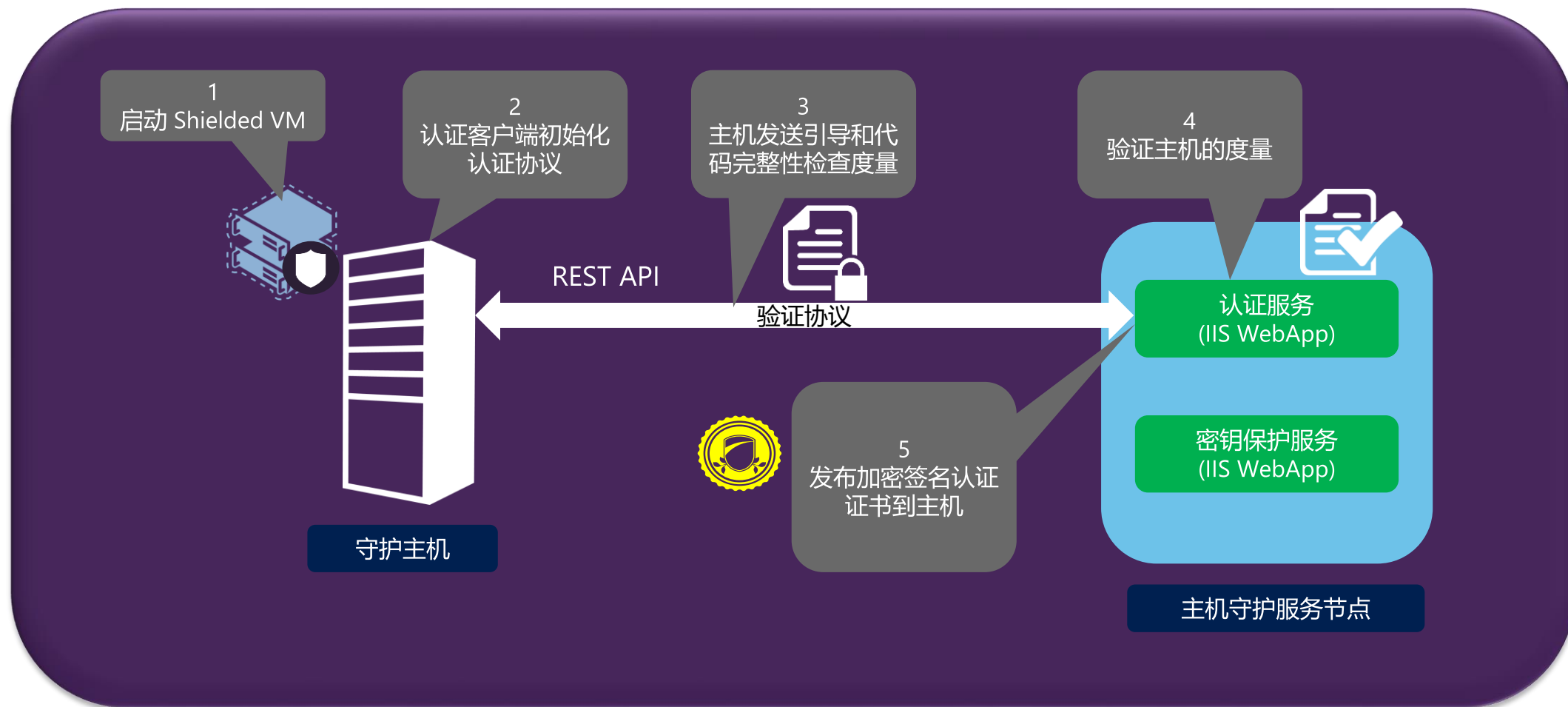
- 对于静态和活动数据进行保护
- 加密到云供应商容灾 (虚拟机已经应用了屏蔽)

弱级别的保障

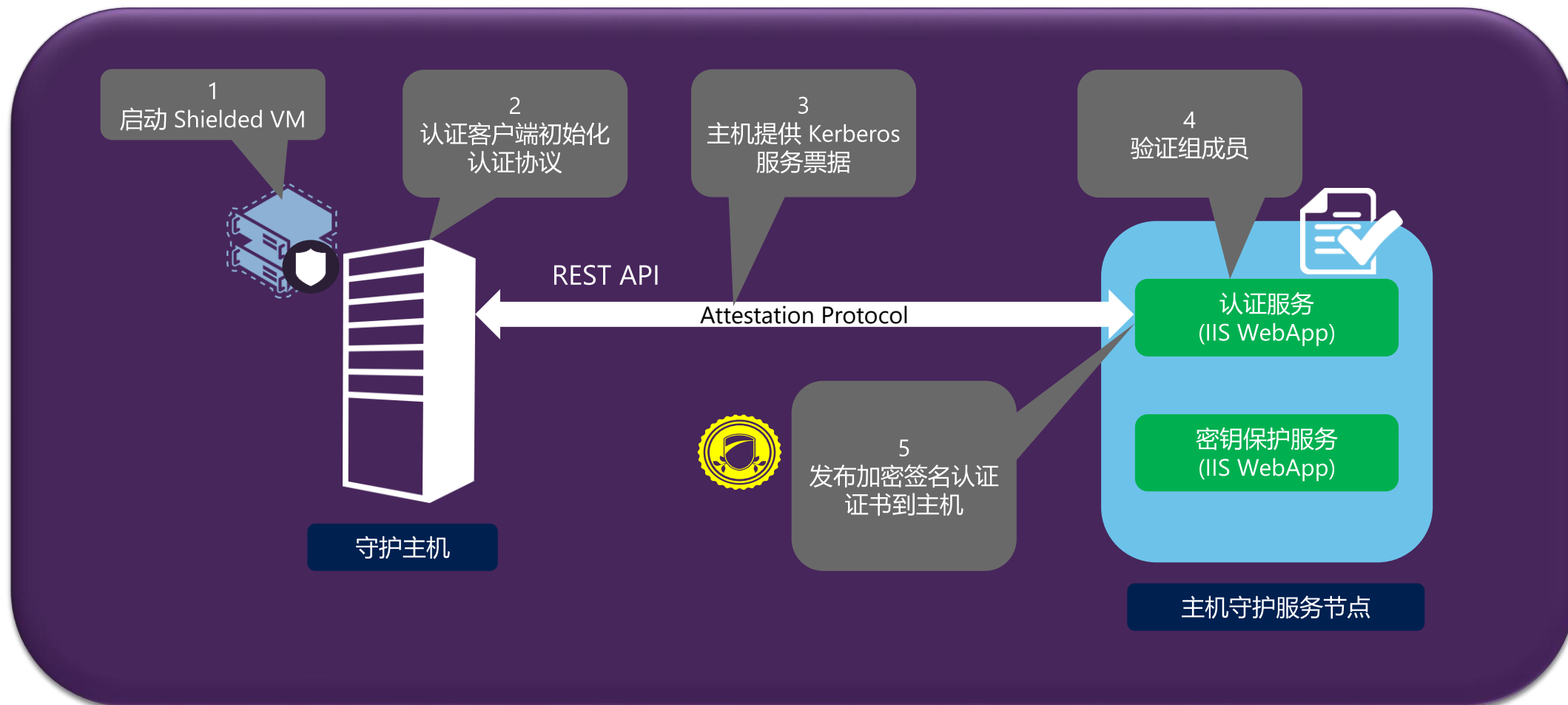
- Fabric管理员可信
- 没有硬件根信任和信任式开机引导
- 没有强制代码完整性检查

... 主要面向企业

认证 workflow (可信硬件)



认证 workflows (可信管理员)



保护虚拟机

虚拟安全模式Virtual Secure Mode

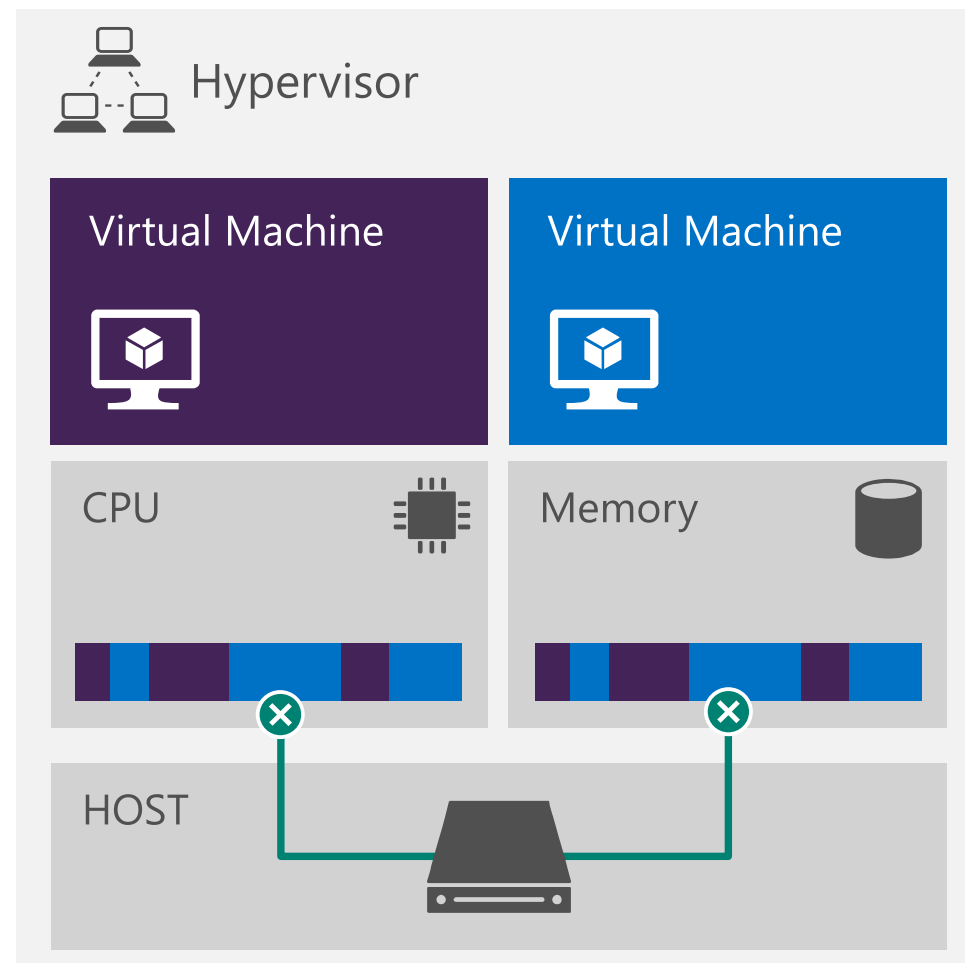
Virtual Secure Mode 防止虚拟机被受感染的主机访问物理内存数据，物理处理器。虚拟安全模式引入了**虚拟信任级别**的概念，包括内存访问保护，虚拟处理器状态和终端子系统。

虚拟信任级别Virtual Trust Levels (VTLs): 现有的特权安全级别上建立的安全机制 (ring 0/ring 3)

内存访问保护: 虚拟机安全级别上的内存访问保护只能在更高VTL中修改

虚拟处理器状态: 在不同的VTL中隔离处理器状态

中断子系统: 低级别的VTL产生的意外中断和遮蔽中断无法影响安全管理的特定VTL



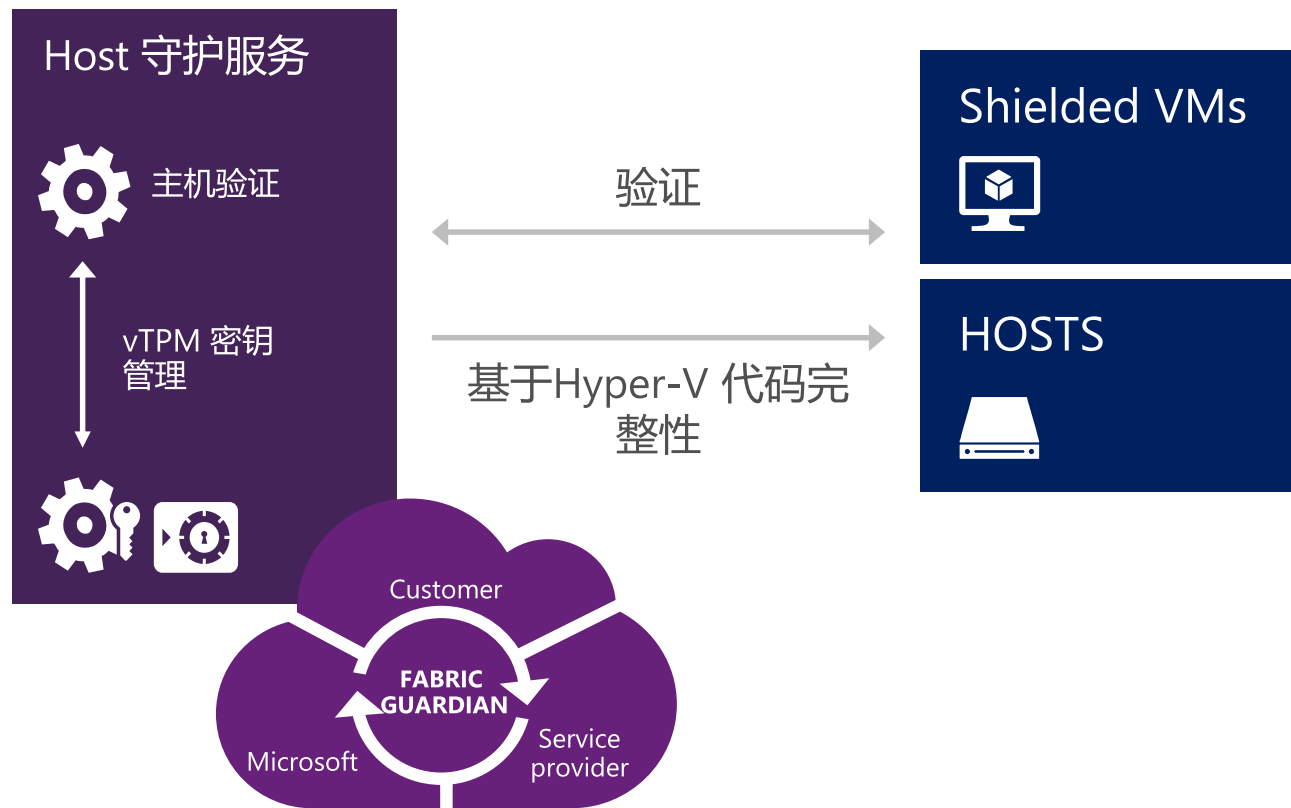
保护虚拟机

主机守护服务 Host Guardian Service

Host Guardian Service 保存合法可信的 fabric 中的密钥和加密虚拟机

Host Guardian Service 作为确定其是否为受信主机的验证服务

Host Guardian Service 可以在**任何地方在线**甚至是虚拟机

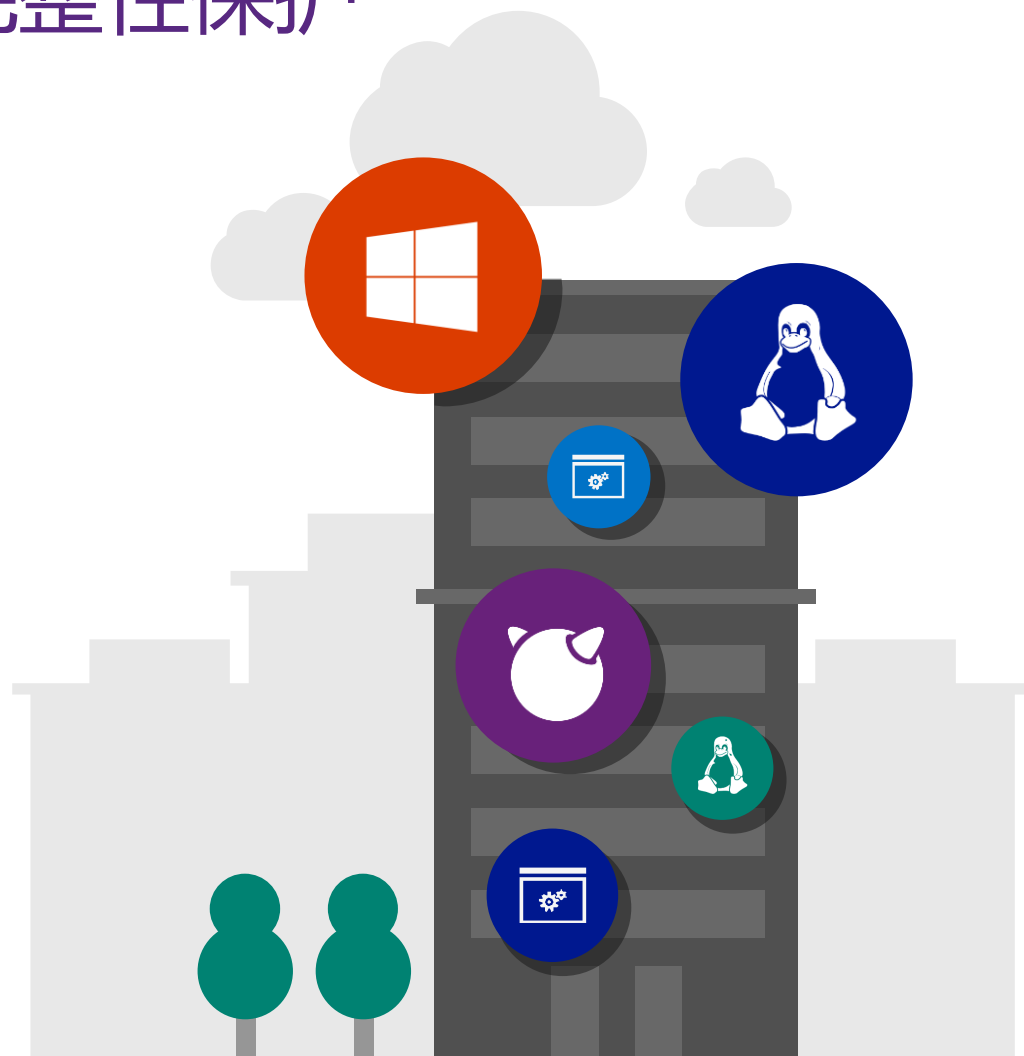


演示

虚拟机安全性

Linux 安全引导

- 提供Linux来宾操作系统内核代码的完整性保护
- 工作于:
 - Ubuntu 14.04 及后继版本
 - SUSE Linux Enterprise Server 12
- PowerShell 启用方法:
 - `Set-VMFirmware "linuxvmname"`
 `-SecureBootTemplate`
 `MicrosoftUEFICertificateAuthority`



主机资源保护

- 动态识别“行为异常”虚拟机并减少其资源分配
- 在Azure中率先默认启用
- 设计用于帮助减少某些虚拟机过渡的使用硬件资源的行为
- 发现不应该在无恶意的虚拟机上存在的行为模式



可用性

故障转移集群

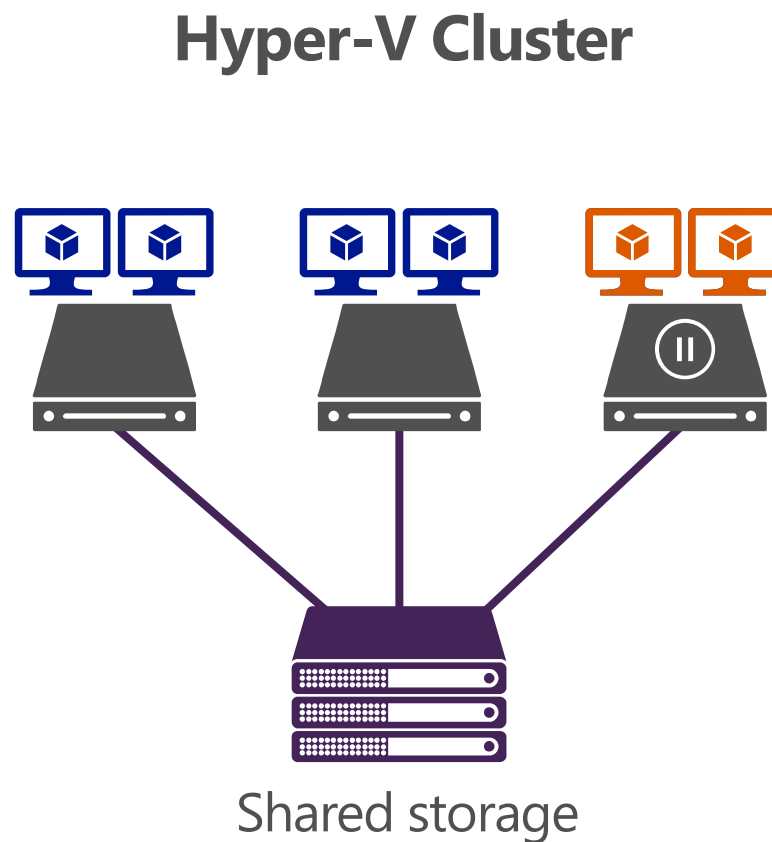
集成方案并在Windows Server技术预览版中增强

VM compute resiliency:

- 针对瞬间状态故障例如暂时性网络中断，或节点无响应提供健壮性
- 即便节点可能脱离了集群成员并处于隔离状态，虚拟机可以继续运行
- 可以根据需要进行配置，默认设置为4分钟。

VM storage resiliency:

- 在瞬间状态存储中断事件中保留租户虚拟机的会话状态。
- 虚拟机栈快速和智能的通知底层的块或文件存储架构故障。
- 虚拟机快速进入 PausedCritical 状态。
- 虚拟机等待存储恢复并保留会话状态用于恢复。



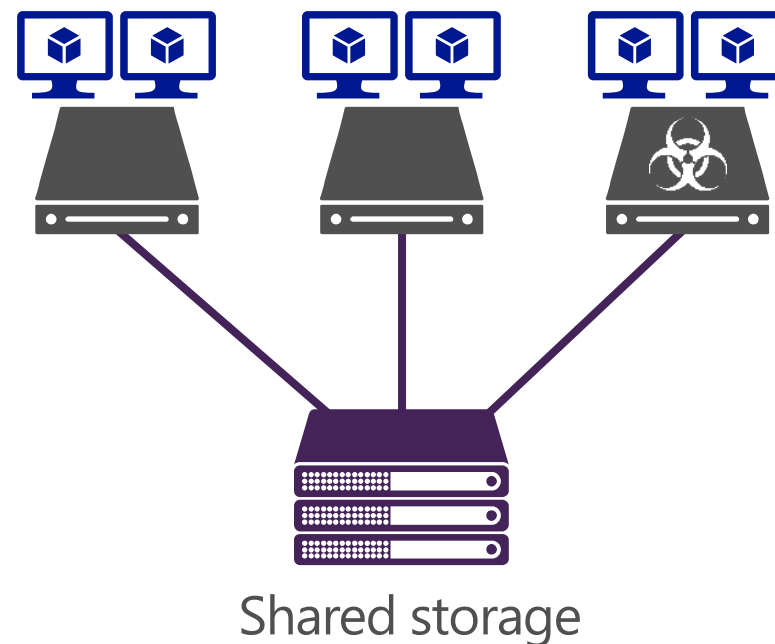
故障转移集群

集成方案并在Windows Server技术预览版中增强

节点隔离保护:

- 不健康节点将被隔离并且被禁止加入集群中。
- 这个功能可以阻止不健康的节点进入集群对整体集群造成负面影响。
- 在一个小时内如果某节点异常脱离集群3次则会触发隔离保护。
- 当节点被至于隔离保护区前，该节点运行的虚拟机将会通过在线迁移转移到其他集群节点中。

Hyper-V Cluster



通过共享 VHDX 建立来宾系统集群

解耦与底层存储拓扑绑定

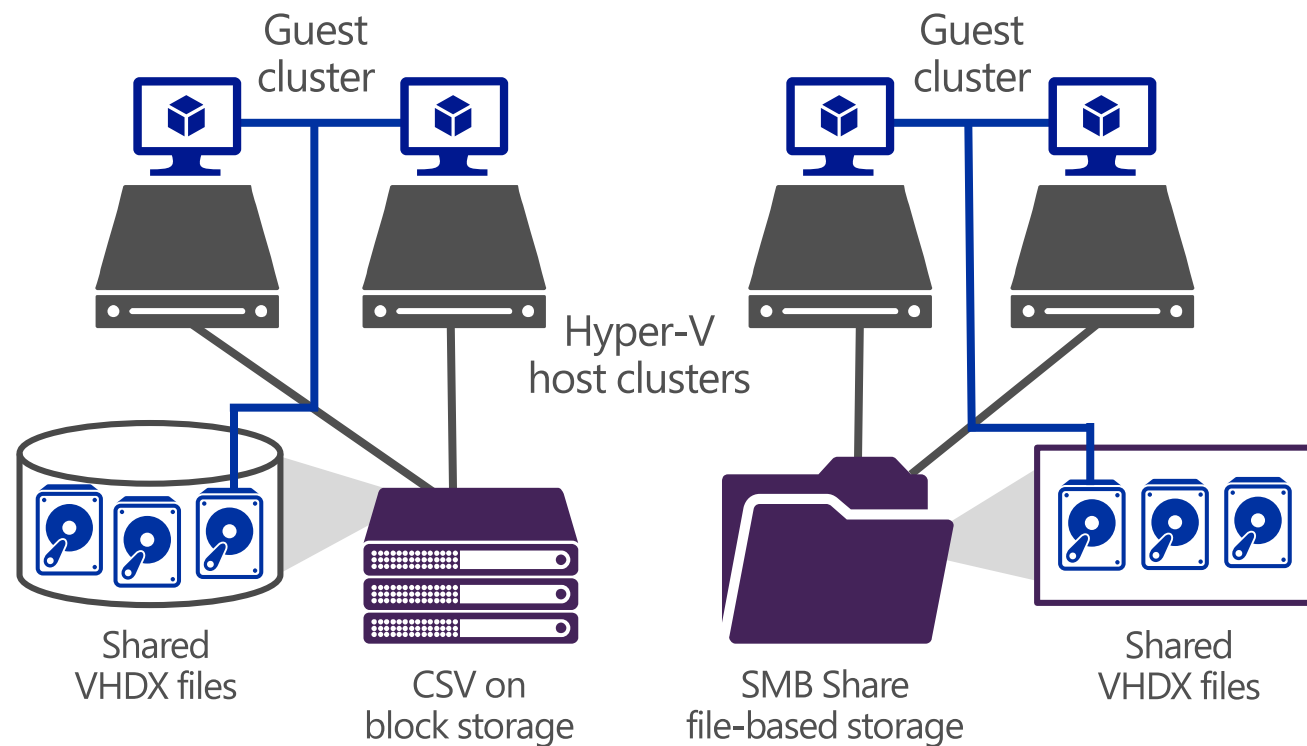
Flexible and secure: 共享VHDX消除了暴露底层物理存储到来宾操作系统的需要。

新功能 共享 VHDX 支持在线调整大小。

流水线虚拟机共享存储:

- 共享 VHDX 文件可以像共享存储一样同时分配给多个虚拟机。
- 虚拟机可以将共享的虚拟SAS磁盘用作创建来宾操作系统或应用级别的集群。
- 利用 SCSI-persistent 保留。
- 共享 VHDX 可以存在于集群共享卷 (CSV) 块存储, 或者在SMB文件共享存储上。

***新功能* 保护:** 共享 VHDX 可以支持 Hyper-V 复制和主机级别备份。

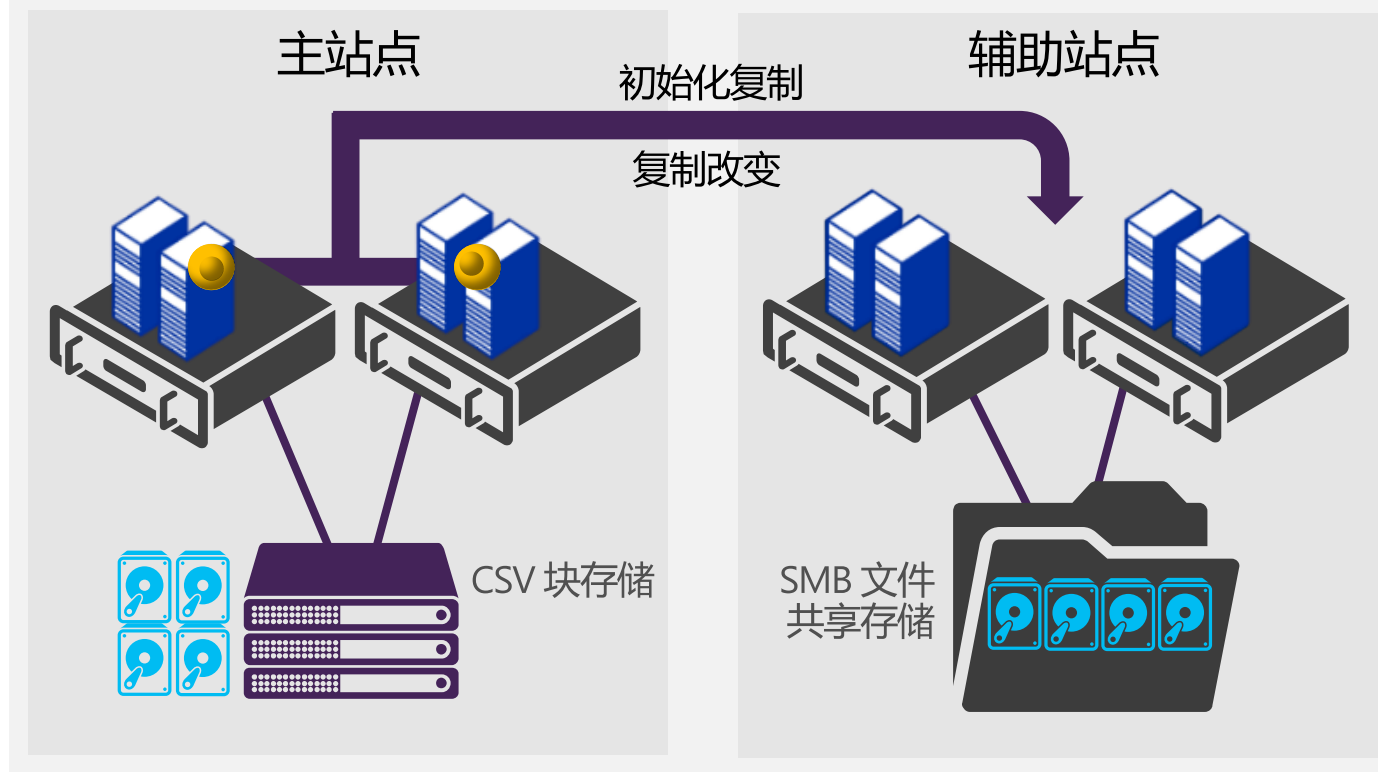


Hyper-V 副本

集成软件级别的虚拟机复制

- 虚拟机复制能力是Windows Server 2012 R2 Hyper-V内置的。
- 配置复制频率 30秒，5分钟或15分钟。
- 跨网络安全复制，可以通过该证书加密。
- 方案灵活，可以与站点间网络，主机或存储硬件无关。
- 不需要其他的虚拟机复制技术，因此成本可控。
- 自动控制在线迁移。
- 简化了配置和管理复杂度，可以通过Hyper-V管理器，PowerShell或者 Azure Site Recovery.

对于站点故障,虚拟机可以在辅助站点启动



副本支持VHDX热添加

- 当添加新的虚拟机磁盘到正在复制中的虚拟机中会自动添加到非复制集中，并且这个集合可以在线更新。
- `Set-VMReplication "VMName" -ReplicatedDisks (Get-VMHardDiskDrive "VMName")`

内存管理

完整的灵活性，以优化主机利用率

静态内存: 启动RAM 表示无论虚拟机内存需求所分配的内存。

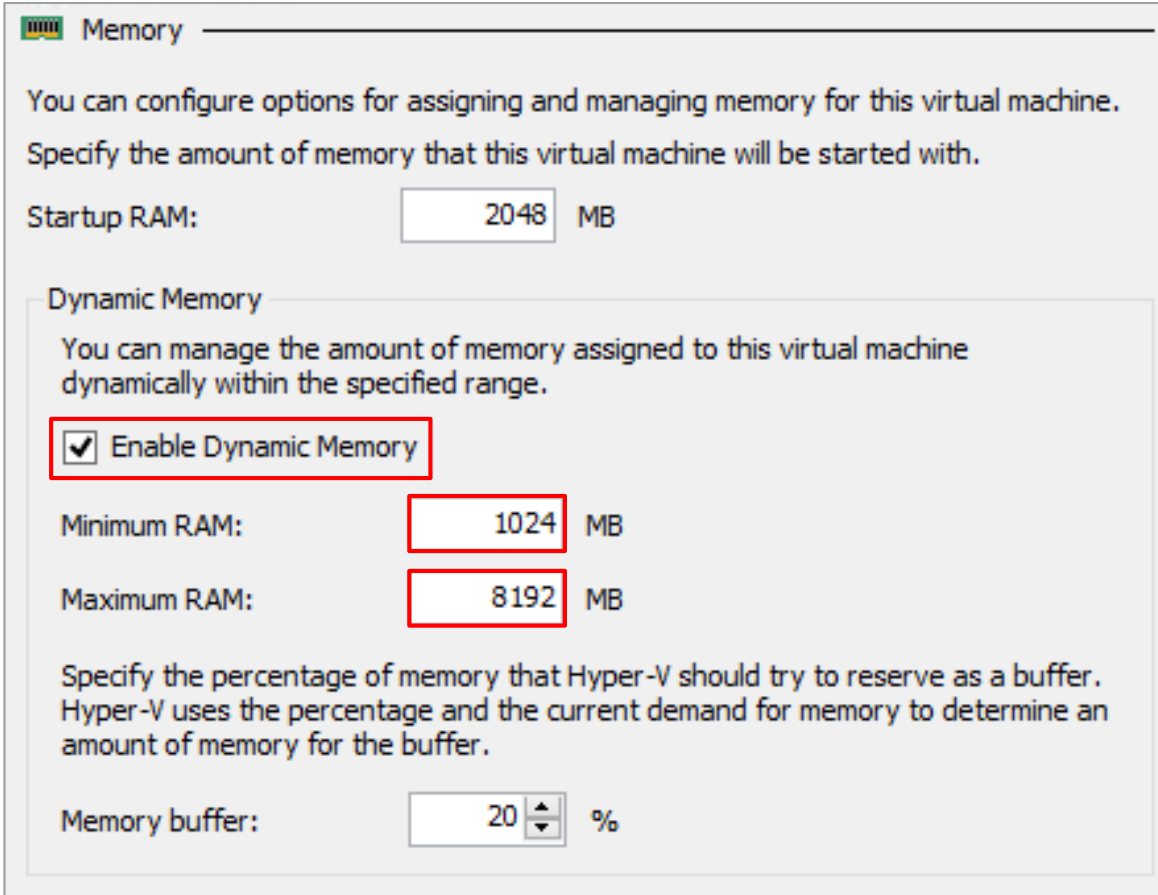
***新特性* 在线调整:** 管理员现在可以在不停机的情况下增加或减少虚拟机内存。

注意无法减小到小于当前内存需求或扩大到超过系统物理内存。

动态内存: 在虚拟机环境自动分配内存。

可以提高资源利用率，提高整合比并且可以保障重启操作的可靠性。

在线调整: 打开动态内存的时候，管理员可以在不停机的情况下增加最大内存和减少最小内存。



Memory

You can configure options for assigning and managing memory for this virtual machine. Specify the amount of memory that this virtual machine will be started with.

Startup RAM: 2048 MB

Dynamic Memory

You can manage the amount of memory assigned to this virtual machine dynamically within the specified range.

☒ Enable Dynamic Memory

Minimum RAM: 1024 MB

Maximum RAM: 8192 MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

演示

内存管理

虚拟化和网络

虚拟网卡增强

灵活性: 管理员现在有能力在不停机的情况下添加和移除虚拟机的虚拟网卡。

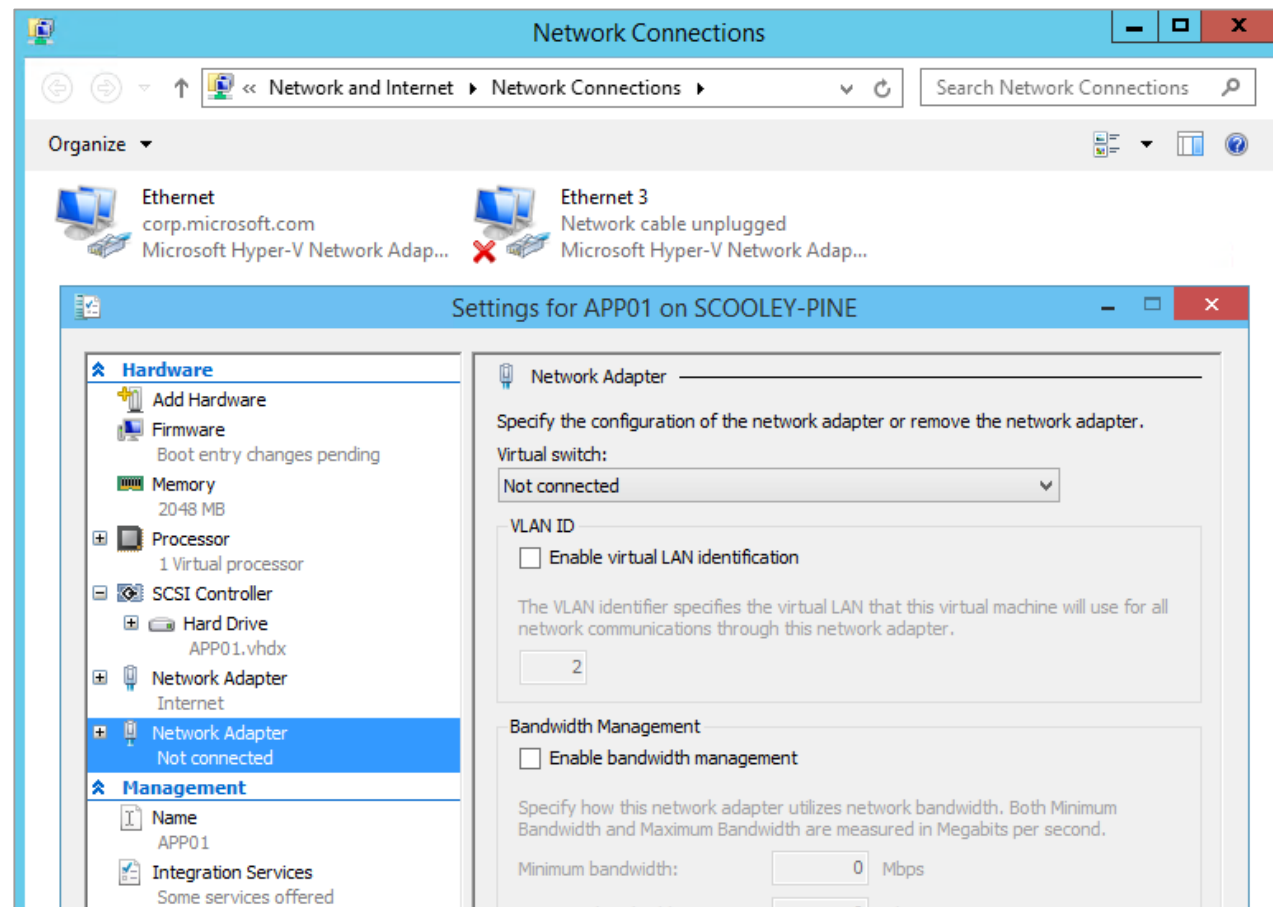
默认启用，仅限于2代虚拟机。

虚拟网卡可以通过Hyper-V 管理器界面或PowerShell操作。

全面支持: 任何受支持的Windows或Linux来宾操作系统均可以使用虚拟网卡热添加和热移除功能。

vNIC 识别: 新功能包括虚拟机设置中命名和查看虚拟网卡，用于标识与物理网络的对应。

```
Add-VMNetworkAdapter -VMName "TestVM" - SwitchName  
"Virtual Switch" -Name "TestNIC" -Passthru |  
Set-VMNetworkAdapter -DeviceNaming on
```



演示

vNICs

升级.

集群操作系统持续升级

对于关键负载升级集群节点无停机时间

流水线升级: 从Windows Server 2012 R2 集群节点升级到Windows Server 2016技术预览版不需要停机包括Hyper-V或者SOFS文件共享服务器工作负载。

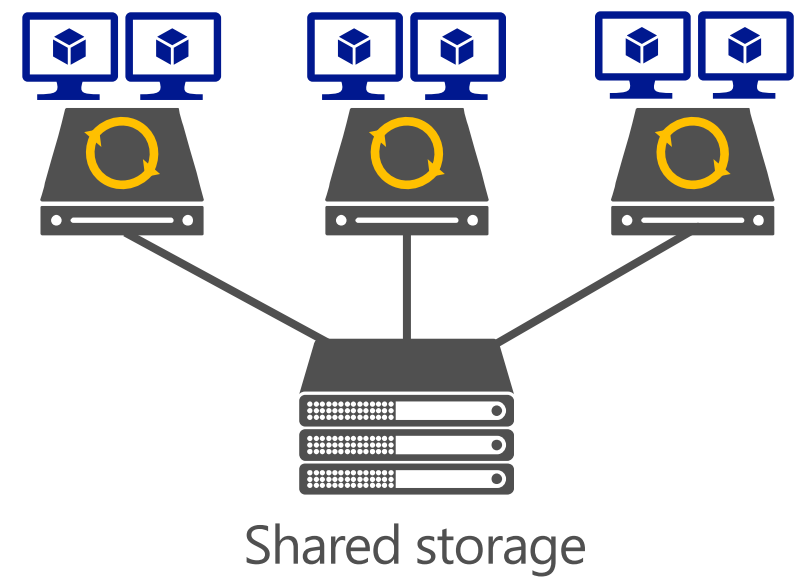
采用这种方式，基础结构可以持续保持更新而不需要影响工作负载。



分阶段升级方法:

1. 一个集群节点暂停并通过在线迁移方式排出工作负载。
2. 当节点迁出, 操作系统通过全新安装的方式替换成新的Windows Server技术预览版。
3. 新升级的节点会重新加入到集群节点中并成为活动节点。此时集群出于混合模式，然后在其他节点重复这个过程完成升级。

集群的功能级别functional level 保持在Windows Server 2012 R2 直到确定所有节点完成升级，并且负载工作正常（此过程为单向不可逆）。确定升级成功，系统管理员可以运行: `Update-ClusterFunctionalLevel`

Hyper-V Cluster



Windows Server 2012 R2 Cluster Nodes	Updated Windows Server Cluster Nodes
	

虚拟机升级

新的虚拟机升级和服务流程

兼容模式: 当虚拟机迁移到Windows Server 2016技术预览版主机，它将保持在Windows Server 2012 R2 兼容模式。

升级虚拟机的过程与主机升级分离。

虚拟机可以被移回早期版本直到它们被手工升级。

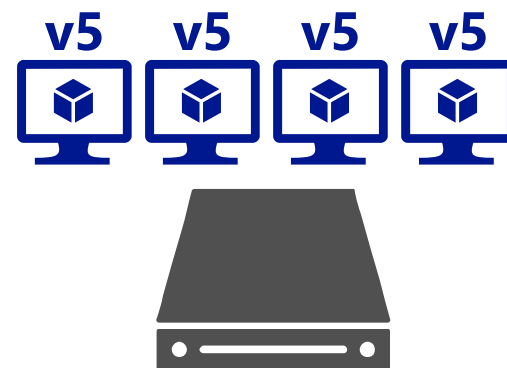
`Update-VMConfigurationVersion vmname`

升级完成后，虚拟机可以获得Hyper-V主机的新的功能。

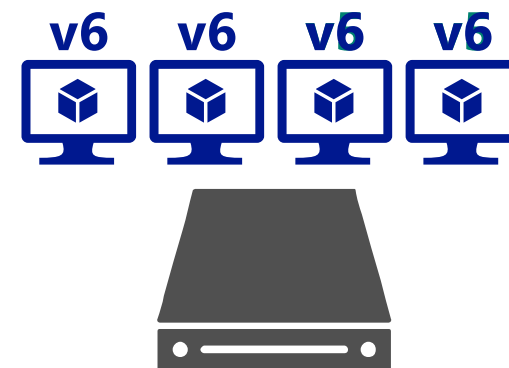
服务模式: 虚拟机驱动（集成服务）根据需要进行升级。

升级的虚拟机驱动会通过Windows升级直接推送到来宾操作系统中。

通过运行 `Update-VMConfigurationVersion`，虚拟机可以升级到新的硬件驱动版本并且使用新的Hyper-V 特性。



Windows Server
2012 R2
Hyper-V



Windows Server
技术预览版
Hyper-V

虚拟机服务

- Windows 8.1 / 2012 R2
 - 虚拟机驱动 (集成服务) 通过主机发行版本升级
 - 需要确保虚拟机驱动与主机版本匹配
 - 通过主机操作系统附带驱动
- Windows 10 / Windows Server 技术预览版
 - 虚拟机驱动 (集成服务) 可以根据需要进行升级
 - 需要可用的最新的来宾操作系统的虚拟机驱动
 - 通过Windows升级直接分发到来宾操作系统中

高效运维原力

生产环境检查点

完全支持生产环境

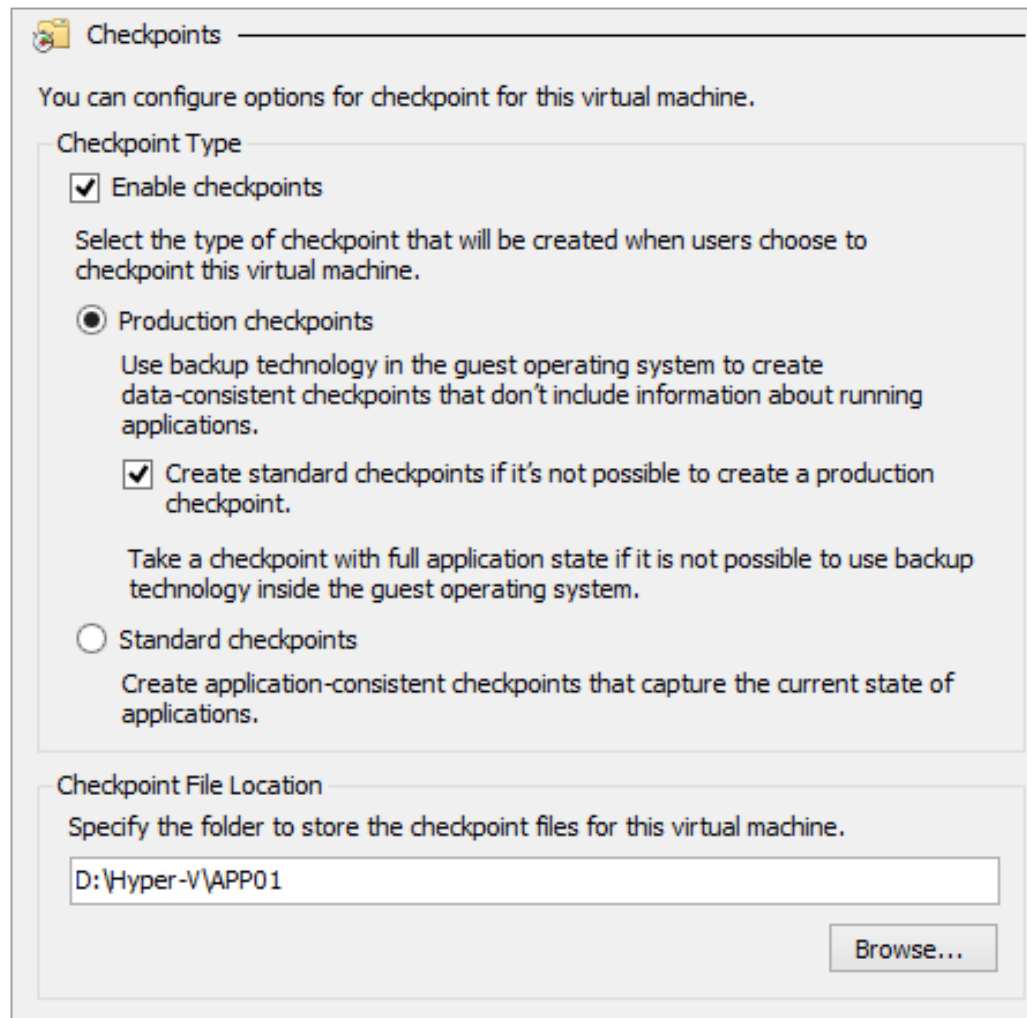
完全支持关键工作负载: 轻松创建时间点虚拟机映像，并且可以用于完全的生产级别的恢复。

VSS: 卷快照服务 (VSS) 用于在虚拟机内部创建生产级别的快照而不是之前使用的状态保存技术。

熟悉: 对于创建和恢复检查点的用户体验没有改变，恢复检查点过程类似于恢复一个全新备份的服务器。

Linux: 虚拟机通过刷新文件系统缓存创建文件系统一致性的检查点。

默认为生产级别检查点: 新创建的虚拟机会使用生产级别检查点及如无法使用生产级别检查点回退到标准检查点方式。



The screenshot shows the 'Checkpoints' configuration window in Hyper-V. It has a title bar with a folder icon and the text 'Checkpoints'. Below the title bar, it says 'You can configure options for checkpoint for this virtual machine.' The main content is divided into two sections: 'Checkpoint Type' and 'Checkpoint File Location'. In the 'Checkpoint Type' section, there is a checkbox 'Enable checkpoints' which is checked. Below it, a text box says 'Select the type of checkpoint that will be created when users choose to checkpoint this virtual machine.' There are two radio button options: 'Production checkpoints' (selected) and 'Standard checkpoints'. The 'Production checkpoints' option has a description: 'Use backup technology in the guest operating system to create data-consistent checkpoints that don't include information about running applications.' Below this, there is a checked checkbox 'Create standard checkpoints if it's not possible to create a production checkpoint.' and a text box: 'Take a checkpoint with full application state if it is not possible to use backup technology inside the guest operating system.' The 'Standard checkpoints' option has a description: 'Create application-consistent checkpoints that capture the current state of applications.' In the 'Checkpoint File Location' section, it says 'Specify the folder to store the checkpoint files for this virtual machine.' There is a text input field containing 'D:\Hyper-V\APP01' and a 'Browse...' button to its right.

Checkpoints

You can configure options for checkpoint for this virtual machine.

Checkpoint Type

☒ Enable checkpoints

Select the type of checkpoint that will be created when users choose to checkpoint this virtual machine.

☒ Production checkpoints

Use backup technology in the guest operating system to create data-consistent checkpoints that don't include information about running applications.

☒ Create standard checkpoints if it's not possible to create a production checkpoint.

Take a checkpoint with full application state if it is not possible to use backup technology inside the guest operating system.

☐ Standard checkpoints

Create application-consistent checkpoints that capture the current state of applications.

Checkpoint File Location

Specify the folder to store the checkpoint files for this virtual machine.

D:\Hyper-V\APP01

Browse...

PowerShell 直连

- 以安全的方式建立了Hyper-V主机和来宾操作系统的边界的连接，可以通过PS cmdlets 或脚本。
 - 目前支持 Win 10/WS2016 主机，来宾操作系统为 Win 10/WS2016 主机
- 不需要配置PS Remoting
- 不需要网络连接.
- 最需要提供来宾系统凭据
- 只能通过主机连接特定的来宾系统

```
Enter-PSSession -VMName VMName
```

```
Invoke-Command -VMName VMName -ScriptBlock { Fancy Script }
```

ReFS 加速 VHDX 操作

- Resilient File System
- 最大化了数据可靠性
- 利用智能文件系统的高级功能:
 - 瞬时固定虚拟磁盘创建
 - 瞬时磁盘检查点合并操作

演示

虚拟机直连及VHDX操作

