LEARNING

LIVES

HERE

Security Best Practices for Hyper-V

Rohit Gulati | Partner Technical Consultant
Microsoft

Agenda

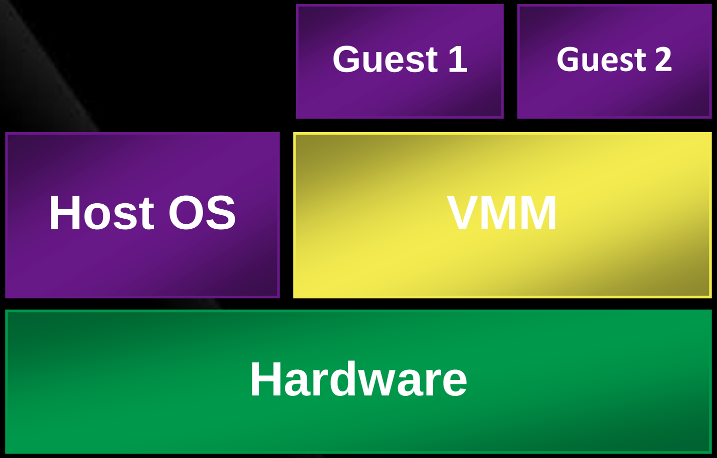
- Virtualization Overview
- Hyper-V Architecture
- Hyper-V Security Overview
- Hyper-V Security Guide
- Summary!

Virtualization Today

- Machine virtualization requires control of privileged operations
  - CPU registers and memory management hardware
  - Hardware devices
- Virtualization usually means emulation, but can also mean controlled access to privileged state
- The core virtualization software is called a Virtual Machine Monitor (VMM)
- There are two approaches to machine virtualization:
  - Hosted virtualization
  - Hypervisor virtualization

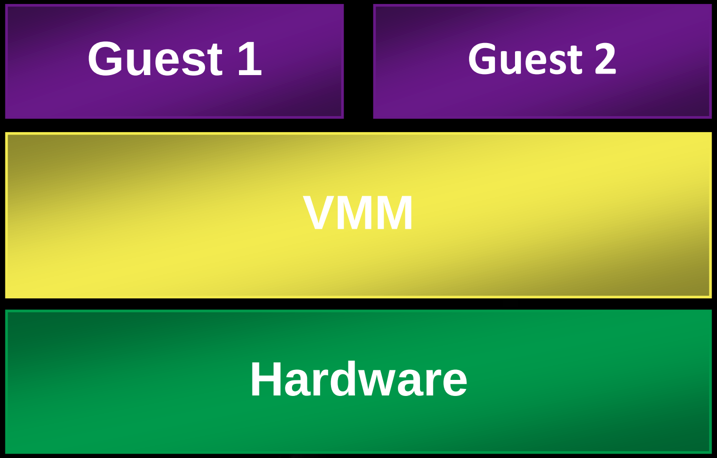
Virtual Machine Monitor Arrangements

- Hosted Virtualization



- Examples:
  - VMware Workstation
  - KVM
  - Virtual PC & Virtual Server

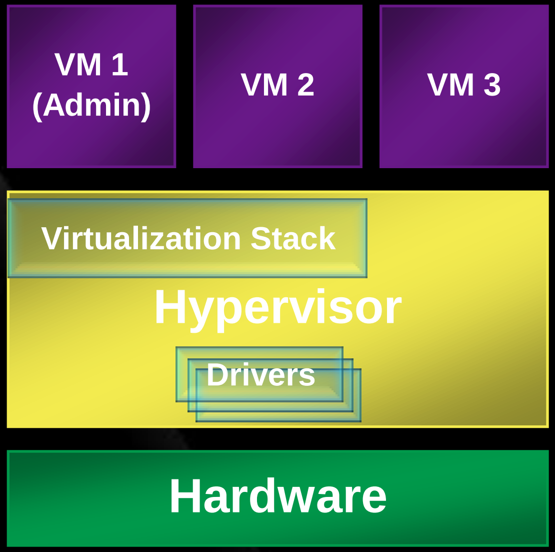
- Hypervisor Virtualization



- Examples:
  - VMware ESX
  - Xen
  - Hyper-V

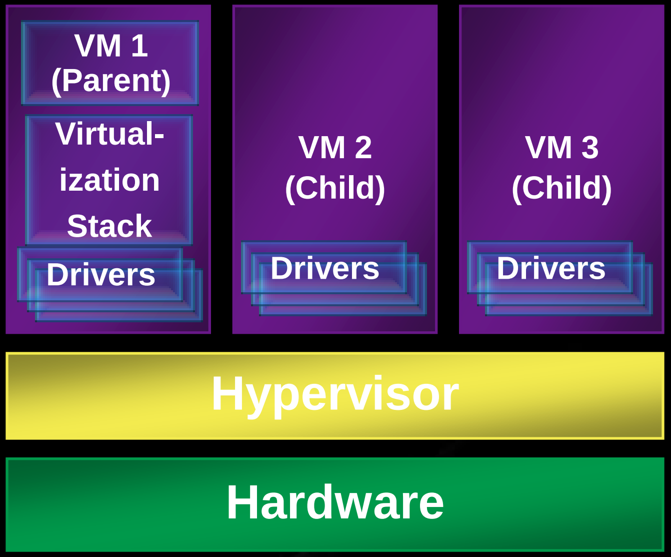
Monolithic Versus Microkernel Hypervisor

- Monolithic Hypervisor



- More simple than a modern kernel, but still complex
- Implements a driver model

- Microkernel Hypervisor



- Simple partitioning functionality
- Increase reliability and minimizes TCB
- No third-party code
- Drivers run within guests

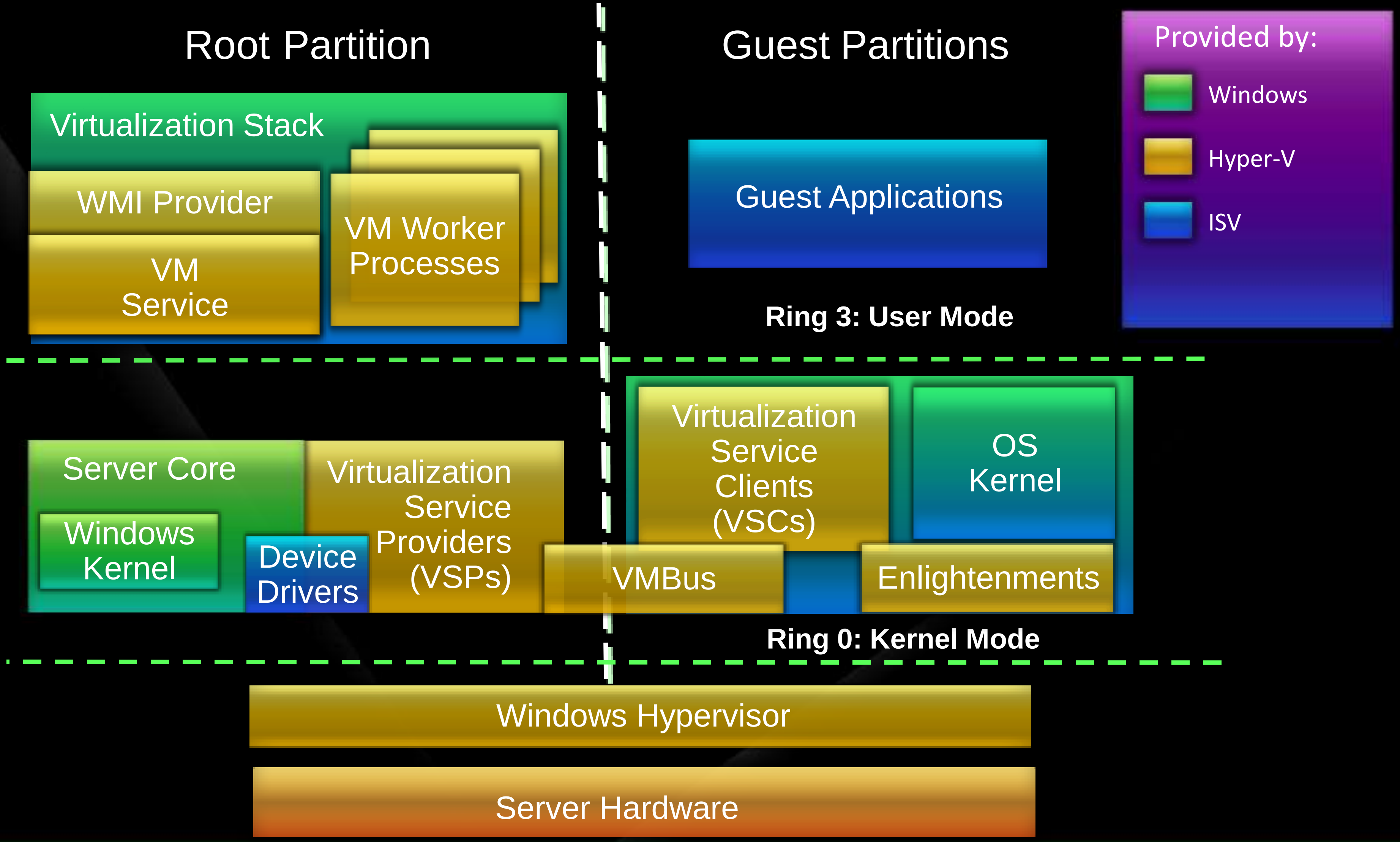
Agenda

- Virtualization Overview
- Hyper-V Architecture
- Hyper-V Security Overview
- Hyper-V Security Guide
- Summary!

Hyper-V Background

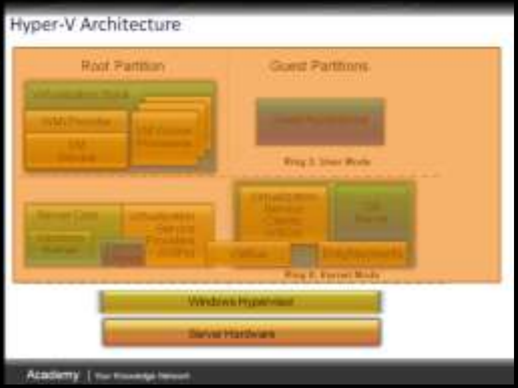
- Three major components
  - Hypervisor
  - Virtualization Stack
  - Virtual Devices
- Windows based virtualization platform
  - Windows Server 2008 x64 Edition technology (32/64 bit guest support)
  - Standard, Enterprise, and Datacenter Editions
  - Standards based
  - Packaged as a Server Role
- Requires hardware assisted virtualization
  - AMD AMD-V
  - Intel VT
- Data Execution Prevention (DEP) should be enabled

Hyper-V Architecture



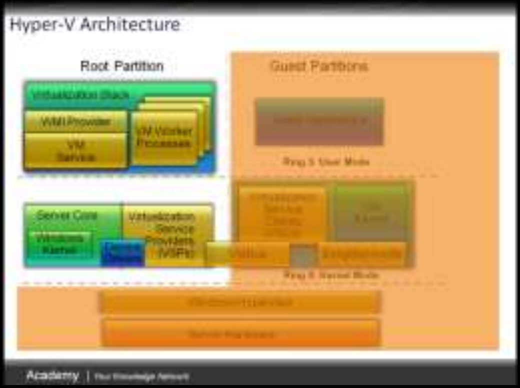
Hypervisor

- Partitioning Kernel
  - Partition is an isolation boundary
  - Few virtualization functions; relies on virtualization stack
- Very thin layer of software
  - Microkernel
  - Highly reliable
- No device drivers
  - Two versions, one for Intel and one for AMD
  - Drivers run in the root partition
  - Leverage the large base of Windows drivers
- Well-defined interface
  - Allow others to create support for their OSes as guests



Virtualization Stack

- Runs within the root partition
- Portion of traditional hypervisor that has been pushed up and out to make a micro-hypervisor
- Manages guest partitions
- Handles intercepts
- Emulates devices

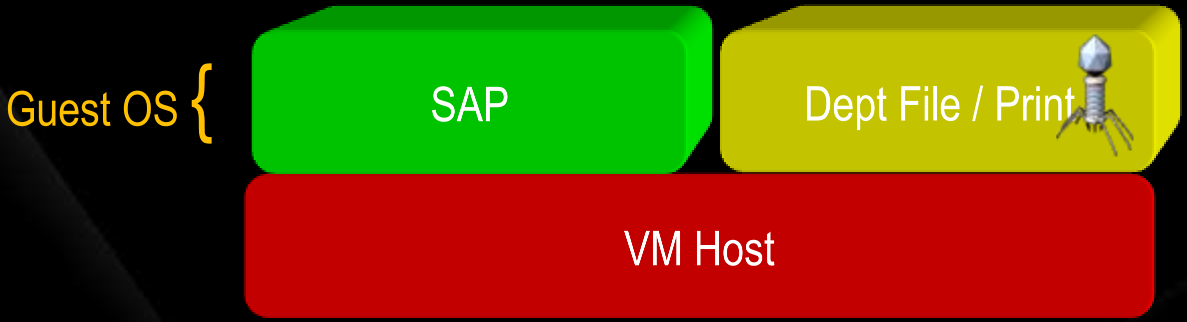


Agenda

- Virtualization Overview
- Hyper-V Architecture
- Hyper-V Security Overview
- Hyper-V Security Guide
- Summary!

VM “Aware” Threats

New technologies can introduce new types of attacks



Guest VMs can not see/detect threats in the VM host due to the virtualizing behavior of the host.

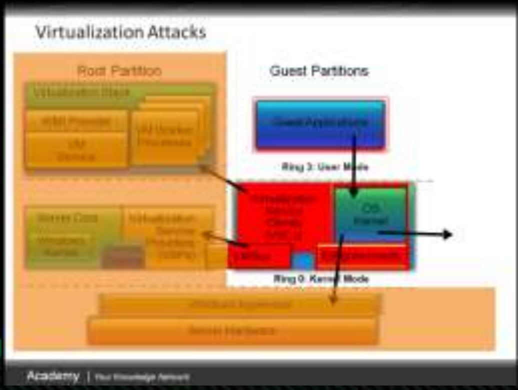
This attack approach is similar, yet much more insidious, than the approach rootkits take to hide their presence.

Top Virtualization Security Concerns

- The loss of separation of duties for administrative tasks, which can lead to a breakdown of defense in depth
- Patching, signature updates, and protection from tampering for offline virtual machine and virtual machine appliance images
- Patching and secure confirmation management of VM appliances where the underlying OS and configuration aren’t accessible
- Limited visibility into the host OS and virtual network to find vulnerabilities and access correct configuration
- Restricted view into inter-VM traffic for inspection by intrusion-prevention systems
- Mobile VMs will require security policy and settings to migrate with them
- Immature and incomplete security and management tools

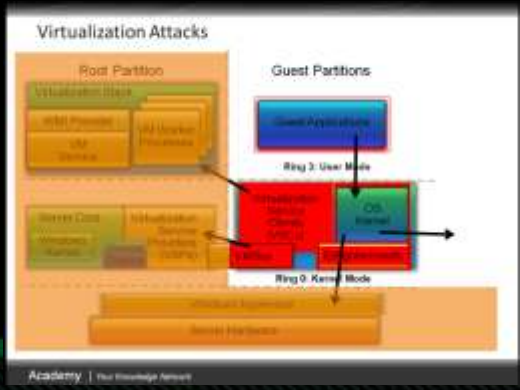
Security Assumptions

- Guests are un-trusted
- Root must be trusted by hypervisor; guests must trust the root
- Code in guests will run in all available processor modes, rings, and segments
- Hypercall interface will be well documented and widely available to attackers
- All hypercalls can be attempted by guests
- Can detect you are running on a hypervisor
  - We'll even give you the version
- The internal design of the hypervisor will be well understood



Security Goals

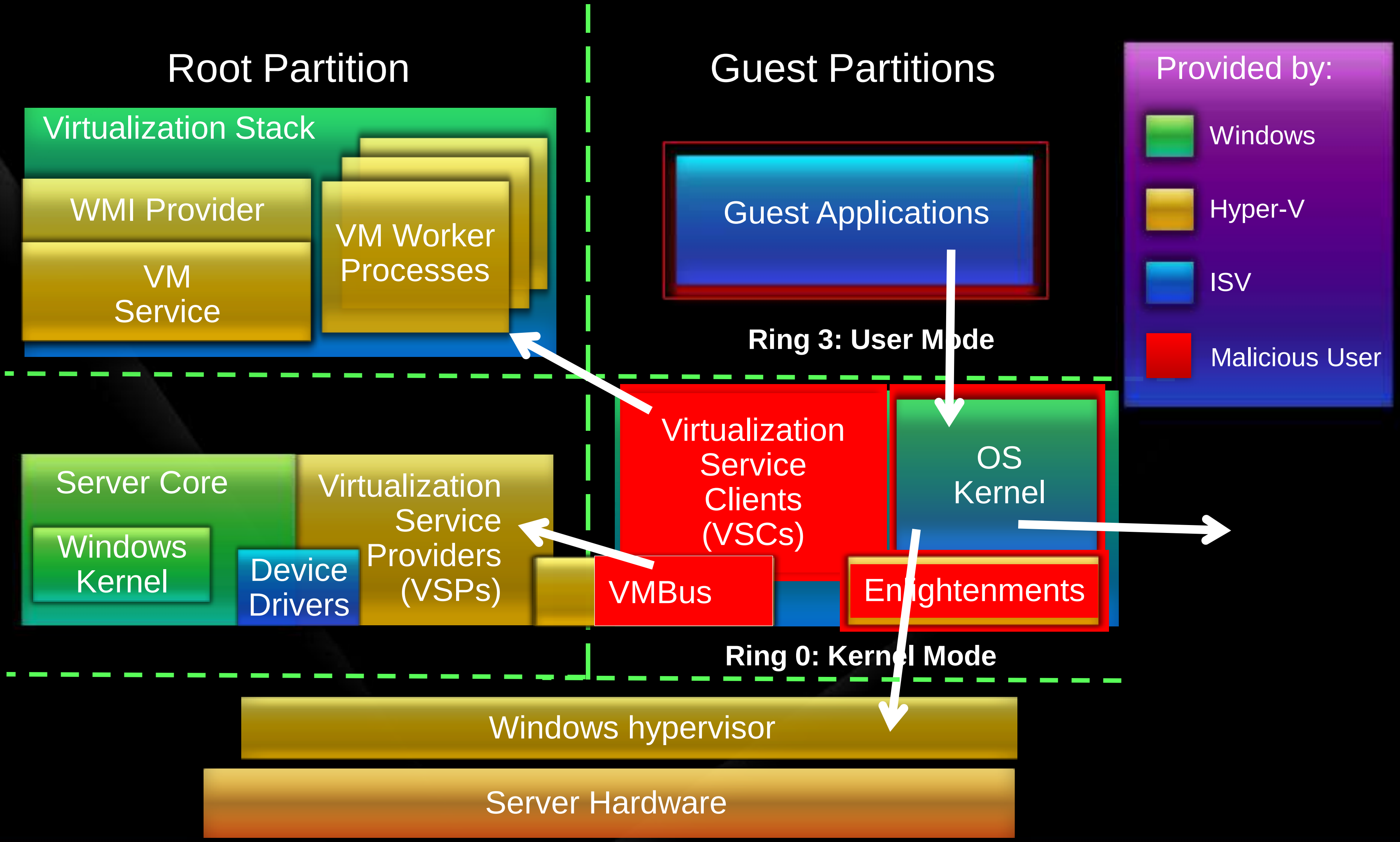
- Strong isolation between partitions
- Protect confidentiality and integrity of guest data
- Separation
  - Unique hypervisor resource pools per guest
  - Separate per-guest worker processes manage state
  - Guest-to-root communications over unique channels
- Non-interference
  - Guests cannot affect the contents of other guests, root, hypervisor
  - Guest computations protected from other guests
  - Guest-to-guest communications not allowed through VM interfaces



Hyper-V Security

- No sharing of virtualized devices
- Separate VMBus per guest to the parent
- No sharing of memory
  - Each has its own address space
- Guests cannot communicate with each other, except through traditional networking
- Guests can’t perform DMA attacks because they’re never mapped to physical devices
- No partition can write into hypervisor memory

Virtualization Attacks



Agenda

- Virtualization Overview
- Hyper-V Architecture
- Hyper-V Security Overview
- Hyper-V Security Guide
- Summary!

Hyper-V Security Guide

- Chapter 1: Hardening Hyper-V
  - Attack Surface
  - Server Role Security Considerations
  - Virtual Machine Configuration Checklist
- Chapter 2: Delegating Virtual Machine Management
  - Using Tools to Delegate Access
  - Delegating Access with Authorization Manager (AzMan)
  - System Center Virtual Machine Manager (SCVMM)
- Protecting Virtual Machines
  - Methods for Protecting Virtual Machines
  - Maintaining Virtual Machines
  - Best Practices

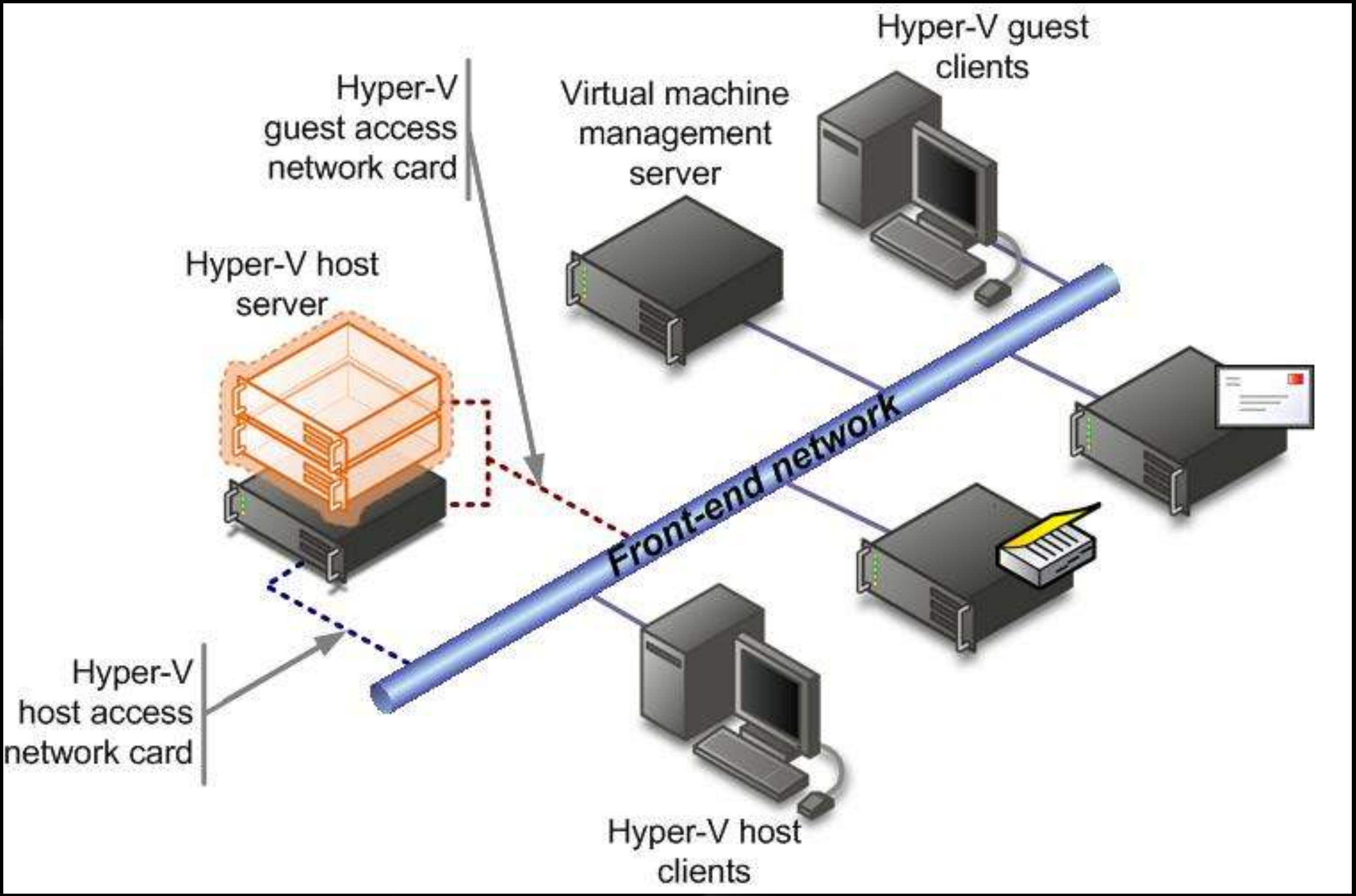
Attack Surface

- Adding the Hyper-V role service changes the attack surface
- The increased attack surface includes:
  - Installed files
  - Installed services
  - Firewall rules
- The attack surface for Hyper-V is documented

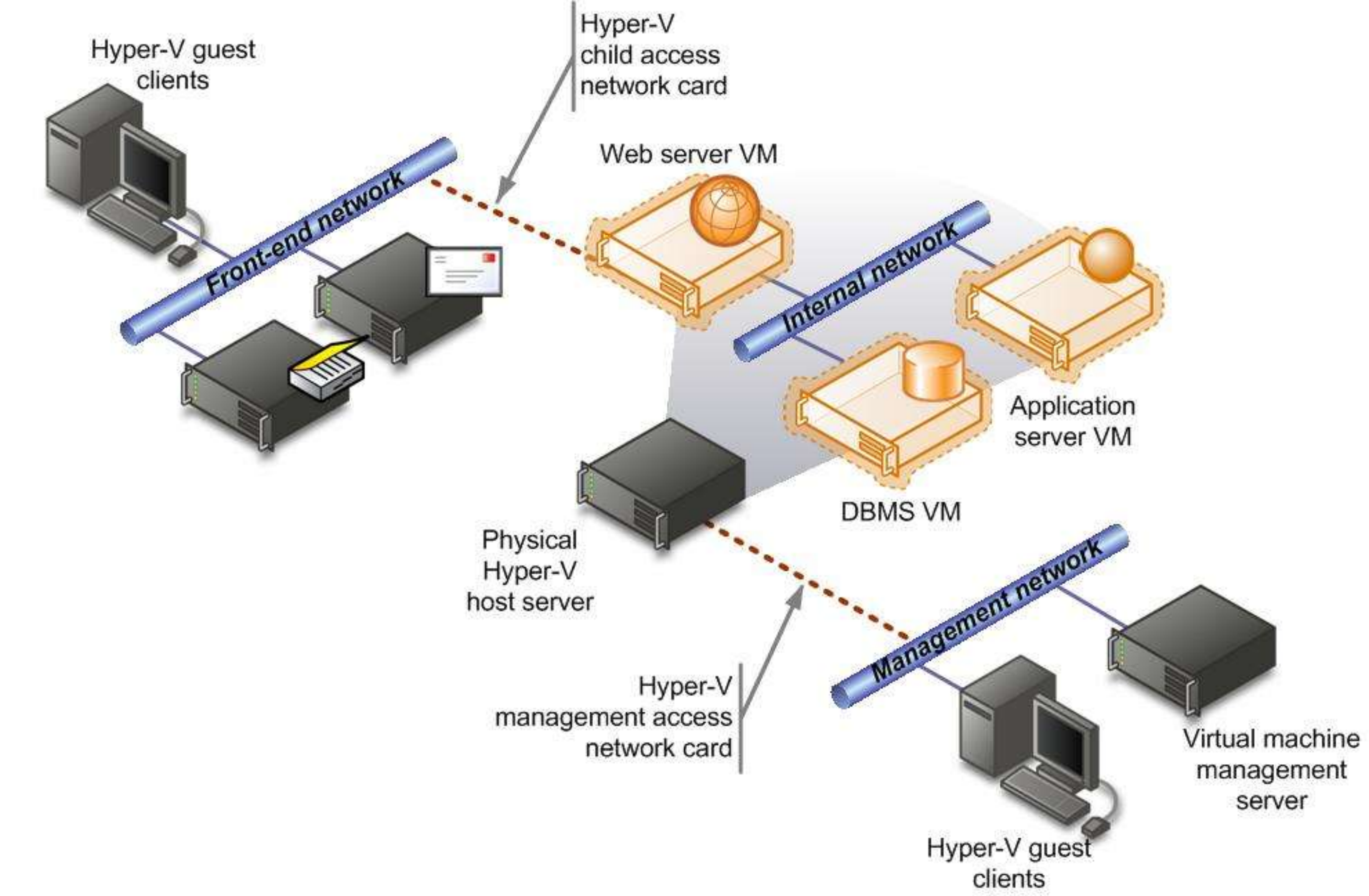
Server Role Security Configuration

- Two main considerations:
  - Parent partition (root) security
  - Child partition (guest, VM) security
- Parent partition
  - Default installation recommendations
  - Host network configuration
  - Secure dedicated storage devices
  - Host management configuration (admin privileges)
- Virtual Machines
  - Configuration recommendations
  - Hardening the OS
  - Checklist

Architecture of an Enterprise Network


Hyper-V guest clients
Hyper-V guest access network card
Virtual machine management server
Hyper-V host server
Front-end network
Hyper-V host access network card
Hyper-V host clients

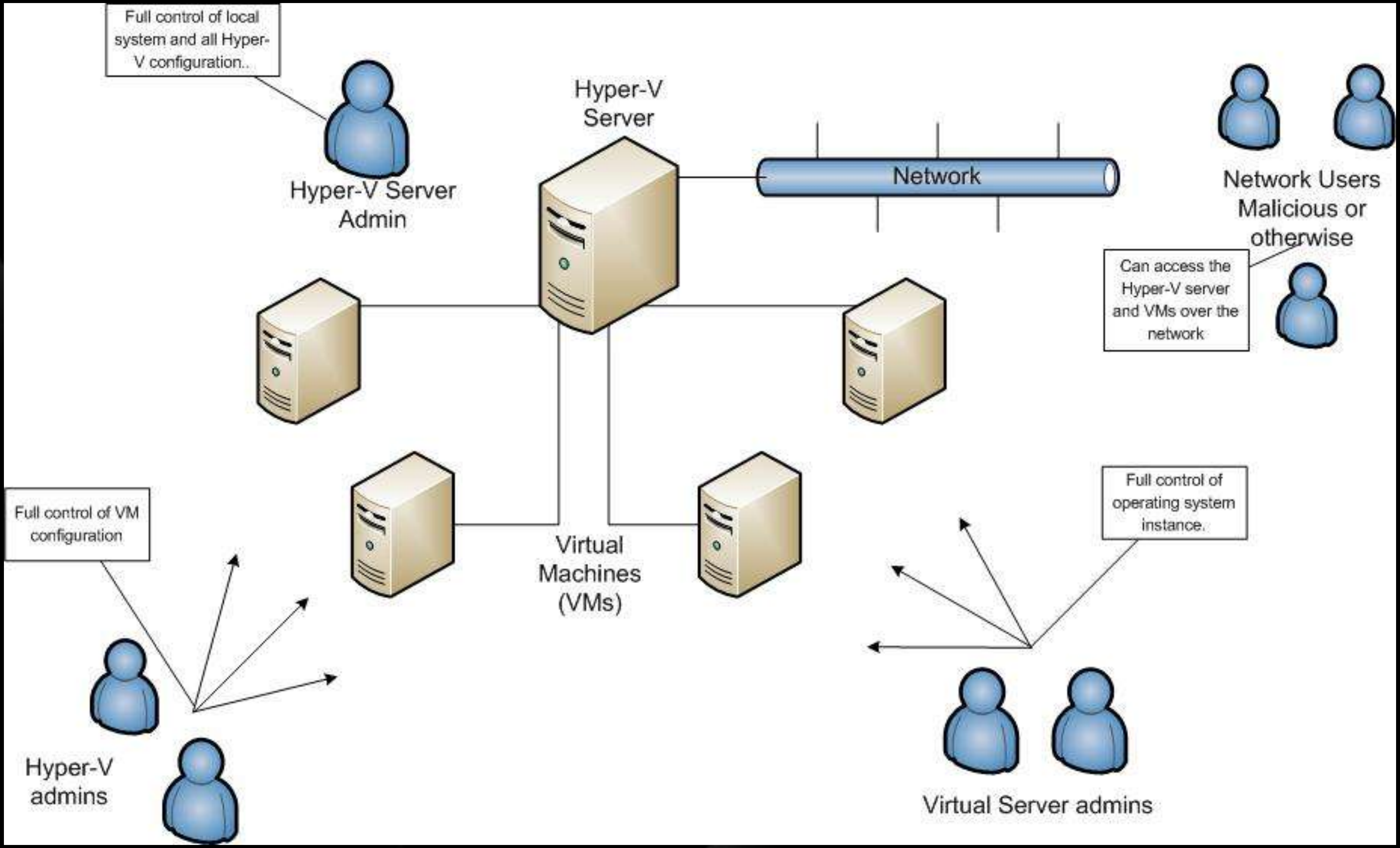
Network Configuration for Multi-tier Web Application



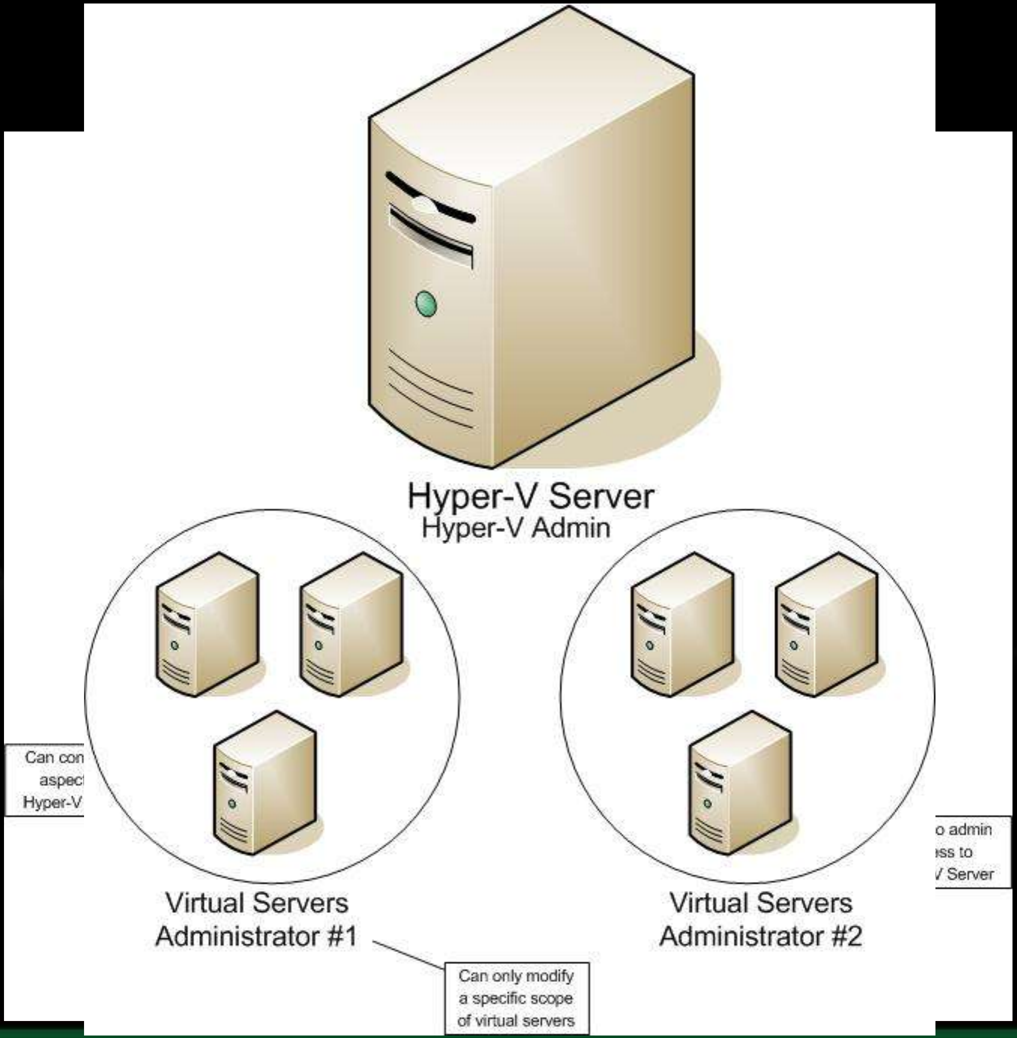
Delegating VM Management

- Hyper-V management console
  - Requires admin account
  - Manage VMs
- Authorization Manager (AzMan)
  - Microsoft Management Console snap-in
  - Users assigned to roles
  - Roles granted permissions to perform operations
  - Hyper-V defines 33 different operations
- System Center Virtual Machine Manager
  - Comprehensive management solution for data centers
  - Manage VMware ESX Server
  - 3 defined profiles

Hyper-V Ecosystem


Full control of local system and all Hyper-V configuration..
Hyper-V Server Admin
Hyper-V Server
Network
Network Users Malicious or otherwise
Can access the Hyper-V server and VMs over the network
Full control of VM configuration
Virtual Machines (VMs)
Full control of operating system instance.
Hyper-V admins
Virtual Server admins

Delegating VM Management



Can con
aspect
Hyper-V

o admin
ıss to
/ Server

Can only modify
a specific scope
of virtual servers

What is Authorization Manager?

- A Role-Based Access Control (RBAC) framework composed of:
  - AzMan administration tool (AzMan.msc)
  - Runtime that allows access checks against policy
- RBAC specifies access in terms of user roles, which are administrator-defined
- Authorization policy is managed separately from application code

AzMan Terminology

Scope

- A collection of similar resources with the same authorization policy
- Virtual machines; virtual networks

Role

- A job category or responsibility
- “Administrators” or “Self-Service Users” (in SCVMM)

Task

- A collection of operations or other actions
- None are defined by default

Operation

- A specific action that a user can perform
- “Start virtual machine”; “Stop virtual machine”

Hyper-V and AzMan

- One default role defined: ***Administrators***
- Defines specific functions for users or roles
  - Start, Stop, Allow Input, Allow Output, etc.
  - 32 operations are defined in the Auth store
- Hyper-V admins do *not* need Administrator access to parent partition OS
- Default authorization data stored in XML:
  - `%ProgramData%\Microsoft\Windows\Hyper-V\InitialStore.xml`
- Authorization data can be stored in Active Directory

Hyper-V Operations at-a-Glance

VM Management Operations	
Read Service	Reconfigure Service

Virtual Machine Operations				
Allow input to a virtual machine	Allow output from a virtual machine	Create virtual machine	Delete virtual machine	Change virtual machine authorization scope
Stop virtual machine	Start virtual machine	Pause and restart virtual machine	Reconfigure virtual machine	View virtual machine configuration

Hyper-V Operations at-a-Glance

Networking Operations				
Create virtual switch	Delete virtual switch	Create virtual switch port	Delete virtual switch port	Disconnect virtual switch port
Create internal Ethernet port	Delete internal Ethernet port	Bind external Ethernet port	Unbind external Ethernet port	Change VLAN configuration on port
Modify switch settings	Modify switch port settings	View switches	View switch ports	View external Ethernet ports
View internal Ethernet ports	View VLAN settings	View LAN endpoints	View virtual switch management service	Modify internal Ethernet port

Hyper-V Authorization Scenarios

- Departmental or Service Administrators

A Hyper-V server hosts virtual machines for two different LOB applications.

Admins for each application needs to have full control over their own virtual machines, but should have no access to the other application’s virtual machines, or to Hyper-V.

Hyper-V Authorization Scenarios

- Departmental or Service Administrators

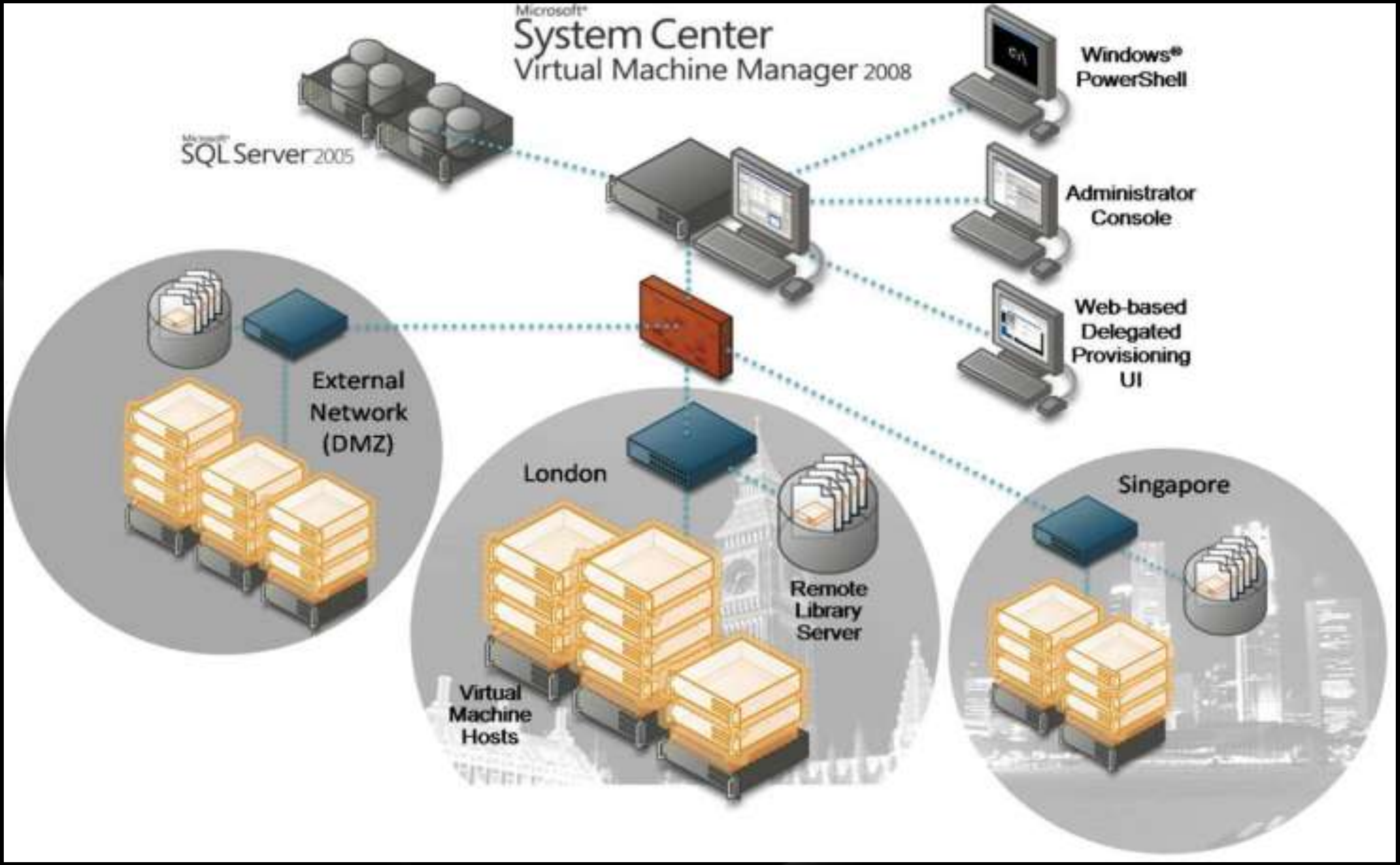
The help desk and, after hours, the Operations Center, perform some first level analysis of issues that are called in by end-users.

They need to be able to view virtual machine configuration information and interact virtual machines. They should not be able to start, stop or save any virtual machines or change any configuration information.

Using AD as an Auth Store

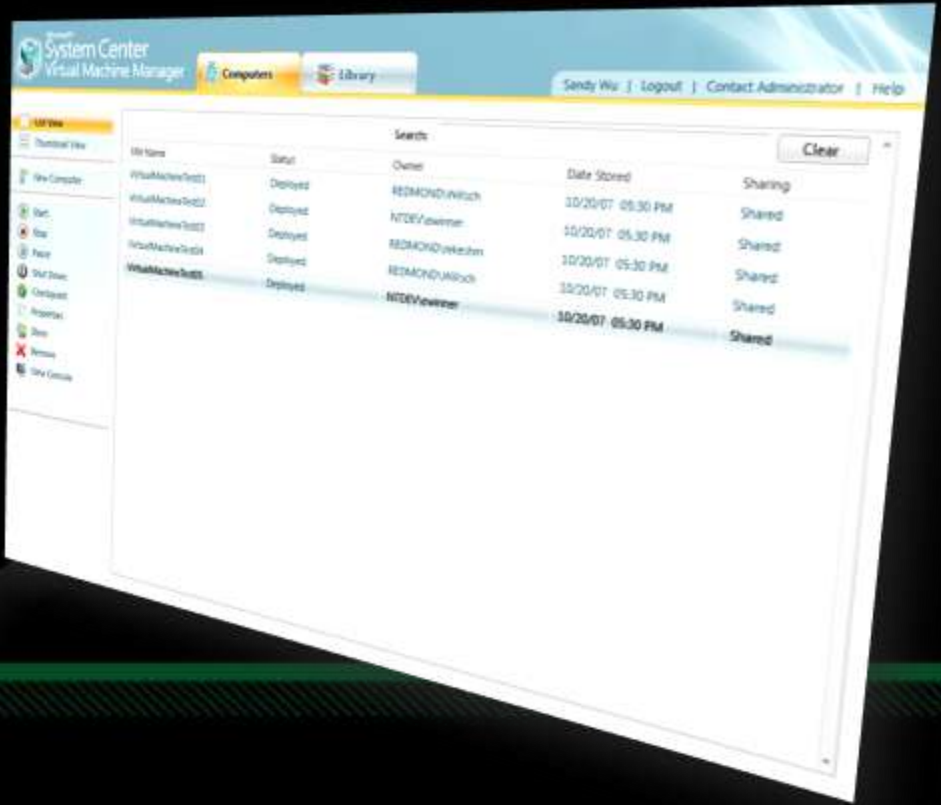
- AzMan supports other auth stores such as Active Directory and SQL Server
- Useful for creating standardized auth policies across several servers
- Use of AD requires WS 2003 domain functional level or better
- Auth policies cannot be created in non-domain partitions
- Hyper-V host computer accounts require *READ* access to the auth store

System Center Virtual Machine Manager



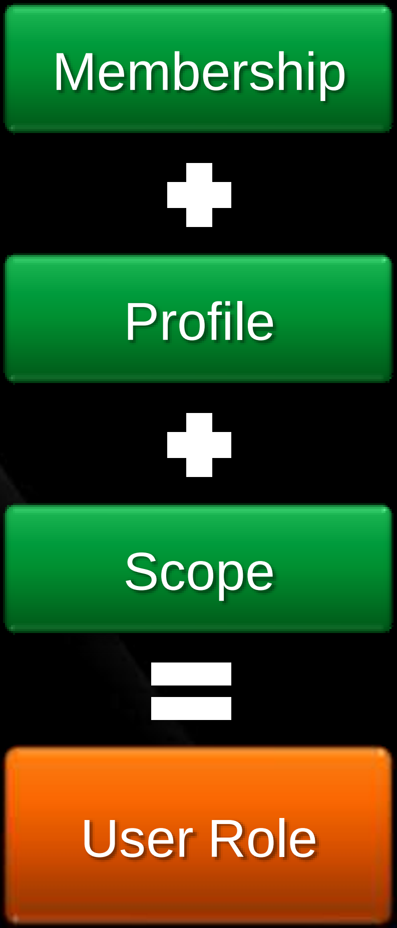
Delegation and Self Service

- Administrators control access through policies which designate capabilities
- Delegated Administrators
  - Manage a scoped environment
- Self service user
  - Web user interface
  - Manage their own VMs
  - Quota to limit VMs
  - Scripting through PowerShell



VM Name	Status	Owner	Date Stored	Sharing
VirtualMachineTest01	Deployed	REDMOND\WRoch	10/20/07 05:30 PM	Shared
VirtualMachineTest02	Deployed	NTDEV\swimmer	10/20/07 05:30 PM	Shared
VirtualMachineTest03	Deployed	REDMOND\vekeshm	10/20/07 05:30 PM	Shared
VirtualMachineTest04	Deployed	REDMOND\WRoch	10/20/07 05:30 PM	Shared
VirtualMachineTest05	Deployed	NTDEV\swimmer	10/20/07 05:30 PM	Shared

Understanding User Roles



Membership

+

Profile

+

Scope

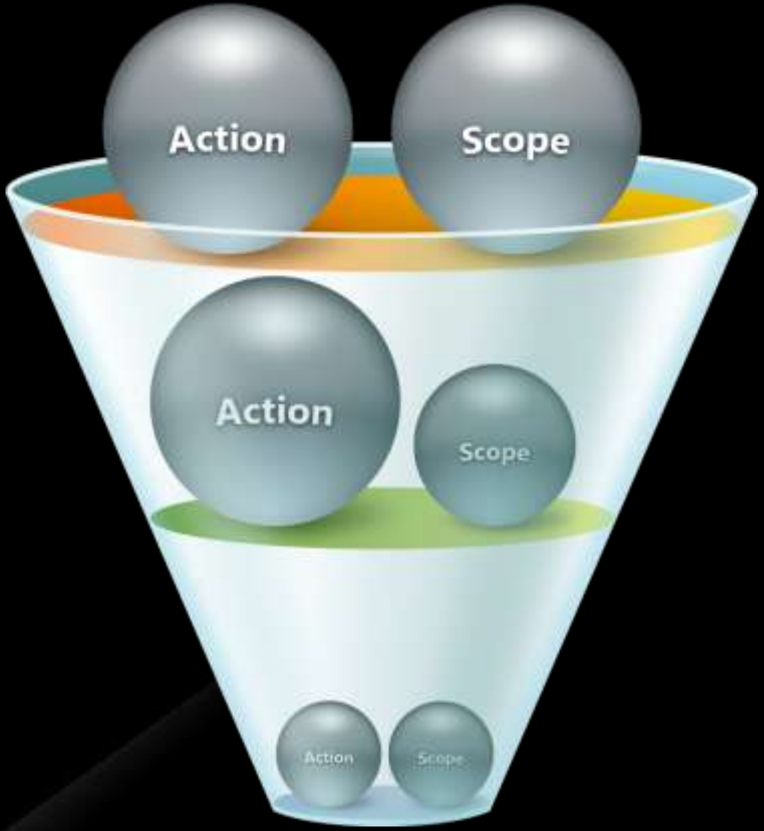
=

User Role

- Membership
  - Determines which users are part of a particular user role
  - Members may be individual users or groups
  - Members may be in multiple user roles including user roles based on different profiles
- Profile determines
  - Which actions are permitted
  - Which user interface is accessible
  - How the scope is defined
- Scope determines
  - Which objects a user may take actions on

Built-In Profiles

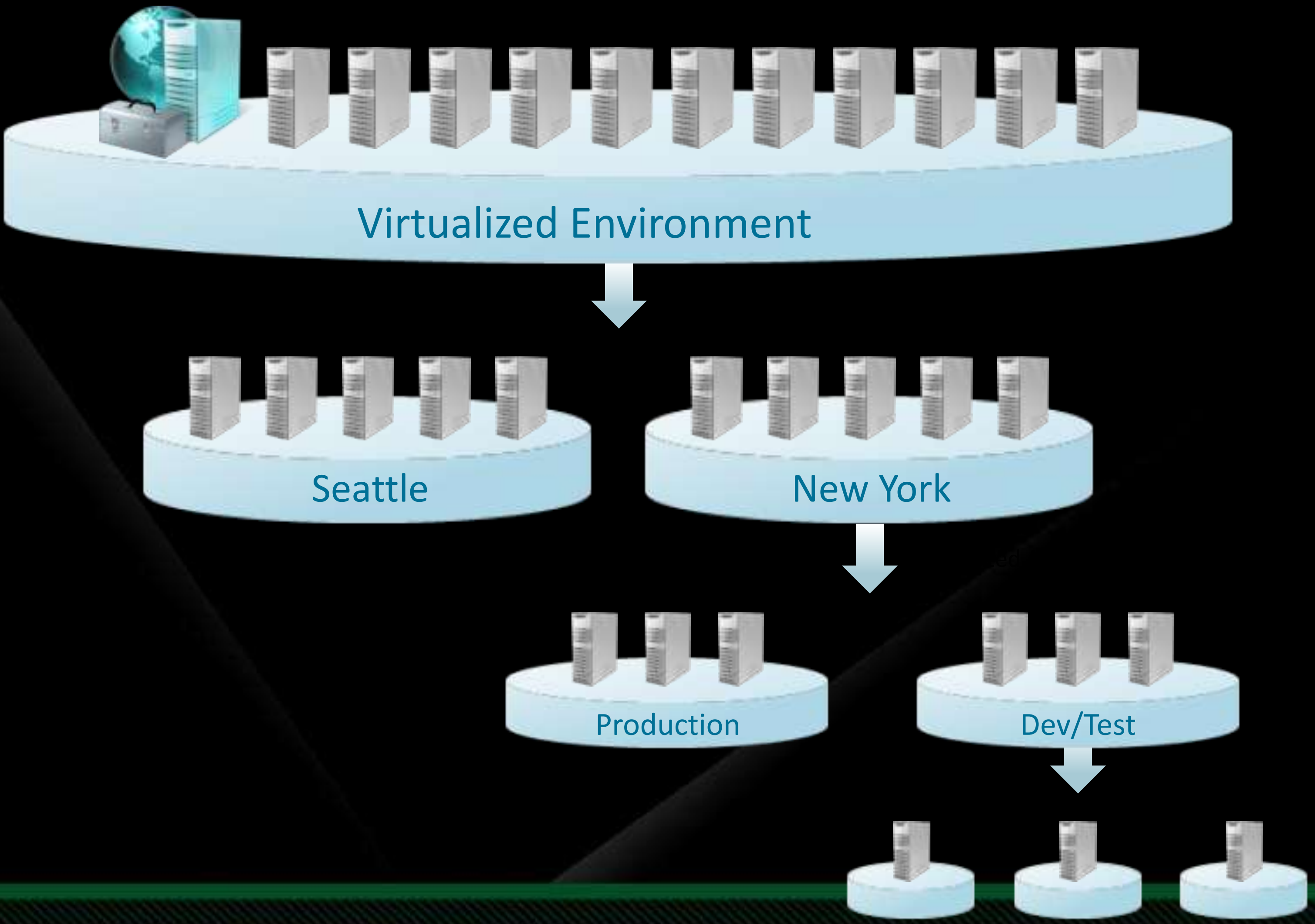
- Administrators
  - Full access to all actions
  - Full access to all objects
  - Can use the Admin console or PowerShell interface
- Delegated Administrators
  - Full access to most actions
  - Scope can be limited by host groups and Library servers
  - Can use the Admin console or PowerShell interface
- Self-Service Users
  - Limited access to a subset of actions
  - Scope can be limited by host groups and Library share
  - Can use the Self-Service Portal or PowerShell interface



Customizing Scopes

- Administrators
  - No scope customization available,
    Administrators have access to all objects
- Delegated Administrators
  - Can be limited to one or more host groups including all child objects
  - Can be limited to one or more Library servers
    including all child objects
- Self-Service Users
  - Can be limited to a single host group where
    new virtual machines may be created
  - Can be limited to a single Library share
    where new virtual machines can be stored
  - Can be limited to specific templates to use for new virtual machines

Delegating Administration



Protecting Virtual Machines

- File system security
- Encryption
- Auditing
- Maintaining virtual machines
- Best practices

Summary

- Virtualization introduces new security concerns
- Hyper-V was designed to achieve strong security goals
- Use the Hyper-V Security Guide to:
  - Install and configure Hyper-V with a strong focus on security
  - Reduce the attack surface of Hyper-V host servers
  - Secure virtual networks and storage devices on a Hyper-V host server
  - Delegate administrative access to virtual machine resources within an organization
  - Protect Virtual Machines - via file system permissions, encryption, and auditing

Online Resources

Virtualization Home Page: www.microsoft.com/virtualization

Virtualization Solution Accelerators: www.microsoft.com/vsa

MAP tool : http://microsoft.com/map

Hyper-V Green Tool : http://hyper-green.com

આભાર

ধন্যবাদ

நன்றி

धन्यवाद

Thank You!

ధన్యవాదాలు

ಧನ್ಯವಾದಗಳು

ଧନ୍ୟବାଦ

ਧੰਨਵਾਦ

നിങ്ങൾക്ക് നന്ദി

Microsoft®

Your potential. Our passion.™