



# W11 – Hyper-V security

Jesper Krogh

[jesper\\_krogh@dell.com](mailto:jesper_krogh@dell.com)

# Speaker intro

- Jesper Krogh
  - Senior Solution architect at Dell
    - Responsible for Microsoft offerings and solutions within Denmark
    - Specialities within: Active Directory, Exchange and the client platform
    - 15 years of consultancy experience
- Dell Services
  - 30000 consultants worldwide
    - Focusing upon infrastructure services
    - Enterprise architecture, Datacenter and End-user computing

# Agenda

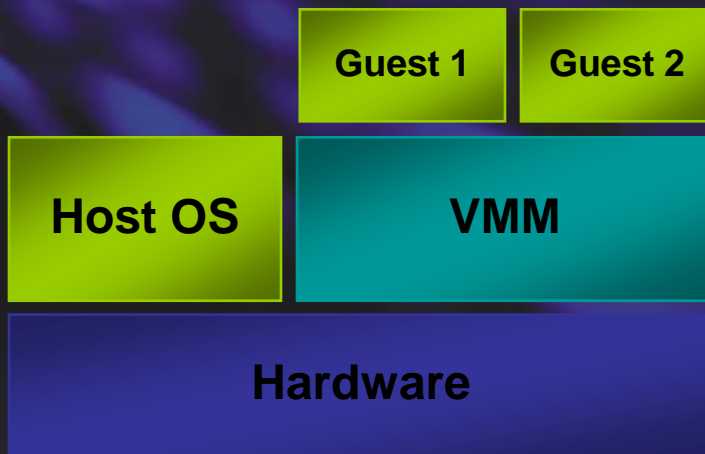
- Virtualization Overview
- Hyper-V Architecture
- Hyper-V Security Overview
- Hyper-V Security Guide
- Summary!

# 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

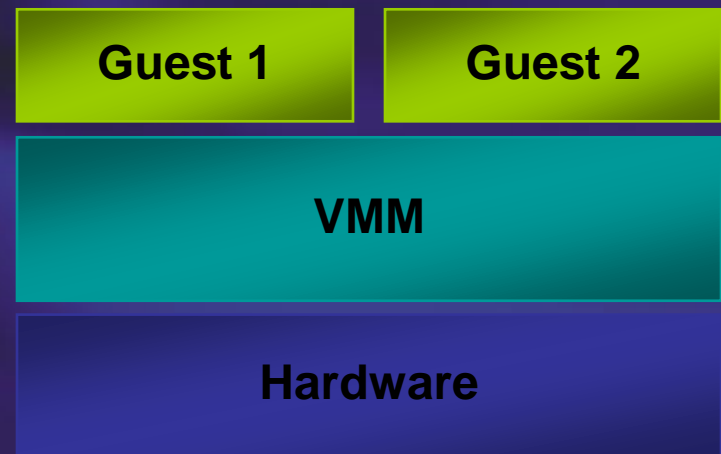
- Hosted Virtualization



- Examples:

- VMware Workstation
- KVM
- Virtual PC & Virtual Server

- Hypervisor Virtualization



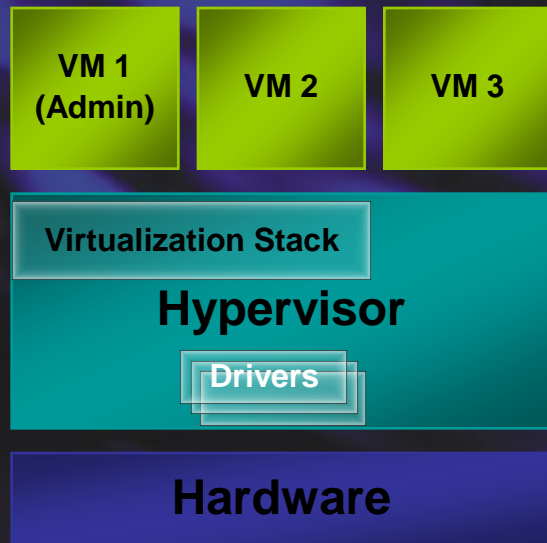
- Examples:

- VMware ESX
- Xen
- Hyper-V



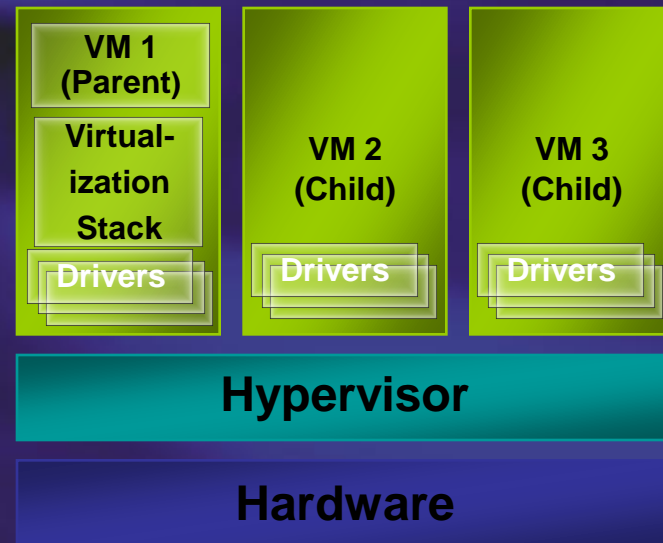
# Monolithic Versus Microkernel Hypervisor

- 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!

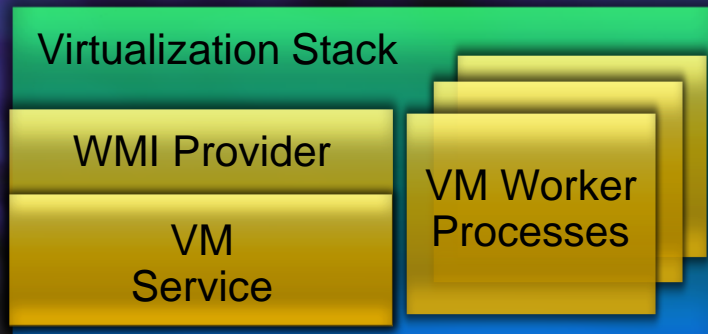
# Hyper-V Background

- 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

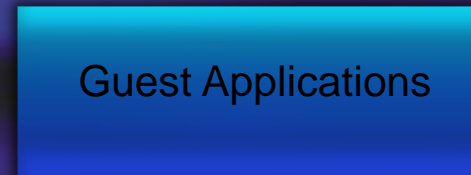


# Hyper-V Architecture

## Root Partition

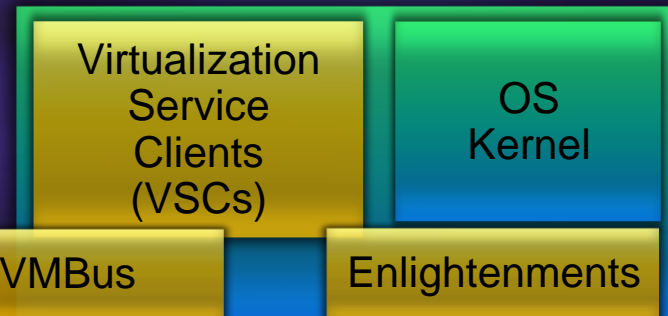
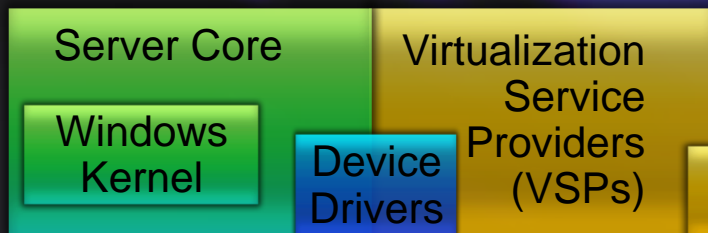
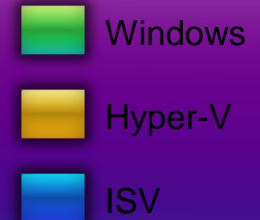


## Guest Partitions



Ring 3: User Mode

Provided by:

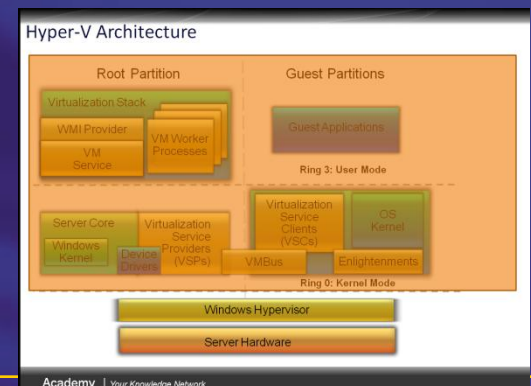


Ring 0: Kernel Mode



# Hypervisor

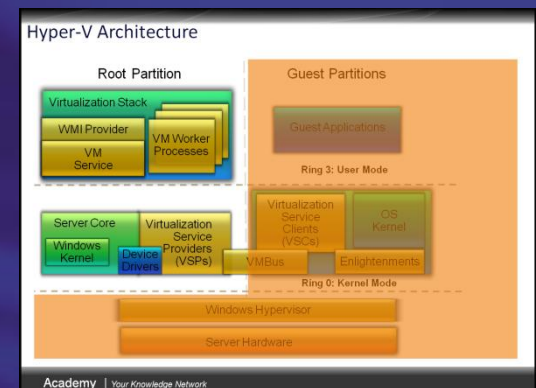
- Partitioning Kernel
  - Partition is an isolation boundary
  - Few virtualization functions; relies on virtualization stack
- Very thin layer of software
  - Microkernel
  - Highly reliable
- No device drivers
  - Two versions, one for Intel and one for AMD
  - Drivers run in the root partition
  -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



Academy | Your Knowledge Network

# 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!



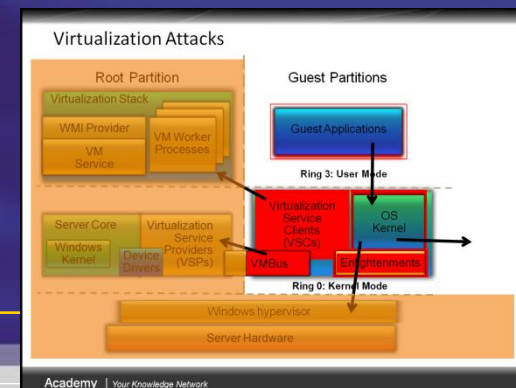
# Top Virtualization Security Concerns

- 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



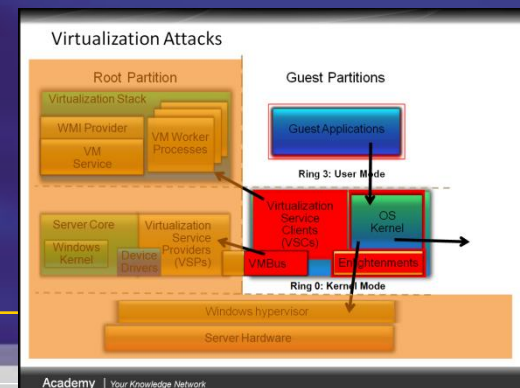
# Security Assumptions

- 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

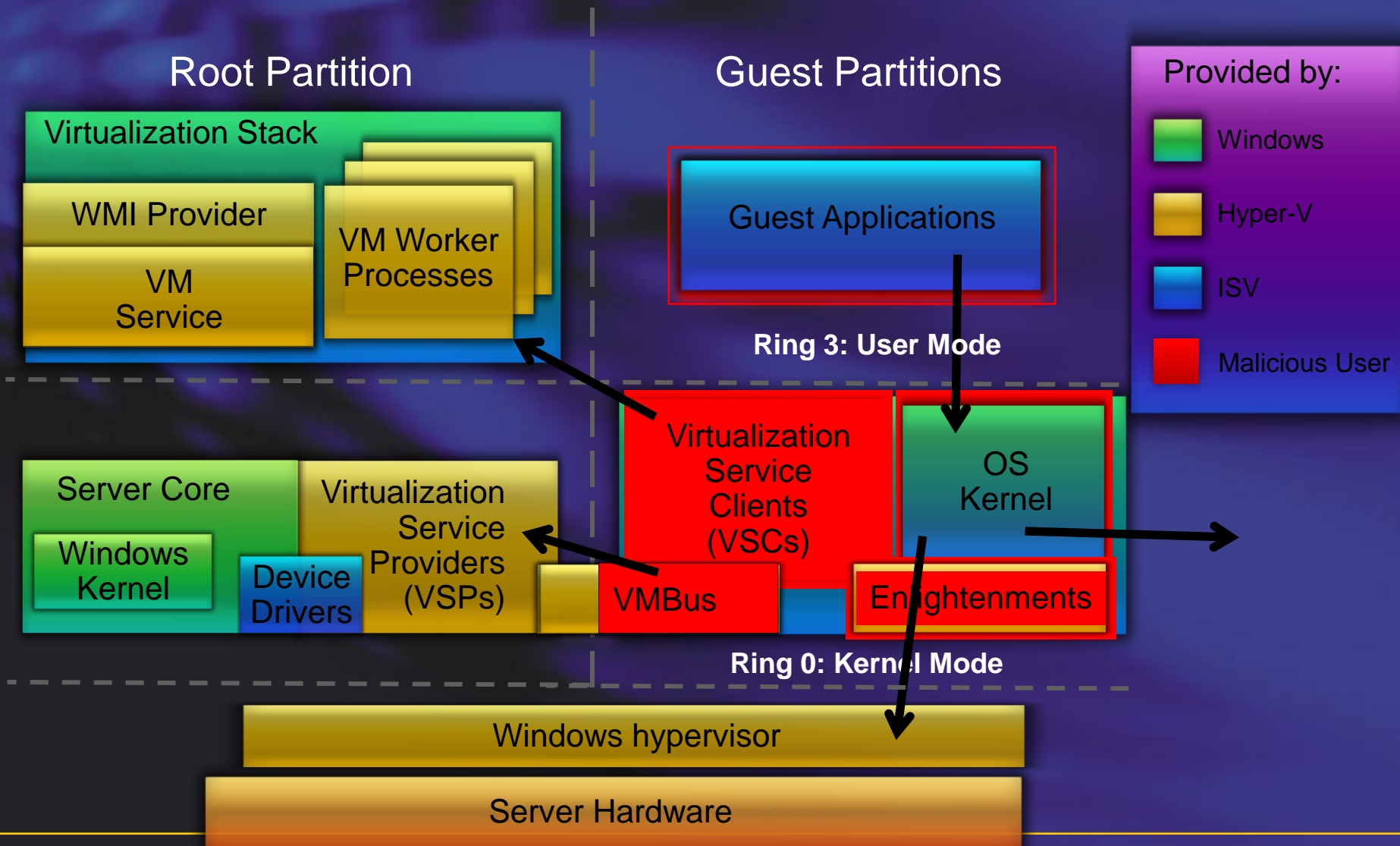
- Strong isolation between partitions
- Protect confidentiality and integrity of guest data
- Separation
  - Unique hypervisor resource pools per guest
  - Separate per-guest worker processes manage state
  - Guest-to-root communications over unique channels
- Non-interference
  - Guests cannot affect 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

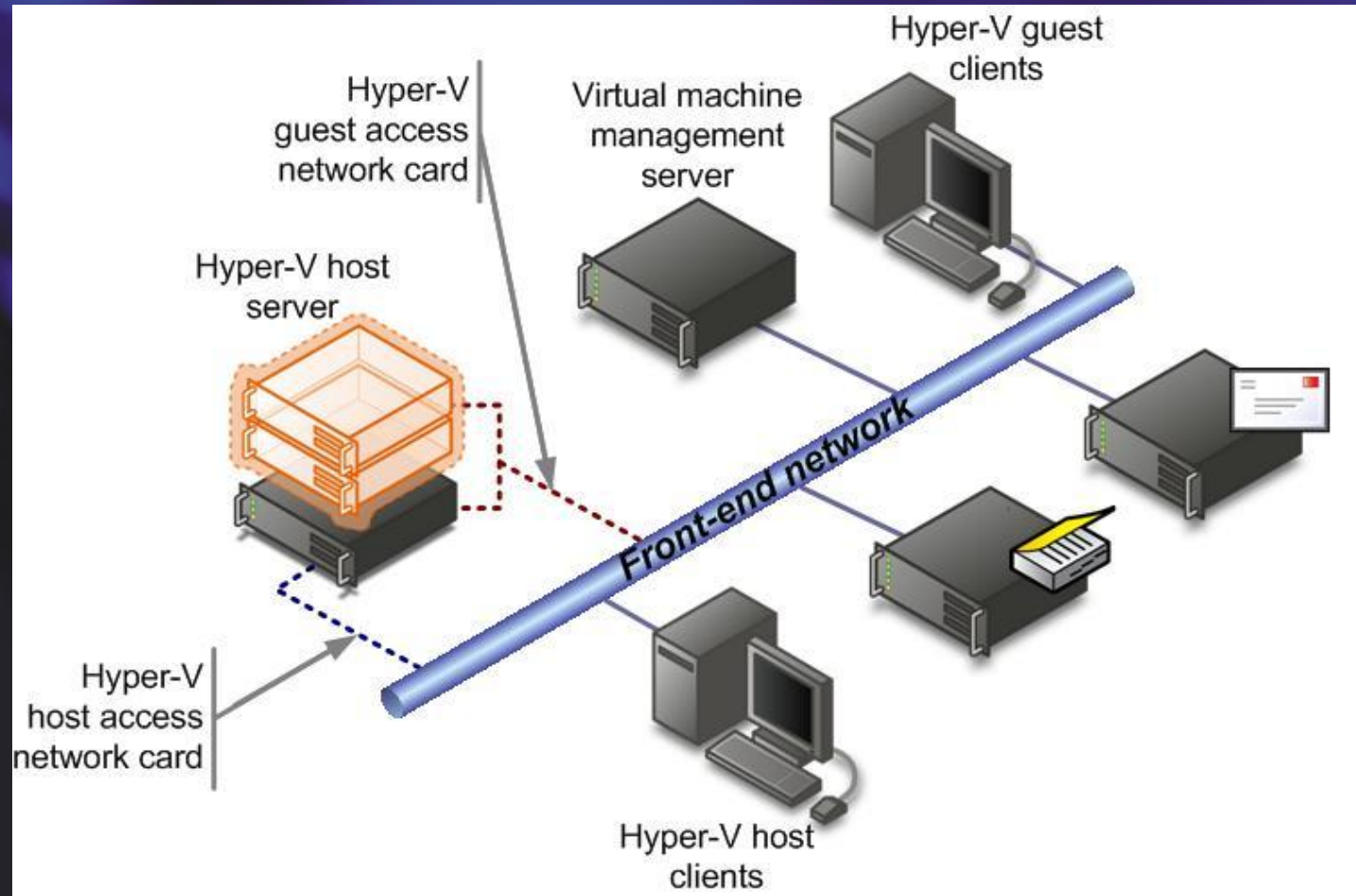
# Attack Surface

- 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
  - [Hyper-V Attack Surface Reference Workbook](#)
  - [Let's see it ☺](#)

# 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



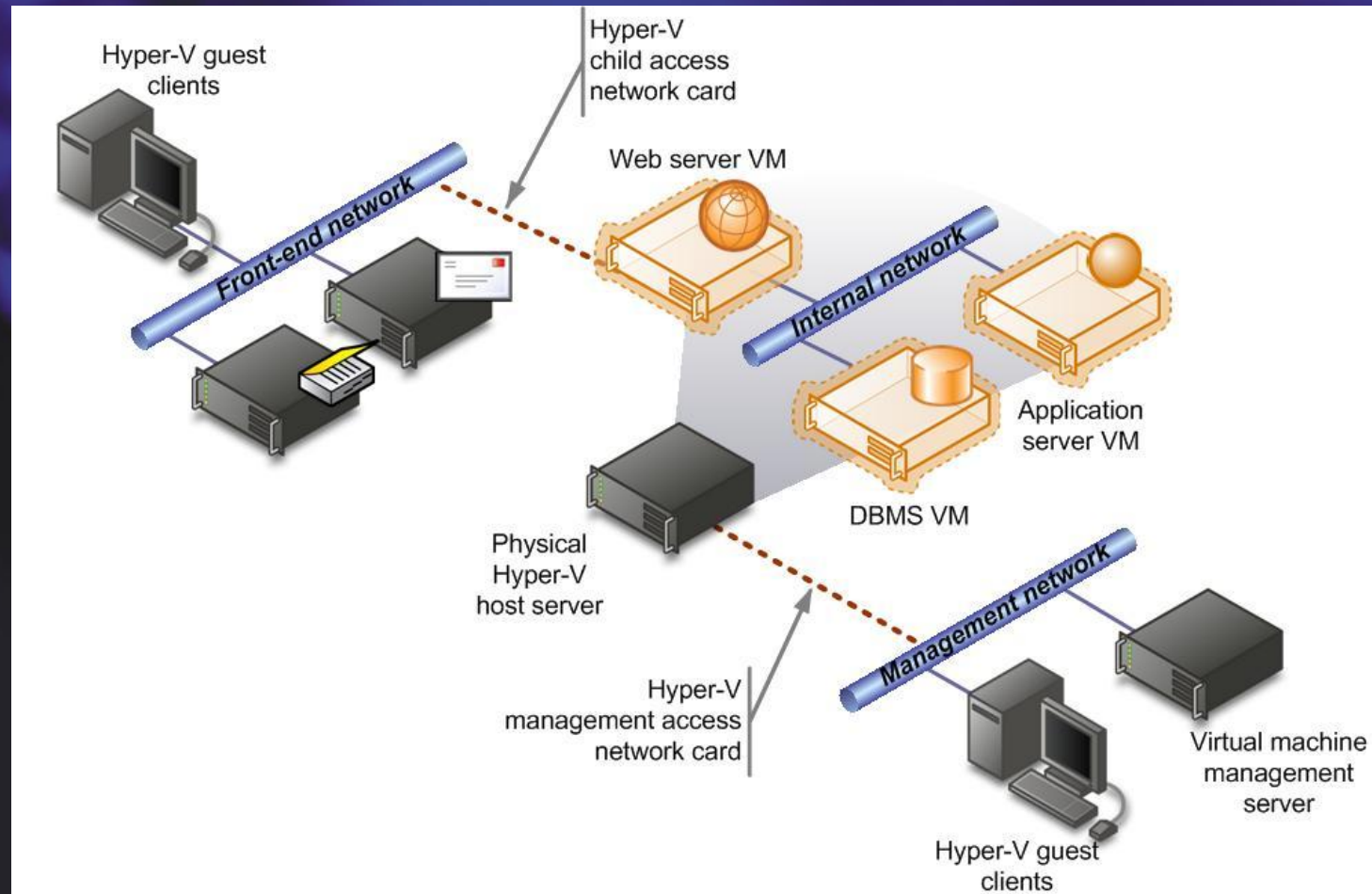


# Hyper-V Networks

- **External virtual networks**
  - use virtual network switches that are bound to a network adapter in the physical computer. Any virtual machines attached to an external virtual network can access the same networks to which the physical adapter is connected.
- **Internal virtual networks**
  - use virtual network switches that are not bound to a network adapter in the physical computer. An internal virtual network is isolated from networks external to the physical computer. However, virtual machines connected to an internal virtual network can communicate with the management operating system.
- **Private virtual networks use**
  - virtual network switches that are not bound to a network adapter in the physical computer, as with internal virtual networks. However, network traffic from virtual machines connected to a private network is completely



# Network Configuration for Multi-tier Web Application



# When installing Hyper-V

- Dedicate one adapter for management

**Add Roles Wizard**

**Create Virtual Networks**

Before You Begin  
Server Roles  
Hyper-V  
**Virtual Networks**  
Confirmation  
Progress  
Results

Virtual machines require virtual networks to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual network.

One virtual network will be created for each network adapter you select. We recommend that you create at least one virtual network now for use with virtual machines. You can add, remove, and modify your virtual networks later by using the Virtual Network Manager.

Ethernet Cards:

Name	Network Adapter
<input type="checkbox"/> Management_NIC	HP NC373i Multifunction Gigabit Server Adapter #2
<input checked="" type="checkbox"/> VirtualMachine_NIC	HP NC373i Multifunction Gigabit Server Adapter

**i** We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual network.

[More about virtual networks](#)

< Previous   Next >   Install   Cancel

# Storage for Virtual Machines

- Configuration normally placed at:
  - `%programdata%\Microsoft\Windows\Hyper-V\`
  - **Should be acceptable for normal scenarios**
- Virtual Harddisks normally placed at:
  - `%users%\Public\Documents\Hyper-V\Virtual Hard Disks`

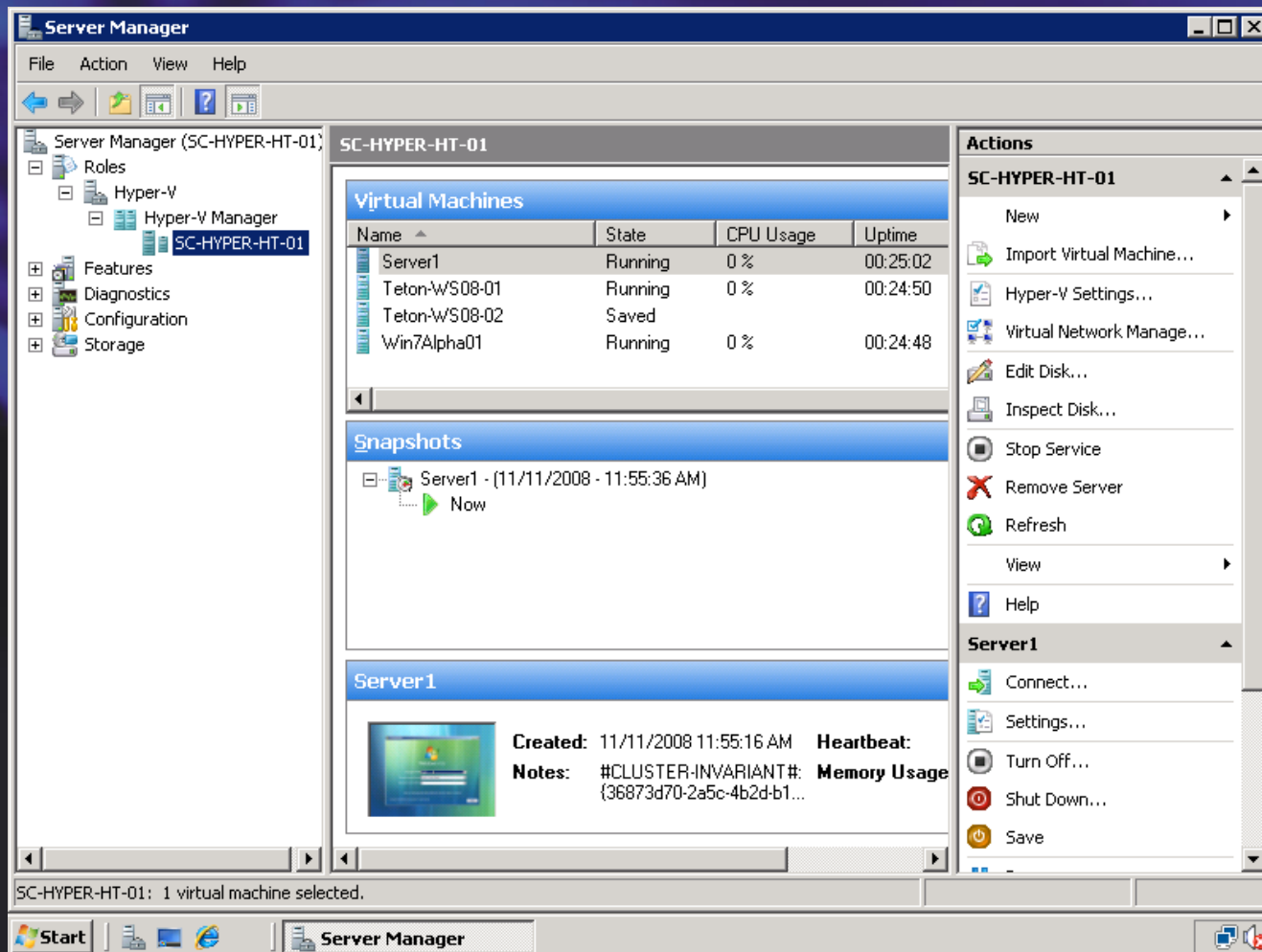
# Securing Dedicated Storage Devices

Set the following permissions (if you change)

Names	Permissions	Apply to
Administrators System	Full Control	This folder, subfolders, and files
Creator Owner	Full Control	Subfolders and files only
Interactive Service Batch	Create files/write data Create folders/append data Delete Delete subfolders and files Read attributes Read extended attributes Read permissions Write attributes Write extended attributes	This folder, subfolders, and files

Exclude Antivirus scanning on the directories and program files vmms.exe and vmwp.exe in C:\Windows\System32

# Normal VM administration

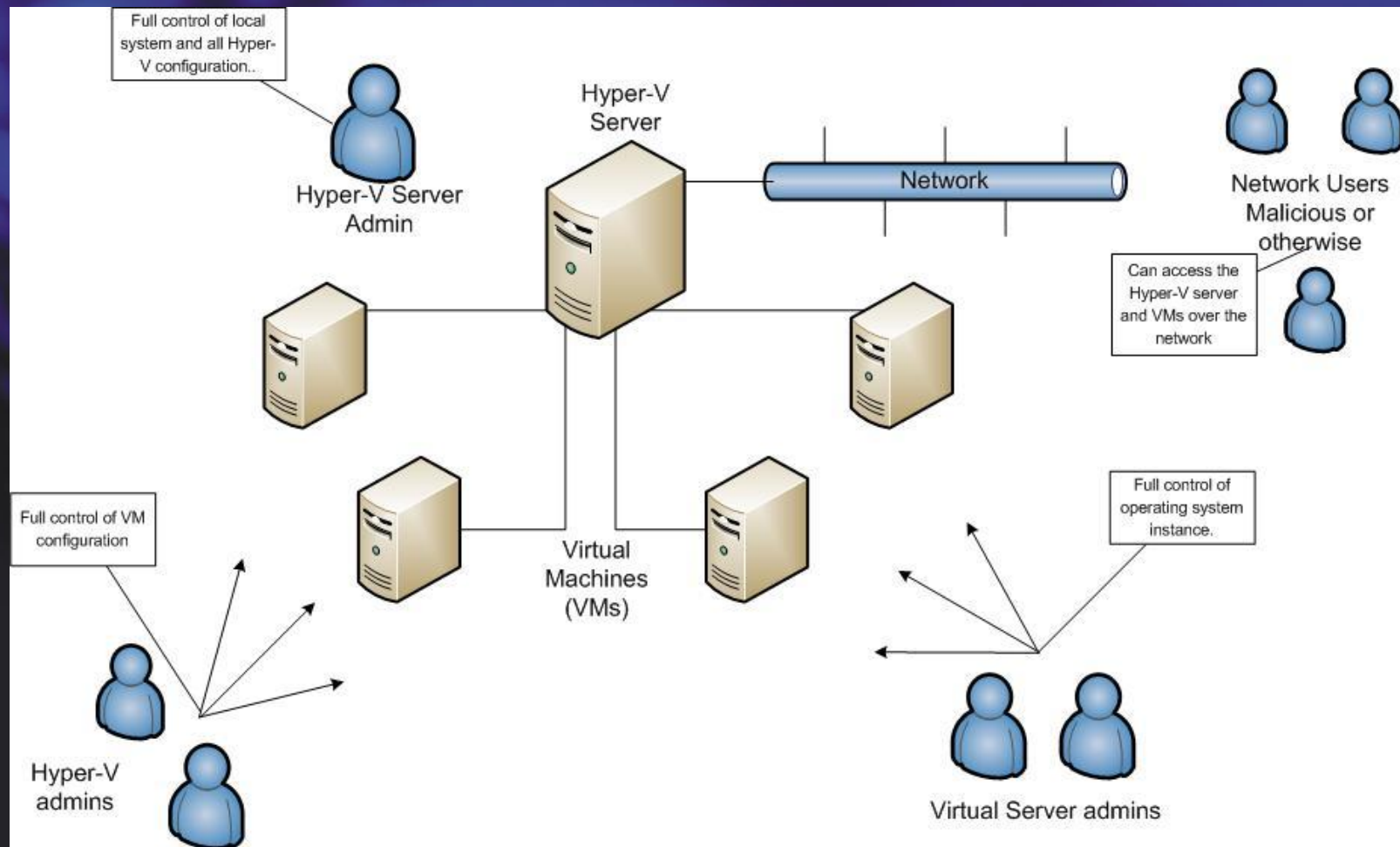




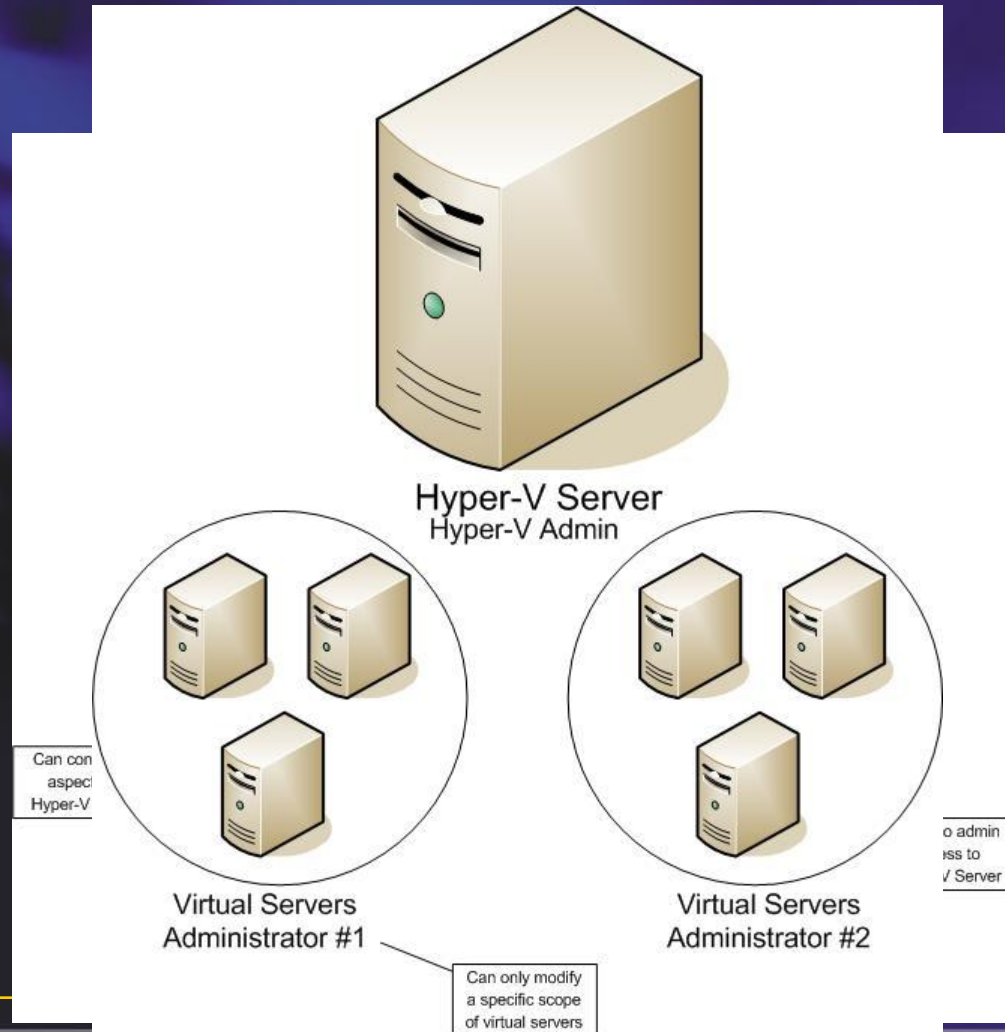
# Delegating VM Management

- 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



# Delegating VM Management



# 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

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

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

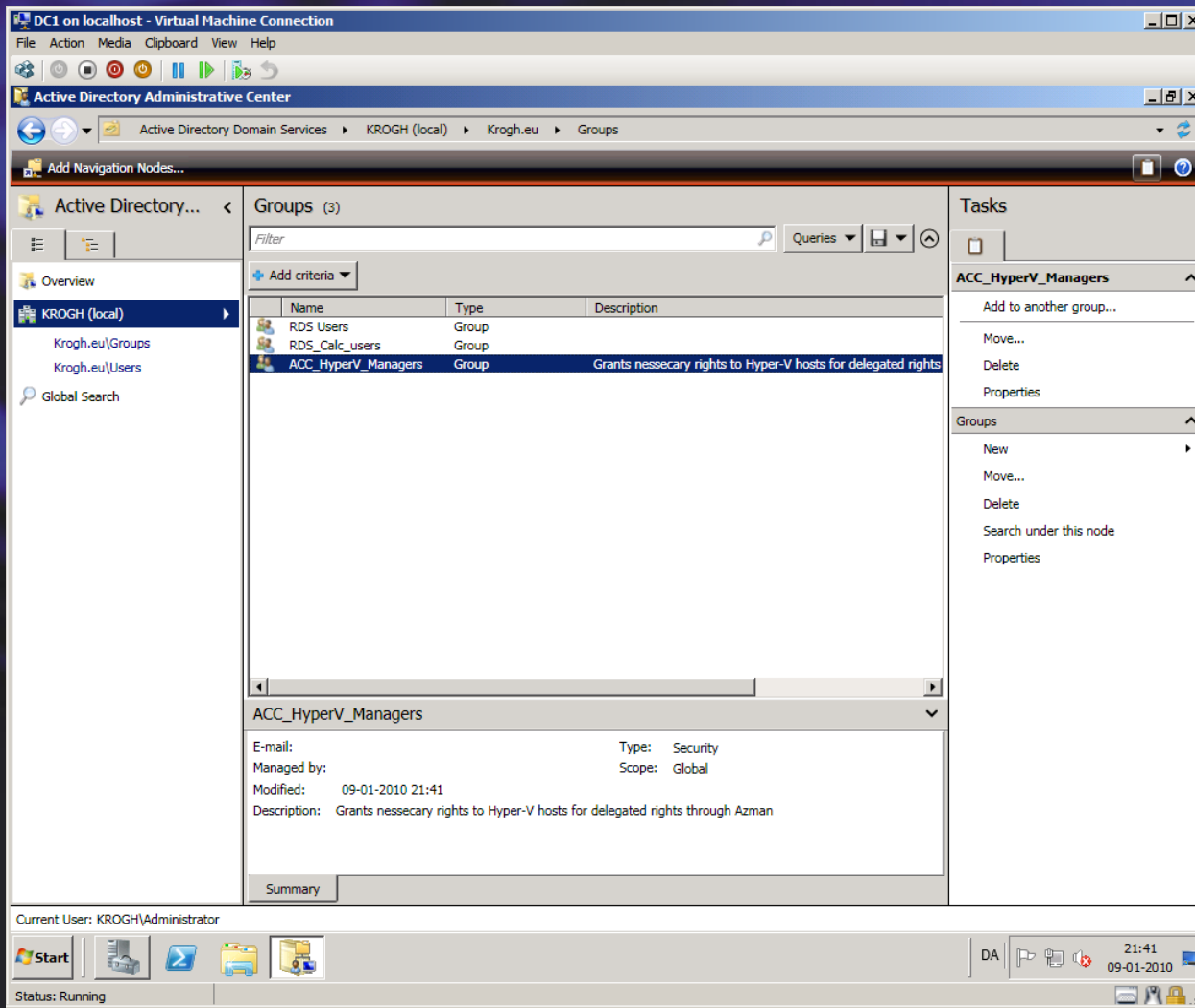
Demo

# CREATING ROLES IN AZMAN

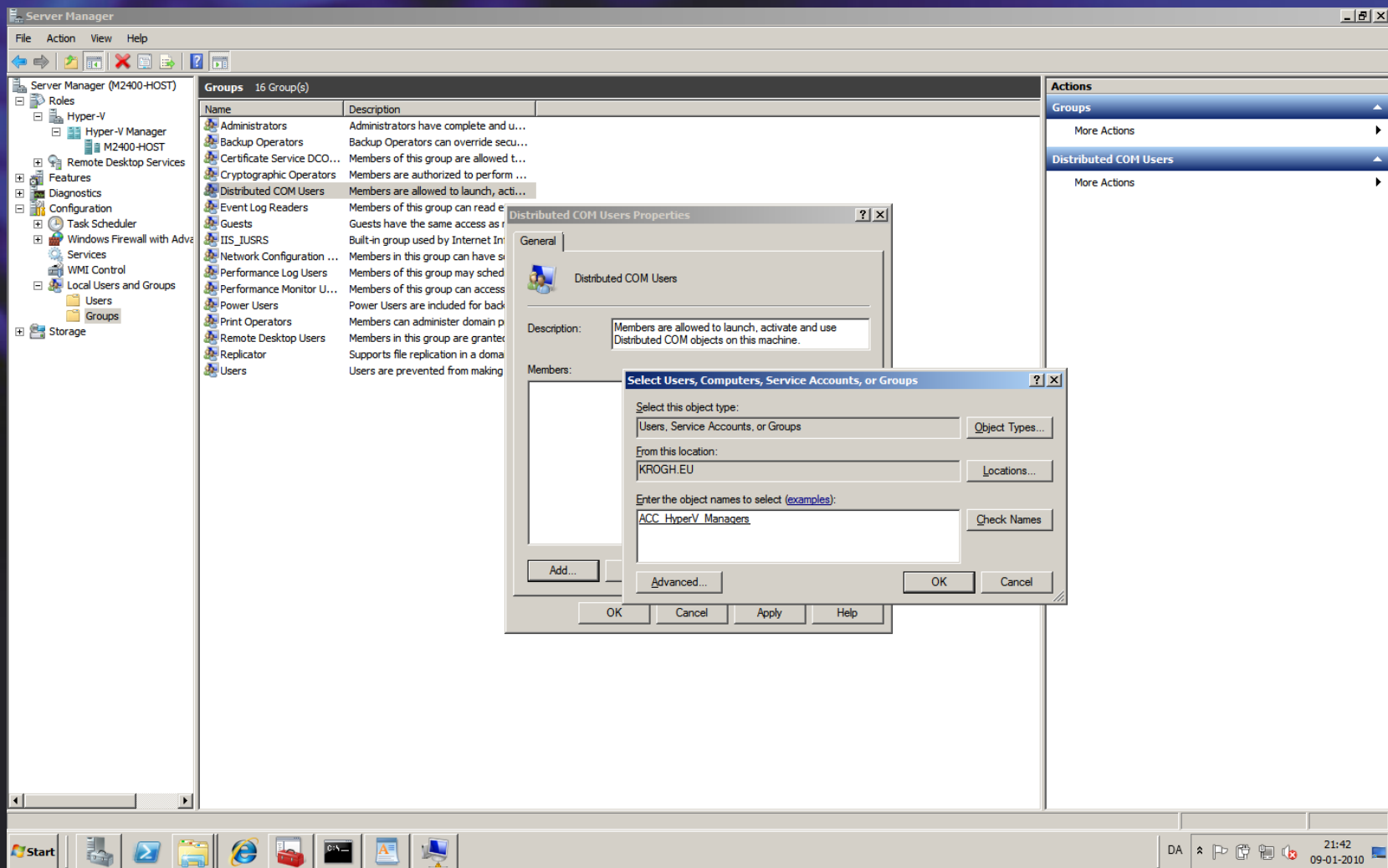
# And the extras

- Users need to have the following rights
  - Membership of "Distributed DCOM Users"
  - Remote Enable and Enable account of:
    - WMI CIMV2 Namespace
    - WMI Virtualization Namespace

# Let's see

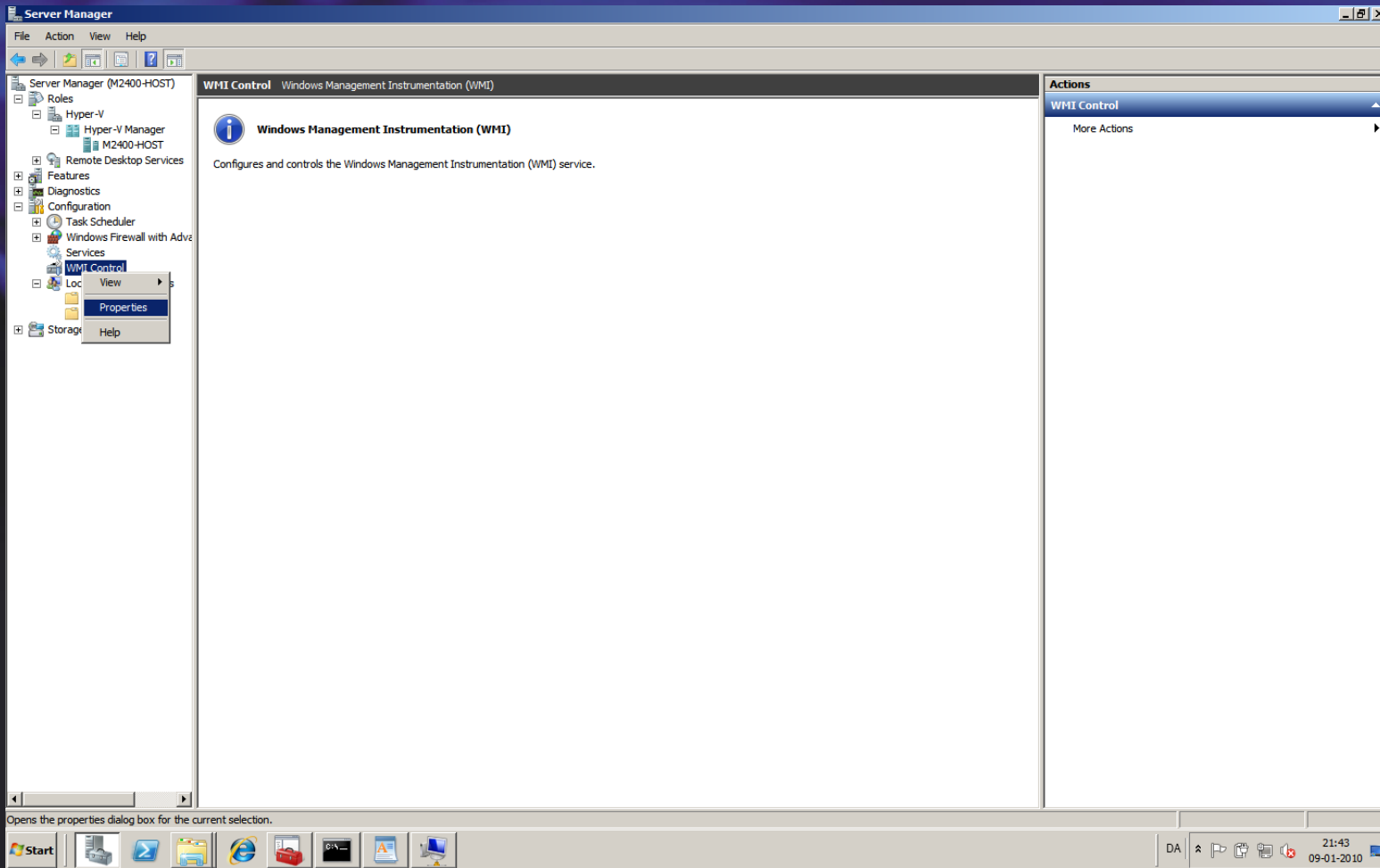


# Let's see

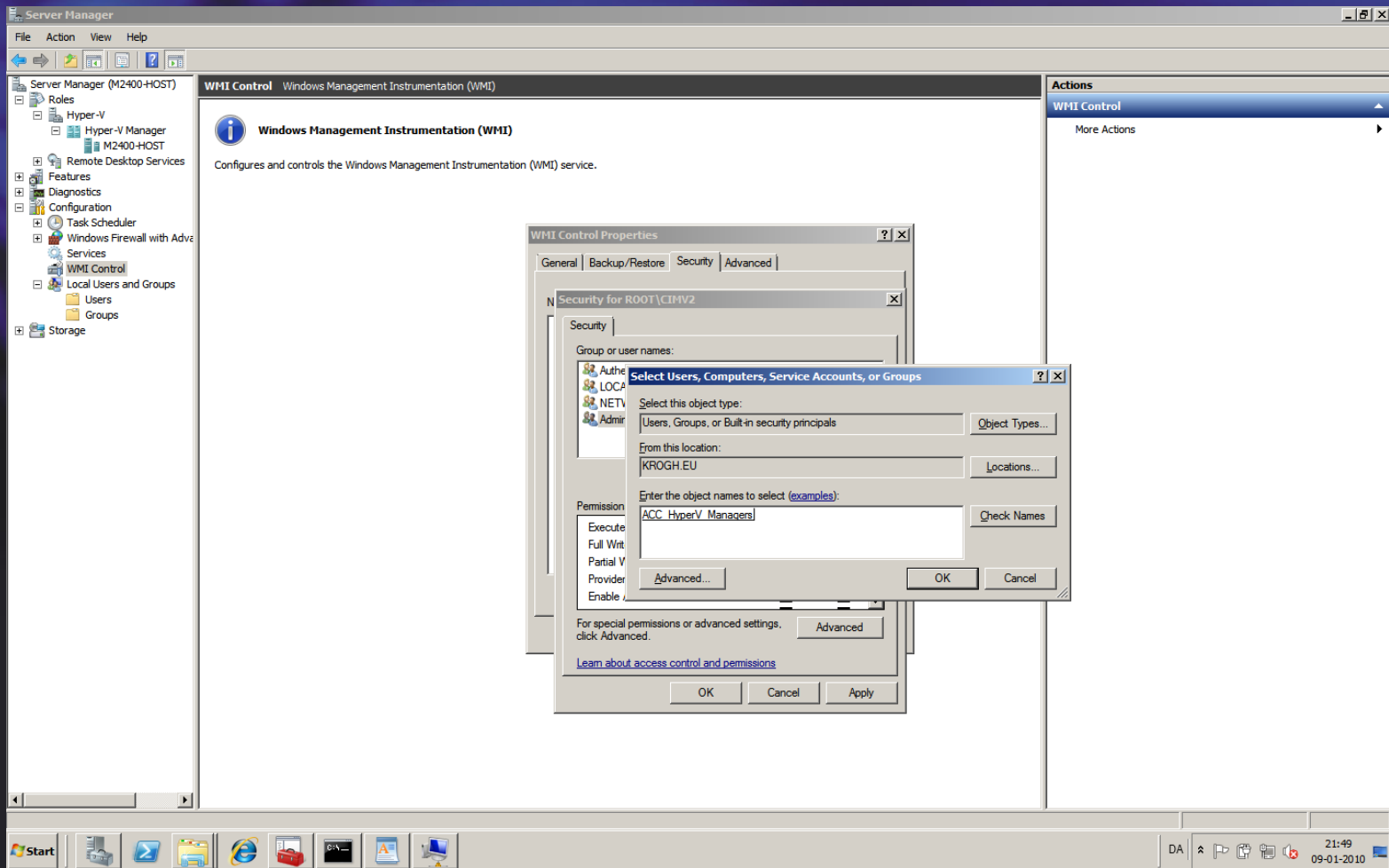




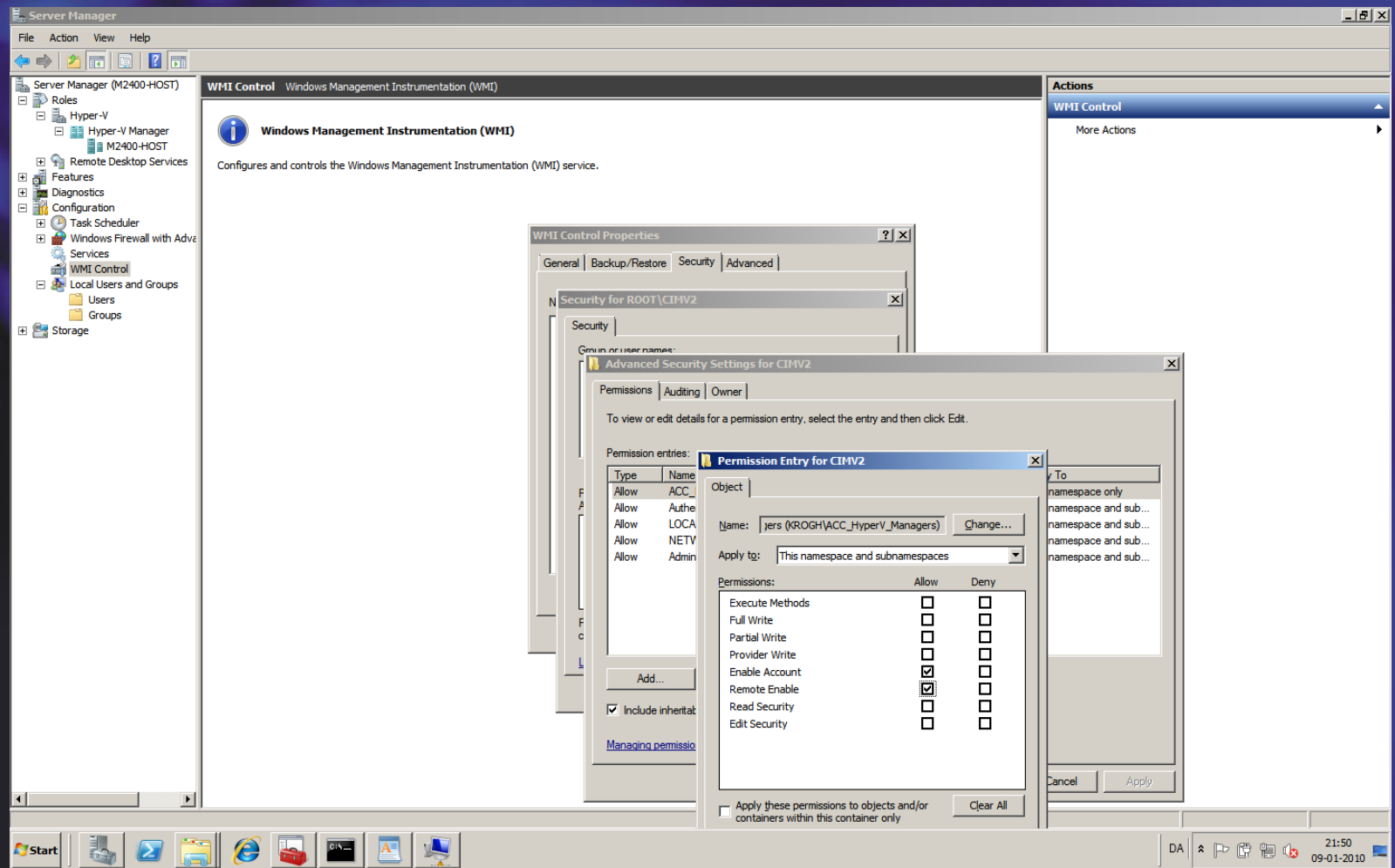
# Let's see



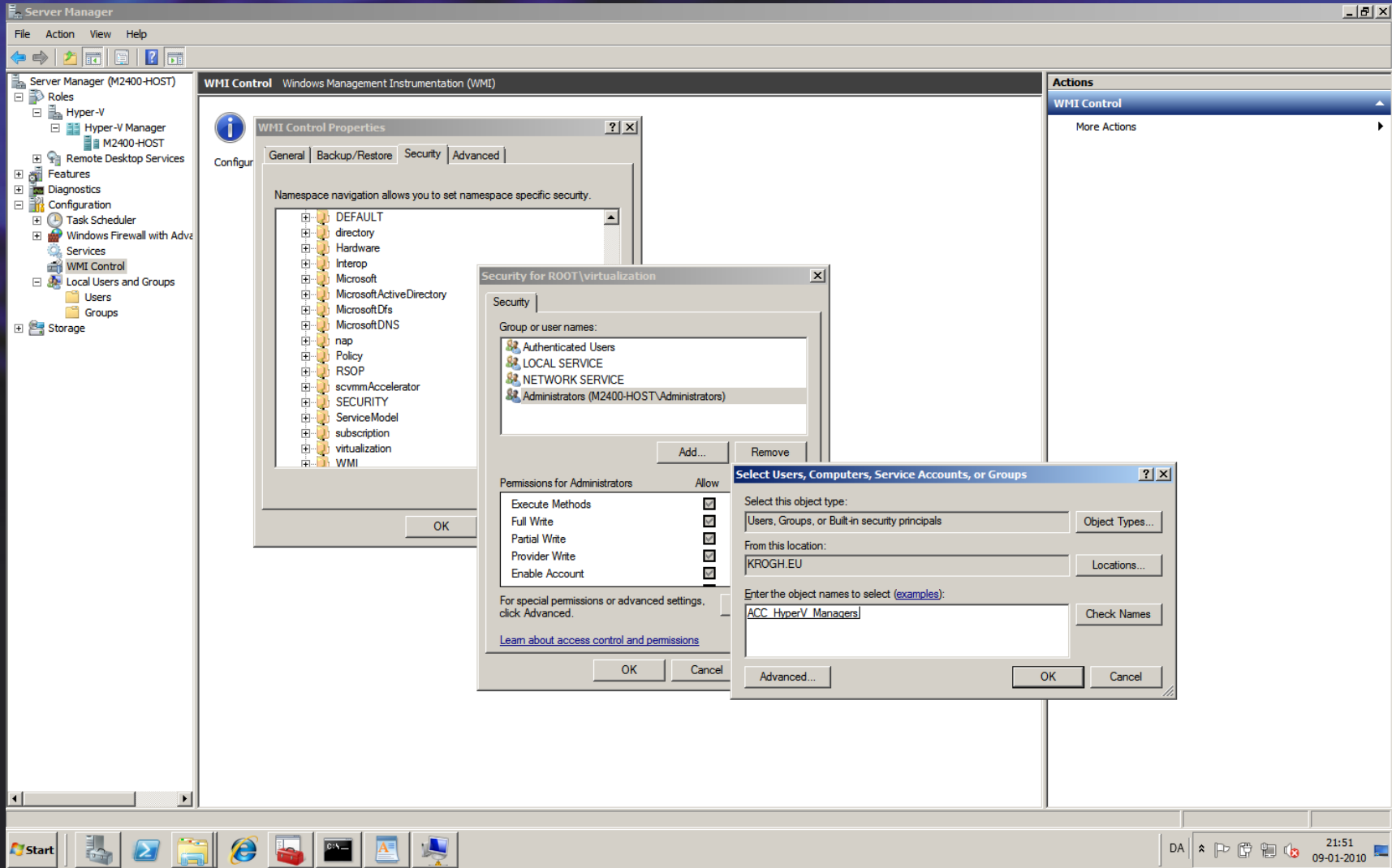
# Let's see



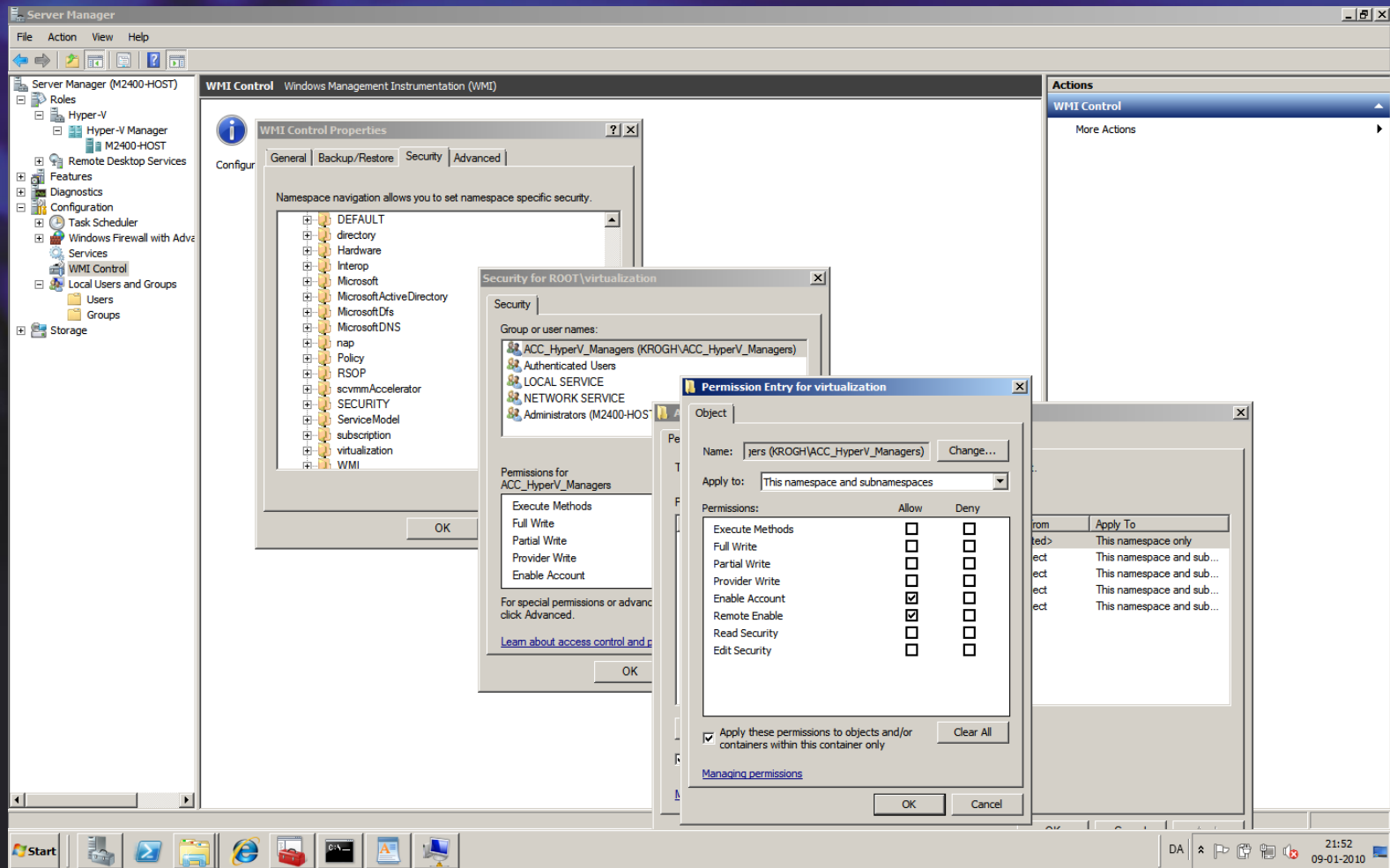
# Let's see



# Let's see

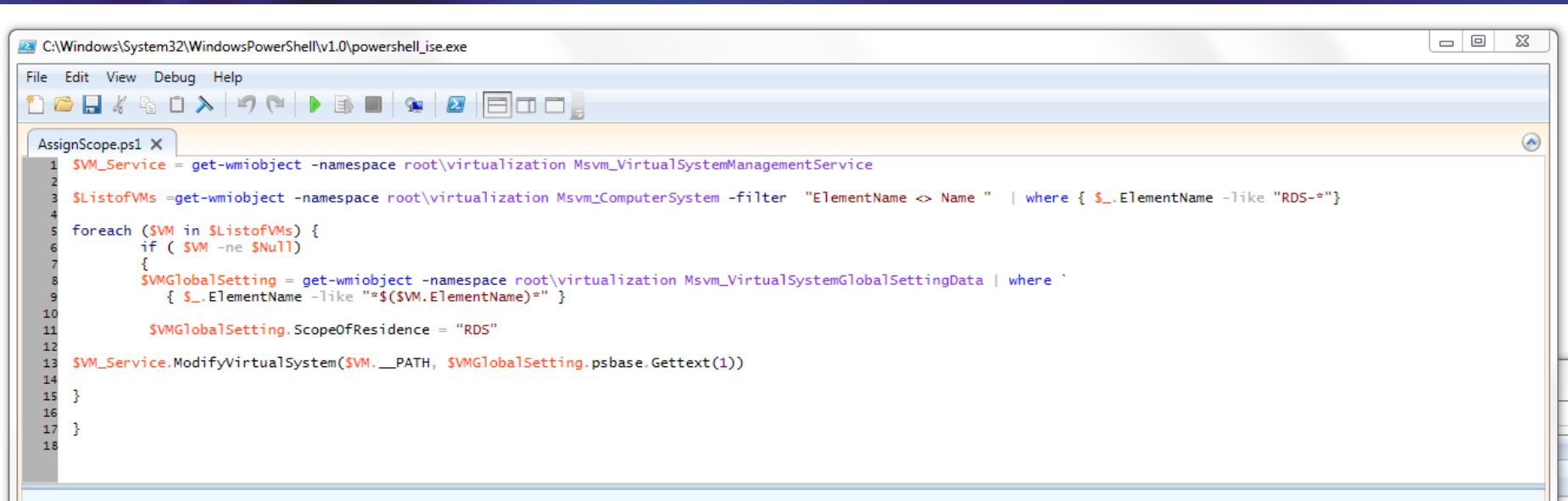


# Let's see





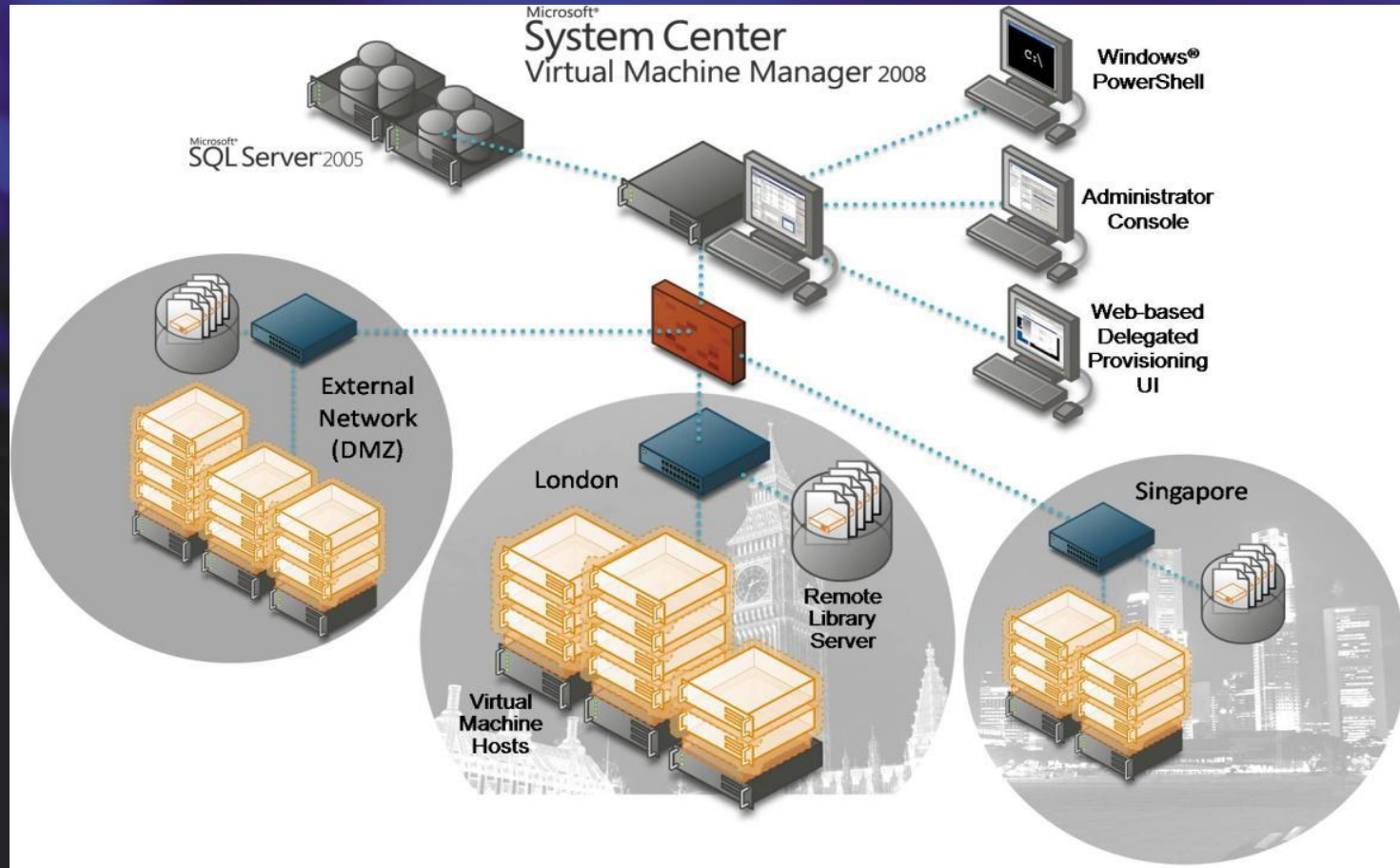
# Let's see



The screenshot shows a Windows PowerShell ISE window titled "C:\Windows\System32\WindowsPowerShell\v1.0\powershell\_ise.exe". The window contains a script named "AssignScope.ps1" with the following code:

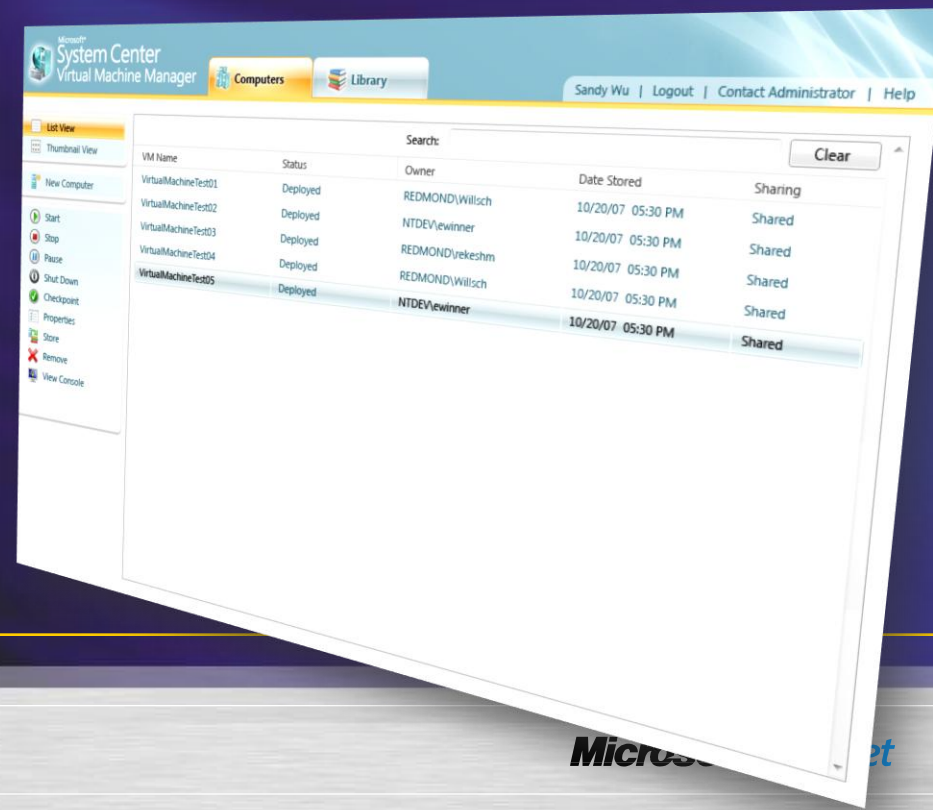
```
1 $VM_Service = get-wmiobject -namespace root\virtualization Msvm_VirtualSystemManagementService
2
3 $ListofVMs = get-wmiobject -namespace root\virtualization Msvm_ComputerSystem -filter "ElementName <> Name " | where { $_.ElementName -like "RDS-*"}
4
5 foreach ($VM in $ListofVMs) {
6     if ( $VM -ne $Null)
7     {
8         $VMGlobalSetting = get-wmiobject -namespace root\virtualization Msvm_VirtualSystemGlobalSettingData | where `
9             { $_.ElementName -like "$($VM.ElementName)*" }
10
11         $VMGlobalSetting.ScopeOfResidence = "RDS"
12
13         $VM_Service.ModifyVirtualSystem($VM.__PATH, $VMGlobalSetting.psbase.GetText(1))
14     }
15 }
16
17 }
18
```

# System Center Virtual Machine Manager

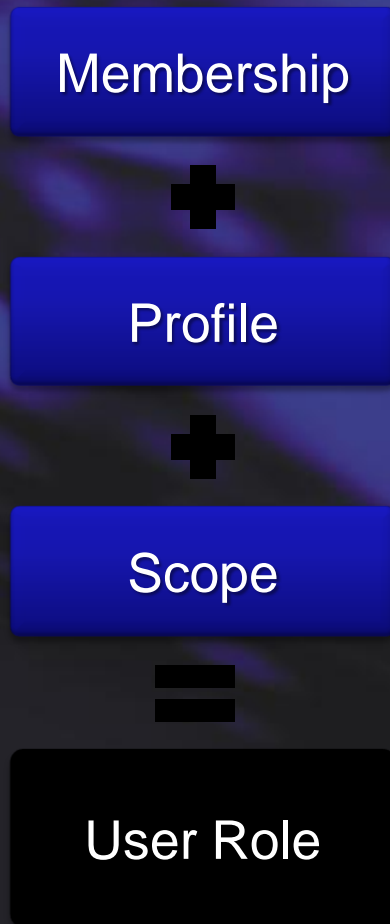


# Delegation and Self Service

- 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



# Understanding User Roles

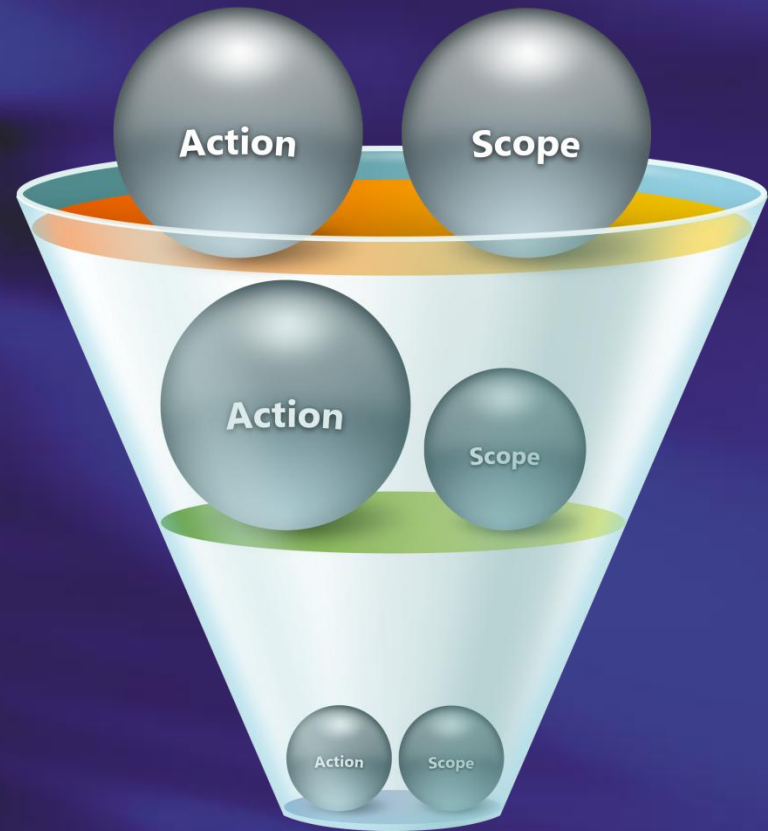


- Membership
  - Determines which users are part of a particular user role
  - Members may be individual users or groups
  - Members may be in multiple user roles including user roles based on different profiles
- Profile determines
  - Which actions are permitted
  - Which user interface is accessible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

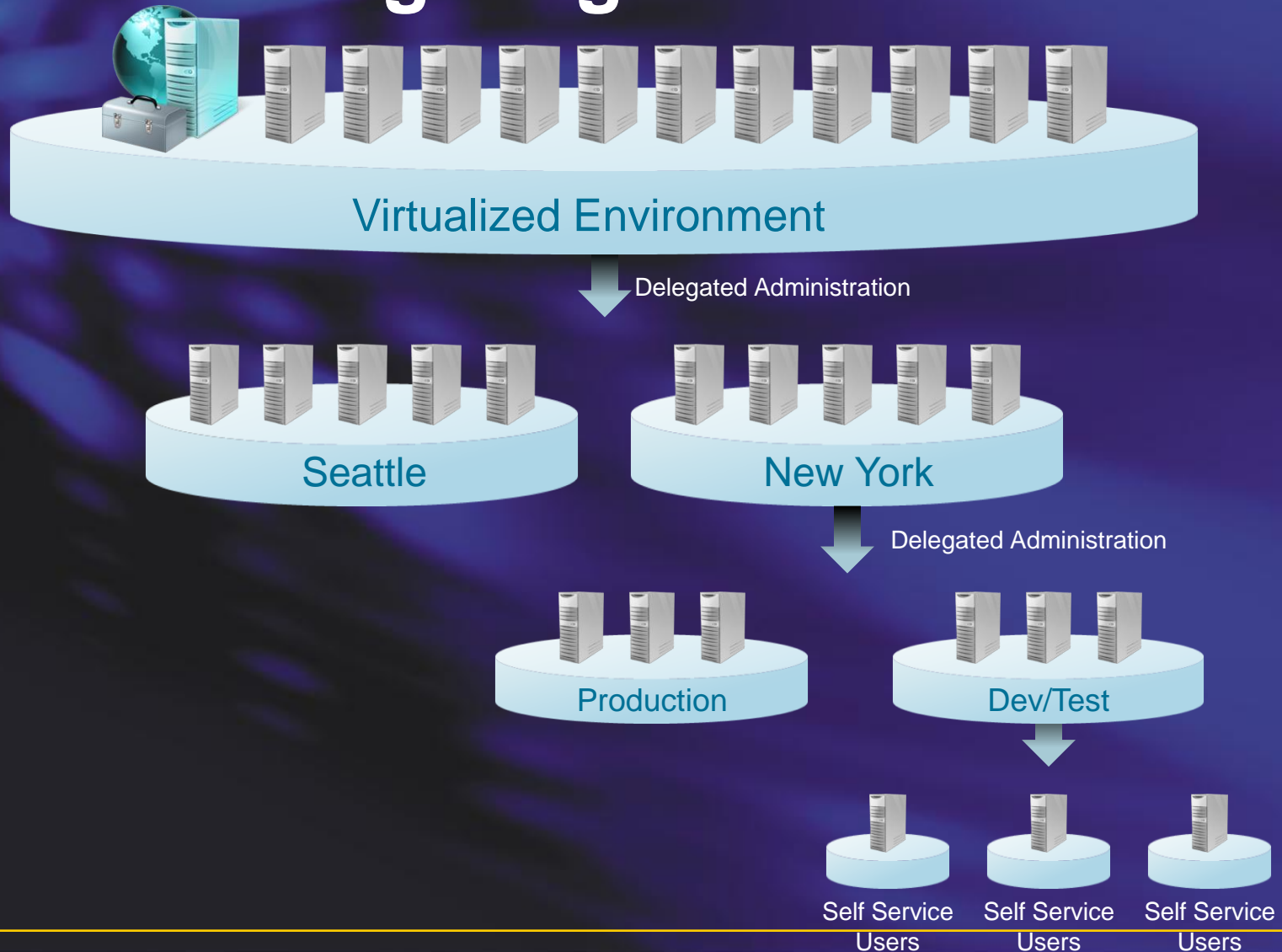




# Customizing Scopes

- 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

- Treat as normal machine
- Remember that the files need to be secured

Demo

# DELEGATING RIGHTS WITHIN SCVMM

# Virtual machine security hardening the OS

- Stick to normal security guidelines
- Enable Firewall and Antivirus
  - As always !
- Place the VM into proper OU
  - Use GPO's to secure the machine



# Protecting the files

- Each virtual machine runs in the context of a virtual machine worker process (vmwp.exe), which runs under the NETWORK SERVICE account and which is able to access the file system resources that make up the virtual machine.
- Delegate Admin rights according to Azman / SCVMM
- Delegate file permissions with groups
- Use encryption
  - Yes – if the machine is insecure

# Offline servicing

- To keep VMs up-2-date might pose a challenge
  - Operating system, applications, antivirus signatures etc.
- Secret:
  - [Offline Virtual Machine Servicing Tool 2.1](#)
- Requirements
  - Windows Server Update Services (WSUS) 3.0 SP1 or WSUS 3.0 SP2
  - System Center Configuration Manager 2007 OR
  - System Center Configuration Manager 2007 SP1, SP2 OR
  - System Center Configuration Manager 2007 R2.

# Offline Virtual Machine Servicing Tool

- The tool uses “servicing jobs” to manage the update operations based on lists of existing virtual machines stored in VMM.
- For each virtual machine, the servicing job:
  - “Wakes” the virtual machine (deploys it to a host and starts it).
  - Triggers the appropriate software update cycle (Configuration Manager or WSUS).
  - Shuts down the updated virtual machine and returns it to the library.

# Summary

## Management system

- Use a Server Core installation for the management operating system.
- Keep the management operating system up to date with the latest security updates
- Use a separate network with a dedicated network adapter for the management operating system of the physical Hyper-V computer.
- Secure the storage devices where you keep virtual machine resource files.
- Harden the management operating system using the baseline security setting recommendations described in the [Windows Server 2008 Security Compliance Management Toolkit](#).
- Configure any real-time scanning antivirus software components installed on the management operating system to exclude Hyper-V resources.
- Do not use the management operating system to run applications.
- Do not grant virtual machine administrators permissions on the management operating system.
- Use the security level of your virtual machines to determine the security level of your management operating system.
- Use BitLocker Drive Encryption to protect resources.



# Summary

## Virtual machines

- Configure virtual machines to use fixed-sized virtual hard disks.
- Store virtual hard disks and snapshot files in a secure location.
- Decide how much memory to assign to a virtual machine.
- Impose limits on processor usage.
- Configure the virtual network adapters of each virtual machine to connect to the correct type of virtual network to isolate network traffic as required.
- Configure only required storage devices for a virtual machine.
- Harden the operating system running in each virtual machine according to the server role it performs using the baseline security setting recommendations described in the [Windows Server 2008 Security Compliance Management Toolkit](#).
- Configure antivirus, firewall, and intrusion detection software within virtual machines as appropriate based on server role.
- Ensure that virtual machines have all the latest security updates before they are turned on in a production environment.
- Ensure that your virtual machines have integration services installed.



# 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](http://www.microsoft.com/virtualization)
- Virtualization Solution Accelerators:
  - [www.microsoft.com/vsa](http://www.microsoft.com/vsa)
- MAP tool :
  - <http://microsoft.com/map>
- Hyper-V Green Tool :
  - <http://hyper-green.com>

# Next session at Xx.xx

- Sessionslokale 1
  - Session title
- Sessionslokale 2
  - Session title
- Sessionslokale 3
  - Session title
- Sessionslokale 4
  - Session title

Campus Days  
14.-16. januar 2010



# Questions

[jesper\\_krogh@dell.com](mailto:jesper_krogh@dell.com)

Campus Days  
14.-16. januar 2010



**THANK YOU!**