ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows Server 2008 & Vista SP1

What's New

Donald E. Hester

Updates

- For updates to this slide deck and other slide decks please see:
- http://www.learnsecurity.org/Shared%20Documents/Forms/AllItems.aspx

Overview

- Active Directory Security Changes
- Network Security Changes
- Data Protection
- Server Core
- Hyper-V
- Terminal Services Changes
- Server Manager

Ten Reasons to transition to Windows Server 2008 (Previously Code Name “Longhorn”)

- Improvements in Security
- Improvements in Networking
- Reliability and Performance
- Server Core
- Server Manager
- Active Directory Enhancements
- Network Access Protection (NAP)
- New Terminal Services Capabilities
- Windows Server Virtualization
- Internet Information Services 7.0

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Windows Server 2008

Web

Delivers rich web-based experiences efficiently and effectively

Virtualization

Reduces costs, increases hardware utilization, optimizes your infrastructure, and improves server availability

Security

Provides unprecedented levels of protection for your network, your data, and your business

Management and Reliability

- Most flexible and robust Windows Server operating system to date
- Provides the most versatile and reliable Windows platform for all of your workload and application requirements

Server Protection Features

Security

- Development Process
- Secure Startup and shield up at install
- Code integrity
- Windows service hardening
- Inbound and outbound firewall
- Restart Manager

Compliance

- Improved auditing
- Network Access Protection
- Event Forwarding
- Policy Based Networking
- Server and Domain Isolation
- Removable Device Installation Control
- Active Directory Rights Management Services

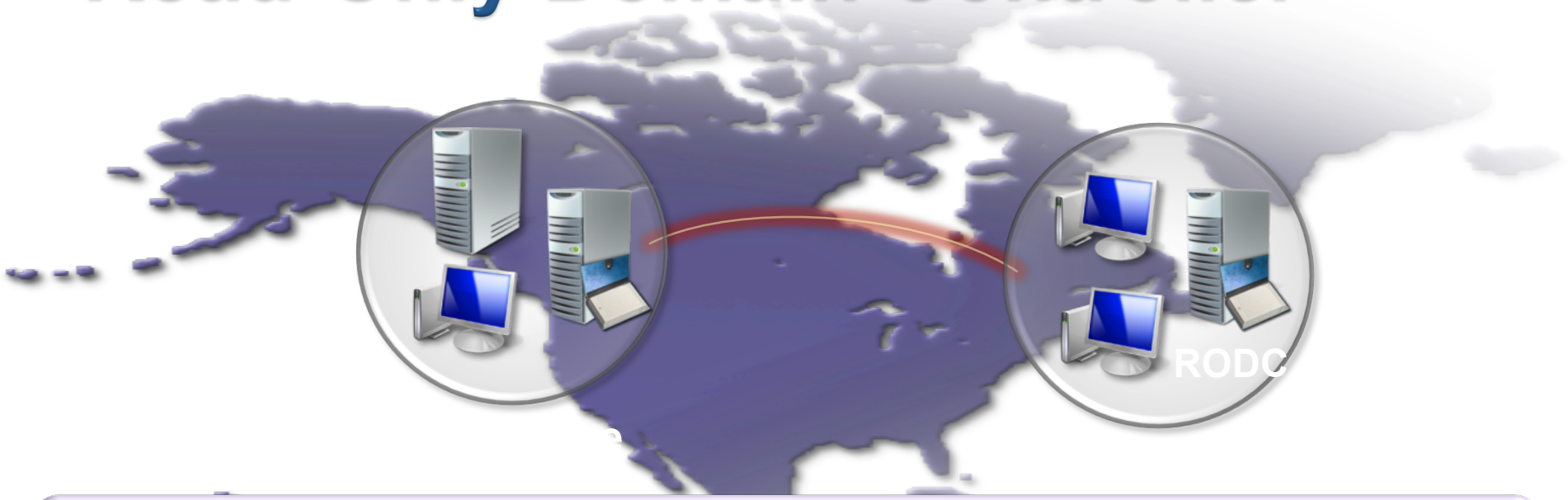
Active Directory Security Changes

- ADFS
- Read Only Domain Controller (RODC)
- Fine-grain Password Policies
- Active Directory Auditing

Active Directory Improvements

- Fine-grained password policies means you can give each group and/or person a different password policy
- New backup tool means bare-metal rebuilds of a dead DC is a snap
- AD snapshots gives ISVs the potential to build AD recovery tools, auditing and forensic analysis tools
- Restartable Directory Services

Read-Only Domain Controller



- Features
  - Read Only Active Directory Database
  - Only allowed user passwords are stored on RODC
  - Unidirectional Replication
  - Role Separation
- Benefits
  - Increases security for remote Domain Controllers where physical security cannot be guaranteed
- Support
  - ADFS,DNS, DHCP, FRS V1, DFSR (FRS V2), Group Policy, IAS/VPN, DFS, SMS, ADSI queries, MOM

"Restartable" Active Directory

- **Introduction:**
  - Restart Active Directory without rebooting
  - Can be done through command line and MMC
  - Can't boot the DC to stopped mode of Active Directory
  - No effect on non-related services while restarting Active Directory
  - Several ways to process login under stopped mode
- **Benefits:**
  - Reduces time for offline operations
  - Improves availability for other services on DC when Active Directory is stopped
  - Reduces overall DC servicing requirements with Server Core

Group Policy Preferences

- Group Policy Preferences lets you create a do-it-yourself group policy setting out of, well, just about anything… with a few mouse clicks
- Built into Windows Server 2008 GPMC
- Part of the Desktop Standard acquisition
- Remote Server Admin Tools (RSAT) delivered for Vista
- Can be utilized on Windows Server 2003, Windows XP, Windows Vista, as well as Windows Server 2008

Kerberos AES Support

Client	Server	KDC	
Down-level	Down-level	Server 2008	TGT may be encrypted with AES if necessary based on policy
Down-level	Vista	Server 2008	Service ticket encryption in AES
Vista	Vista	Server 2008	All messages in AES
Vista	Vista	Down-level	GSS encryption in AES
Vista	Down-level	Server 2008	AS-REQ/REP, TGS-REQ/REP in AES.
Down-level	Vista	Down-level	No AES
Vista	Down-level	Down-level	No AES
Down-level	Down-level	Down-level	No AES

For TGTs to be AES the domain must be Windows Server 2008 Functional Level.

Kerberos Resources

- Kerberos: http://www.microsoft.com/kerberos
- Windows Vista Authentication Features:

  http://technet2.microsoft.com/WindowsServer2008/en/library/f632de29-a36e-4d82-a169-2b180deb638b1033.mspx
- MSDN Authentication:

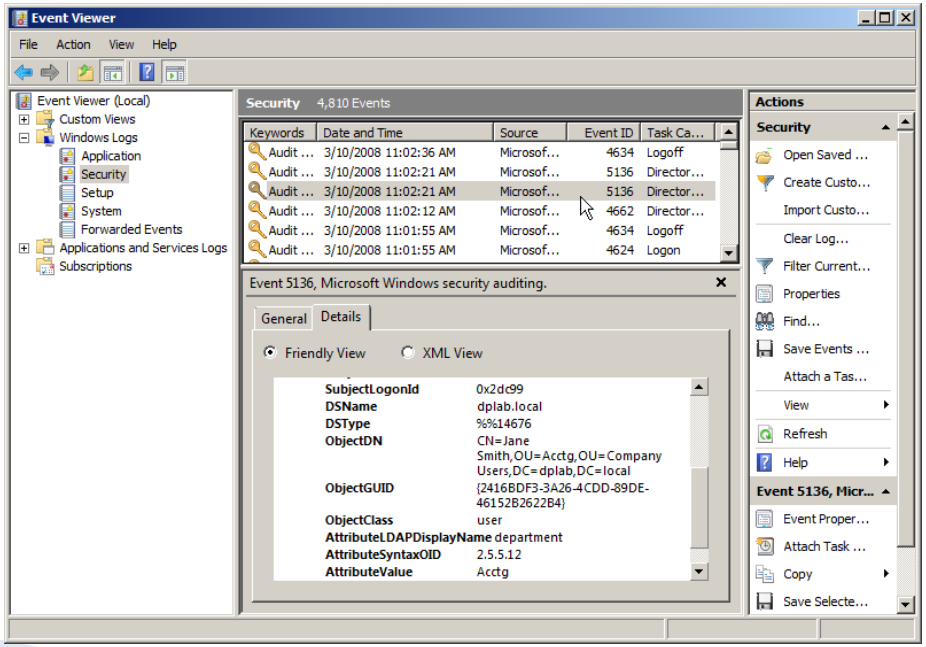
  http://msdn2.microsoft.com/en-us/library/aa374735.aspx

Audit Logs

- In Windows Server 2008 you can now set up AD DS auditing with a new audit subcategory to log old and new values when changes are made to objects and their attributes.
- In Windows 2000 Server and Windows Server 2003, there was one audit policy, **Audit directory service access**, that controlled whether auditing for directory service events was enabled or disabled. In Windows Server 2008, this policy is divided into four subcategories:
  - **Directory Service Access**
  - **Directory Service Changes**
  - **Directory Service Replication**
  - **Detailed Directory Service Replication**

Directory Services Auditing

- A new event (5136) is generated when the action is performed on the object
- This event lists the previous value of the changed attribute, and the new value



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Fine-Grained Passwords

- Before Windows Server 2008
  - One password policy per domain
- In Windows Server 2008
  - Still set only one password policy at domain level
  - Additional settings for users needing different policy available in ADSIEdit
  - These settings are called Password Settings objects (PSOs)
- Does NOT apply to:
  - Computer objects
  - Organizational Units
- Requires **Windows Server 2008 Domain Functional Mode**

Fine-Grained Passwords

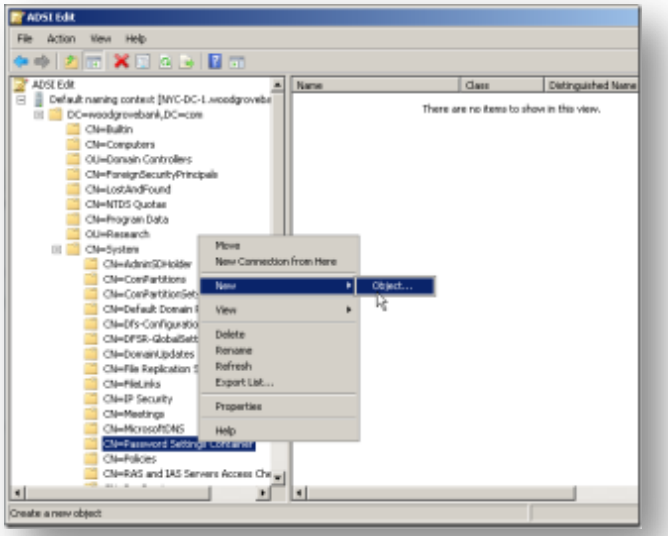
- PSO settings include attributes for the following password and account settings:
  - Enforce password history
  - Maximum password age
  - Minimum password age
  - Minimum password length
  - Passwords must meet complexity requirements
  - Store passwords using reversible encryption
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout after

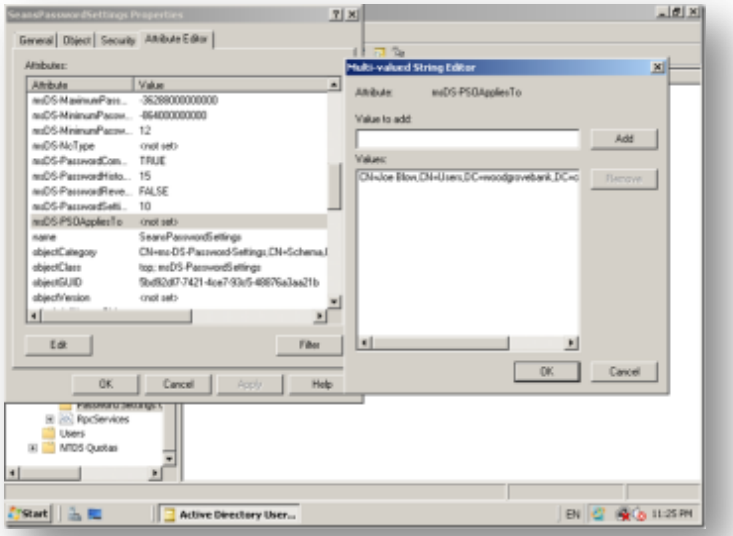
Fine-Grained Passwords

- A user or group object can have multiple PSOs linked to it, either because of membership in multiple groups that each have different PSOs applied to them or because multiple PSOs are applied to the object directly.
- However, only one PSO can be applied as the effective password policy.
- Only the settings from that PSO can affect the user or group.
- The settings from other PSOs that are linked to the user or group cannot be merged in any way.

Fine-Grained Passwords

- To create and manage use one of the following tools:
  - ADSIEdit
  - LDIF





ISACA
Serving IT Governance Professionals
San Francisco Chapter

Fine-Grained Passwords

- LDIF file sample:

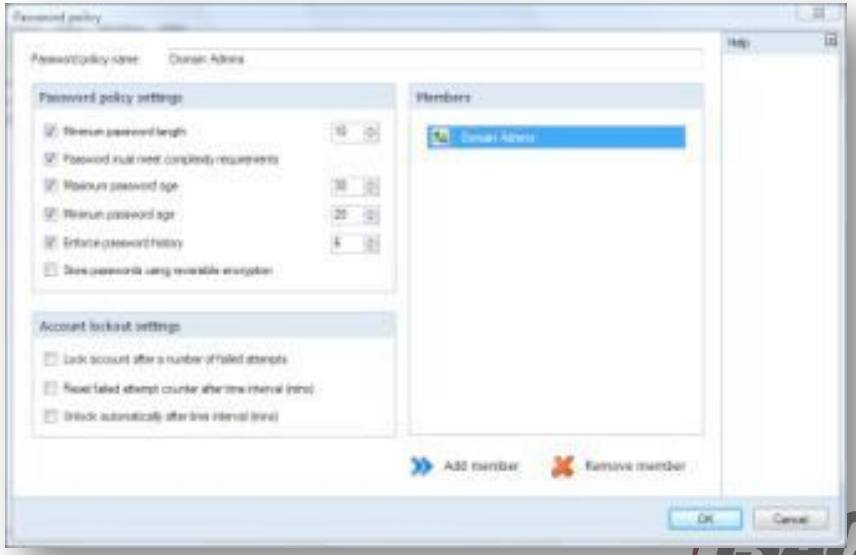
```
dn: CN=PSO1, CN=Password Settings
   Container,CN=System,DC=contoso,DC=com
changetype: add
objectClass: msDS-PasswordSettings
msDS-MaximumPasswordAge:-1728000000000
msDS-MinimumPasswordAge:-864000000000
msDS-MinimumPasswordLength:8
msDS-PasswordHistoryLength:24
msDS-PasswordComplexityEnabled:TRUE
msDS-PasswordReversibleEncryptionEnabled:FALSE
msDS-LockoutObservationWindow:-18000000000
msDS-LockoutDuration:-18000000000
msDS-LockoutThreshold:0
msDS-PasswordSettingsPrecedence:20
msDS-PSOAppliesTo:CN=user1,CN=Users,DC=contoso,DC=com
```

- To import:

```
Ldifde -i -f c:\pso.ldf
```

Fine-Grained Passwords

- Some 3rd-Party freeware tools:
  - Fine Grain Password Policy Tool
  - http://blogs.chrisse.se/blogs/chrisse/archive/2007/07/14/fine-grain-password-policy-tool-beta-1-is-ready.aspx
  - Fine-Grained Password Policies pack for PowerGUI
  - http://dmitrysotnikov.wordpress.com/2007/06/19/free-ui-console-for-fine-grained-password-policies
  - Specops Password Policy Basic
  - http://www.specopssoft.com/wiki/index.php/SpecopsPasswordPolicybasic/SpecopsPasswordPolicybasic



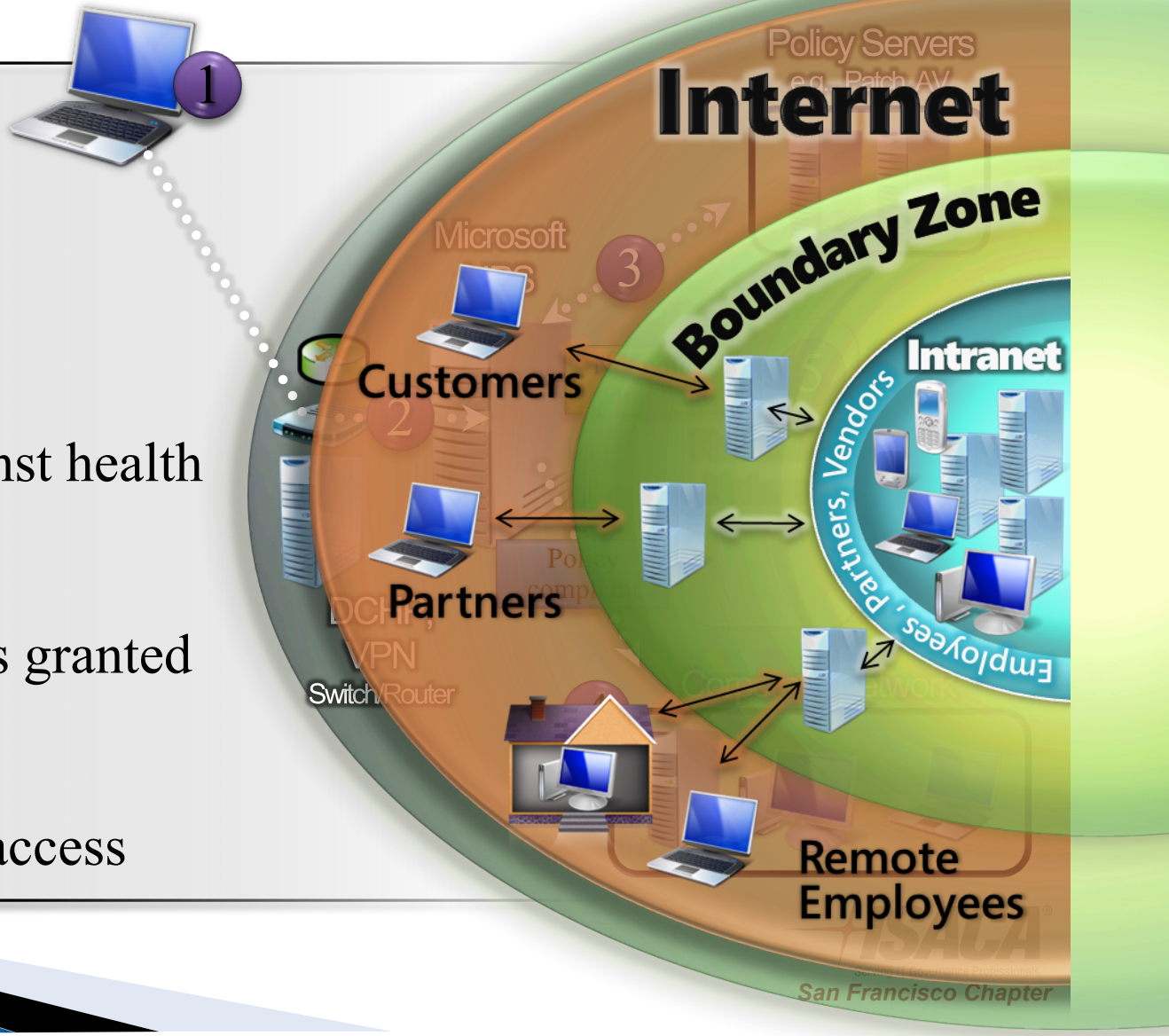
Network Security Changes

- Network Access Protection (NAP)
- TCP/IP changes
- Secure Socket Tunneling Protocol (SSTP)
- Advanced Firewall

Network Access Protection

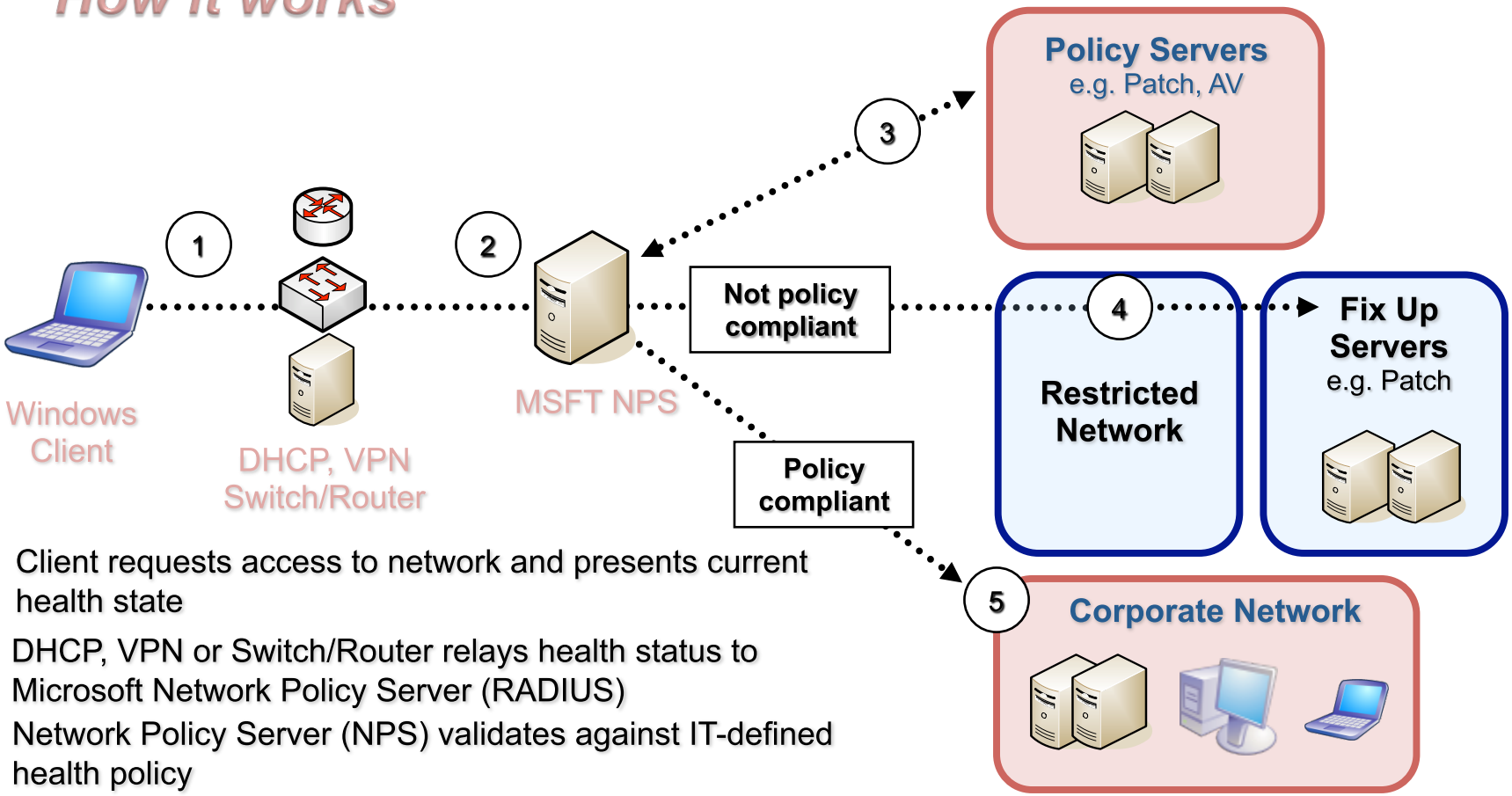
How it works

1. Access requested
2. Health state sent to NPS (RADIUS)
3. NPS validates against health policy
4. If compliant, access granted
5. If not compliant, restricted network access and remediation



Network Access Protection

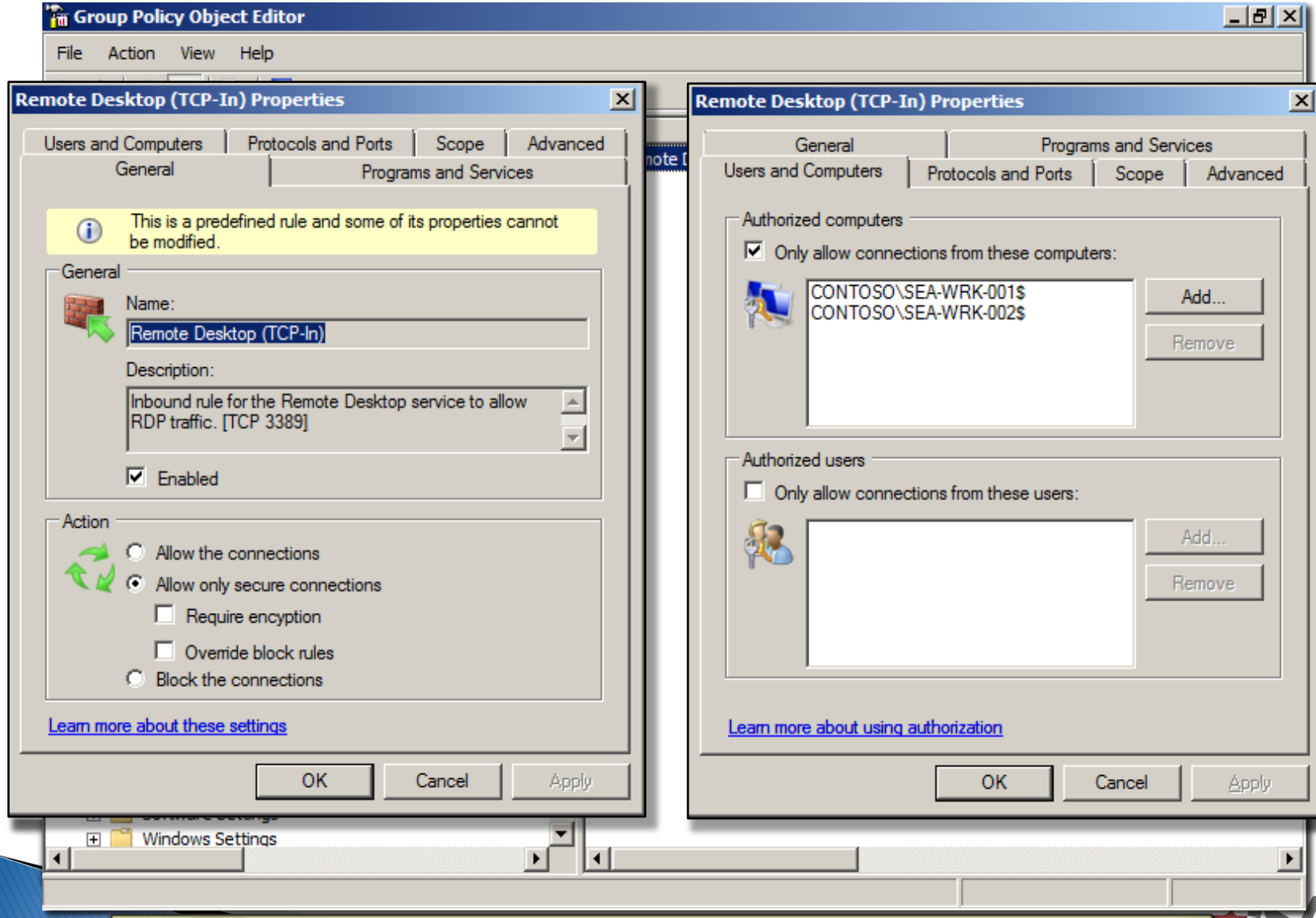
How it works



1. Client requests access to network and presents current health state
2. DHCP, VPN or Switch/Router relays health status to Microsoft Network Policy Server (RADIUS)
3. Network Policy Server (NPS) validates against IT-defined health policy
4. If not policy compliant, client is put in a restricted VLAN and given access to resources to bring it into compliance, (Repeat 1 - 4)
5. If policy compliant, client is granted full access to corporate network

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows Firewall w/ Advanced Security



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Data Protection

- BitLocker
- ADRMS

Server Core

- Only a subset of the executable files and DLLs installed
- No GUI interface installed, no .NET, no PowerShell (for now)
- Nine available Server Roles
- Can be managed with remote tools

Server Core Roles

- Active Directory Domain Services Role
- Active Lightweight Directory Services Role
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS) Server Role
- File Services Role
- Hyper-V Role
- Print Services Role
- Streaming Media Services Role
- Web Services (IIS) Role

Server Core Supported Features

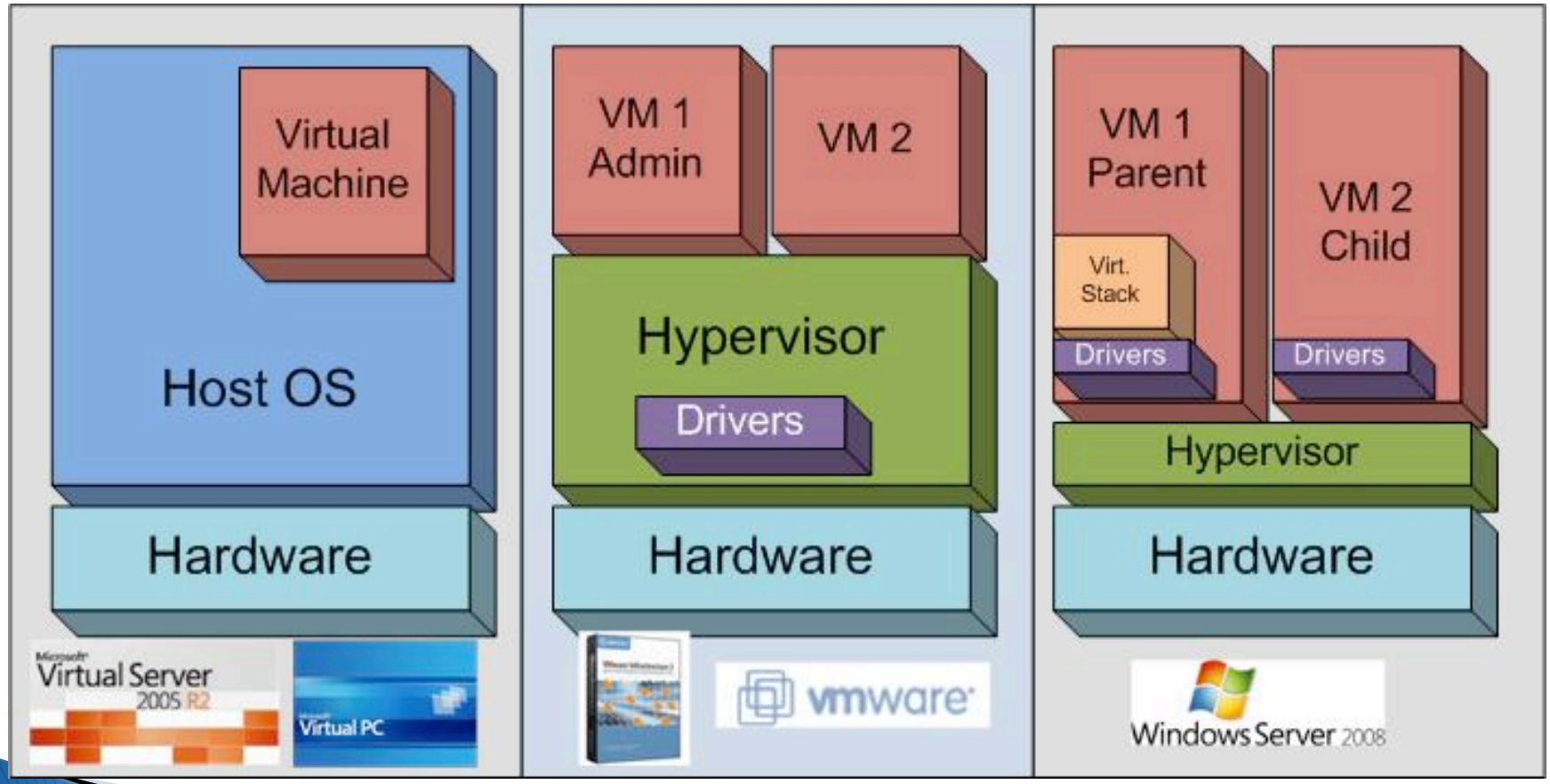
- Backup
- BitLocker
- Failover Clustering
- Multipath I/O
- Network Time Protocol (NTP)
- Removable Storage Management
- Simple Network management protocol (SNMP)
- Subsystem for Unix-based applications
- Telnet Client
- Windows Internet Naming Service (WINS)

Hyper-V

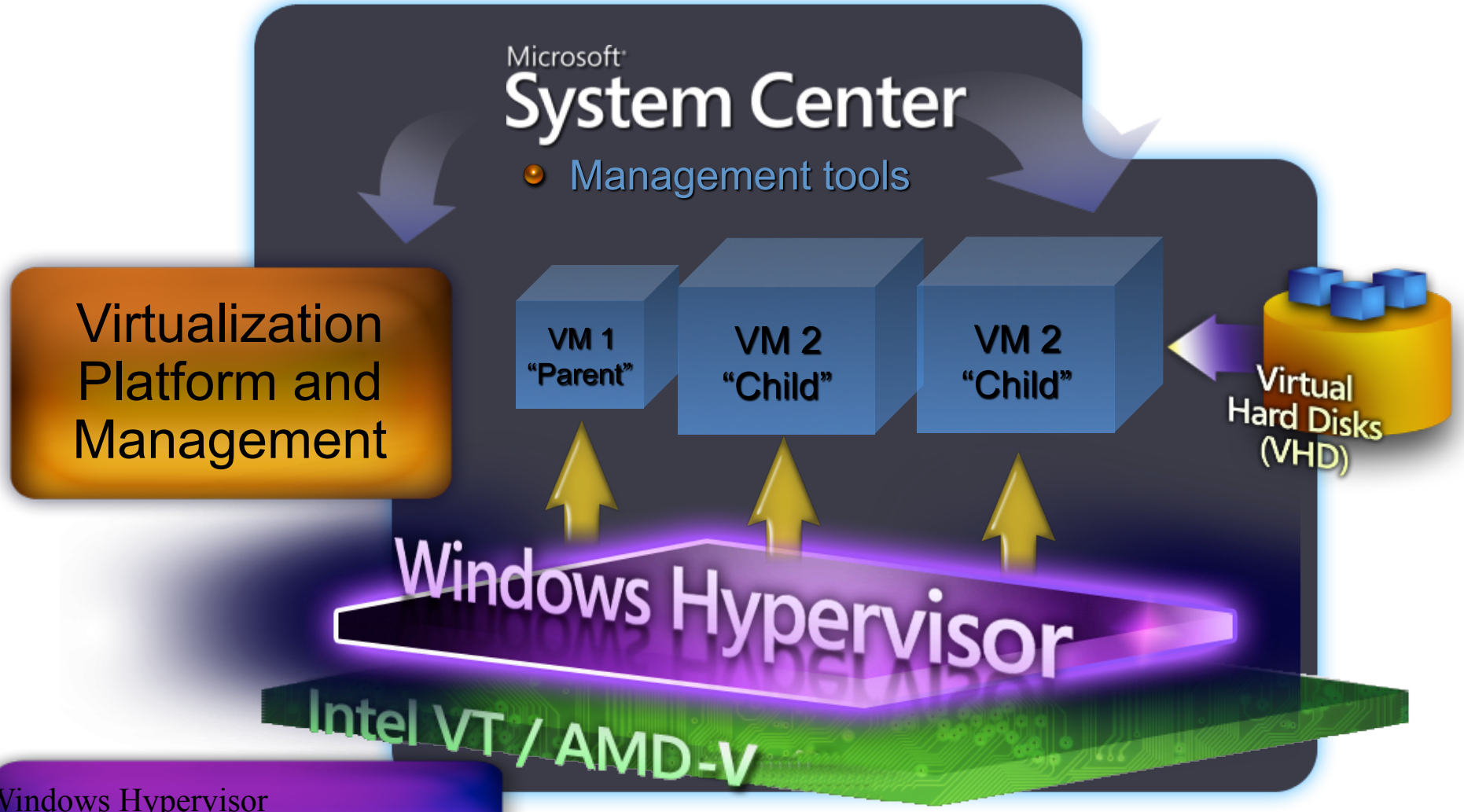
Features

- 64 and 32 bit support, 4 core support
- New better I/O support with synthetic device drives instead of emulated drivers
- Because there is no emulation overhead goes down and I/O response goes up
- Enlightened OS
- OS is aware it is running virtualized
- Vista and Server 2008 support, patch for server 2003 soon
- 3rd party Zensource will have an upgrade for various flavors of Linux so that they can be enlightened

Server/Machine Virtualization



Hyper-V Overview



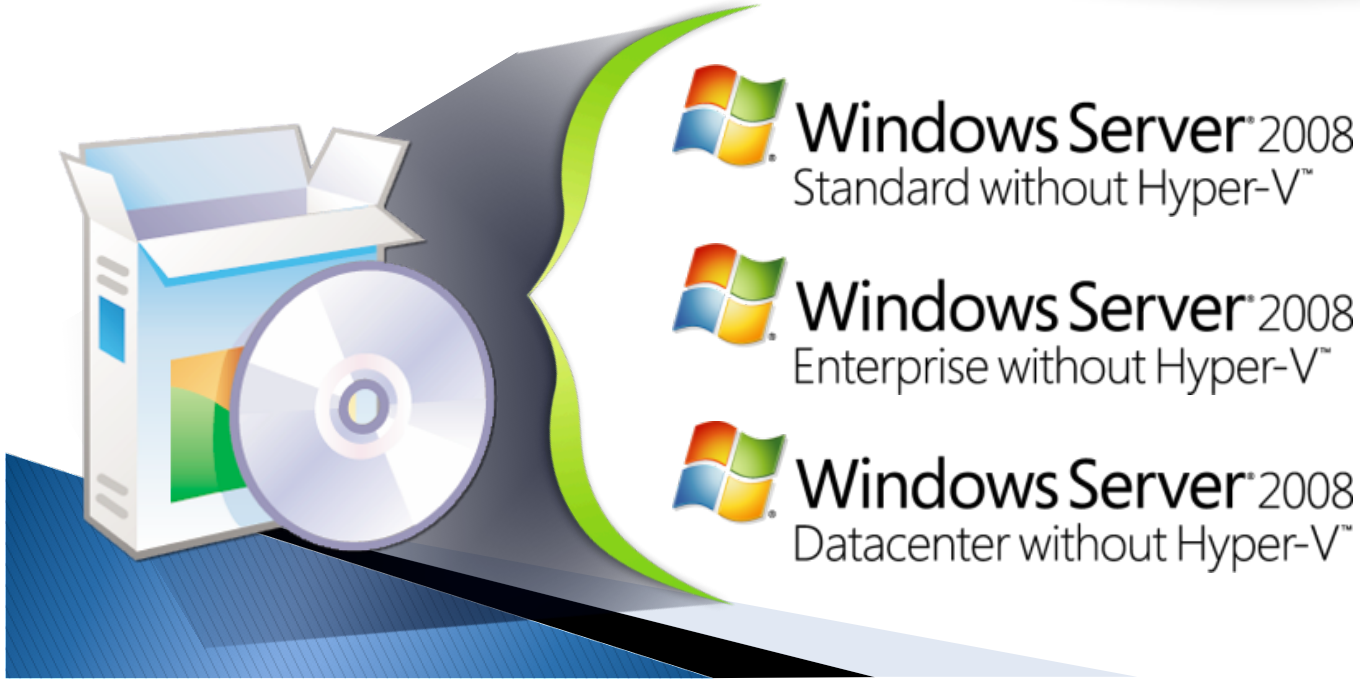
Windows Hypervisor

- Powerful virtualization built into the Windows platform

ISACA
Serving IT Governance Professionals
San Francisco Chapter

New SKUs and Product

Microsoft® Hyper-V™ Server



Windows Server® 2008 Standard without Hyper-V™

Windows Server® 2008 Enterprise without Hyper-V™

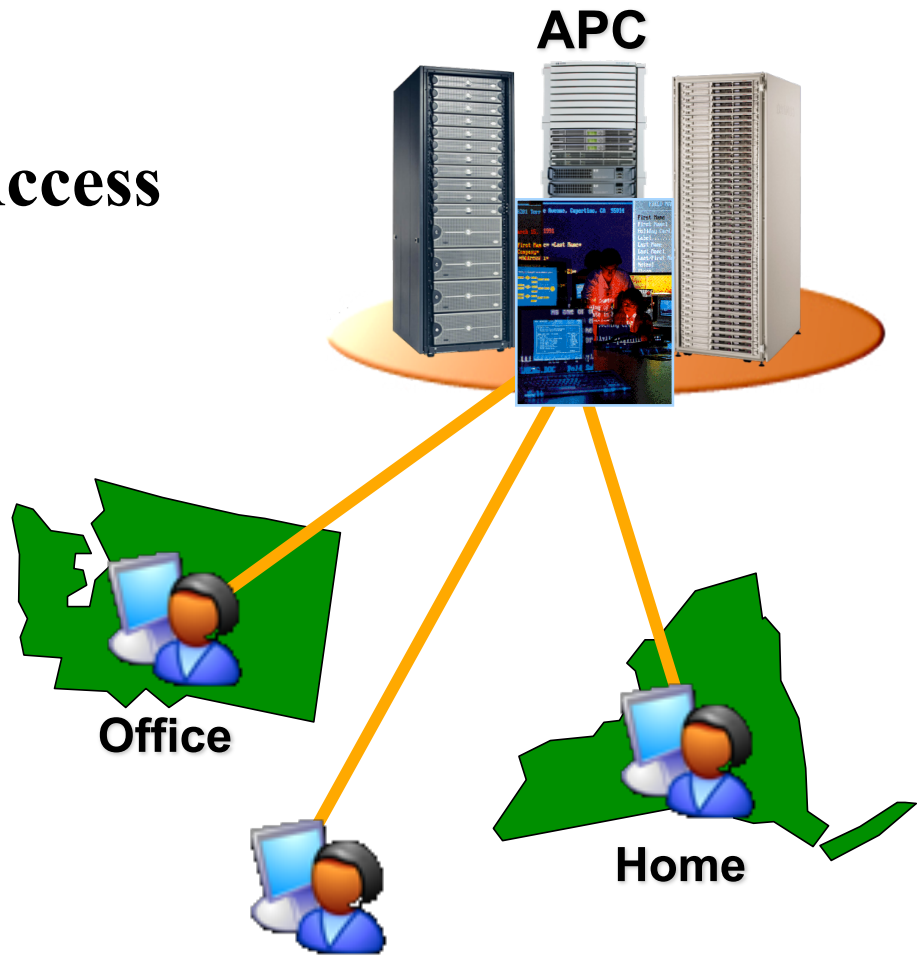
Windows Server® 2008 Datacenter without Hyper-V™

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Terminal Services Changes

Terminal Services Enhancements

- **Centralized Application Access**
  - App Deployment ("app virtualization")
  - Branch Office
  - Secure Anywhere Access
- **New features**
  - TS Gateway
  - TS Remote Programs
  - SSO for managed clients



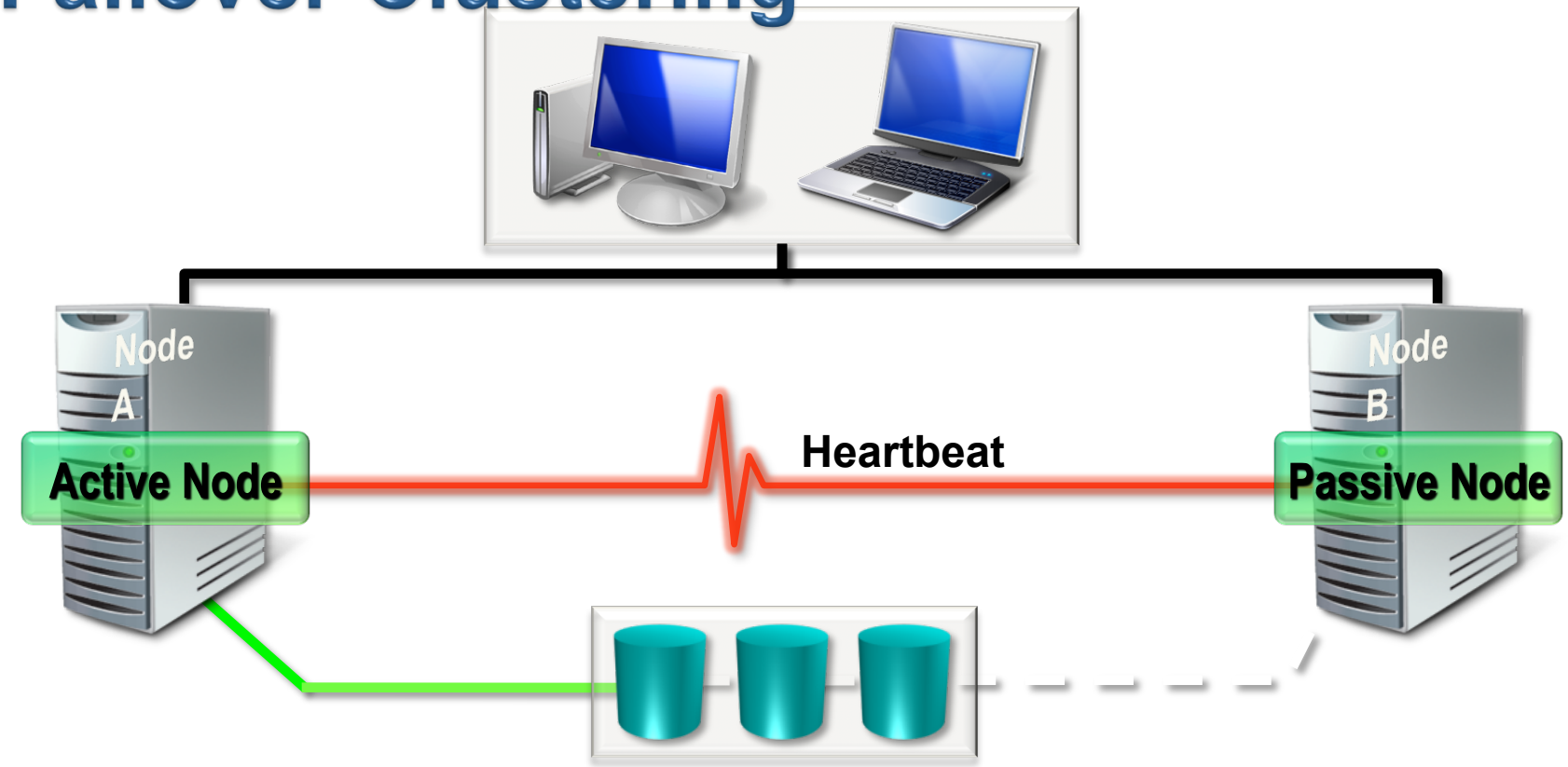
ISACA
Serving IT Governance Professionals
San Francisco Chapter

Terminal Services Gateway

- **Security (compared to VPN)**
  - Authentication with passwords, smartcards
  - Uses industry standard encryption and firewall traversal (SSL, HTTPS)
  - RDP traffic still encrypted end-to-end – client to terminal server
  - Client machine health can be validated (using NAP)
  - SSL termination devices can terminate SSL traffic on separate device. (for intrusion detection or filtering in DMZ)
  - User can access applications and desktops via Web Browser
  - Friendly with home machines
  - Crosses firewalls and NATs (w/ HTTPS:443)
  - Granular access control at the perimeter
    - Connection Authorization Policy (CAP)
    - Resource Authorization Policy (RAP)

Server Manager

Failover Clustering



- New Validation Wizard
- Support for GUID partition table (GPT) disks in cluster storage
- Improved cluster setup and migration
- Improvements to stability and security – no single point of failure
- IPv6 support
- Multi-site Clustering

Questions

Donald E. Hester

Maze & Associates
www.MazeAssociates.com
Blog
www.LearnSecurity.org
LinkedIn
http://www.linkedin.com/in/donaldehester