

T1 - Windows 7, Vista and Server 2008 R2

Donald E. Hester



September 21, 2009 – September 23, 2009

Windows Server 2008 & Vista SP1

What's New
Donald E. Hester



**MAZE &
ASSOCIATES**

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

The image shows a silver and black humanoid robot with a server rack for a torso, standing in a server room. Text overlays include:

- Manageability Updates**
It manages, implements, updates and never takes a sick day.
- Meet IT 24-7**
Watch more videos of the ultimate server unleashed.
- Web**
Serving up better, faster, more secure experiences.

At the bottom left, there is a small text box: "by Box" and "It's not just enough robots? Thought so."

- For updates to this slide deck and other slide decks please see:
- <http://www.learnsecurity.org/>

Overview

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



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



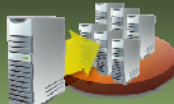
Windows Server 2008

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



Windows Vista/Server 2008 Security

INTEGRITY PROTECTION

Windows Integrity Controls

- One goal was CC (Common Criteria) compliance (TCSEC Level B)
- MIC (Mandatory Integrity Control) later named WIC (Windows Integrity Control)
- Has been available for decades but only in military computers
- That means there may be files that not even the administrator can delete

MIC

- *Mandatory Integrity Control (MIC)*, a model in which data can be configured to prevent lower-integrity applications from accessing it.
- The primary integrity levels are Low, Medium, High, and System.
- Processes are assigned an integrity level in their access token.
- Seurable objects such as files and registry keys have a new mandatory access control entry (ACE) in the System Access Control List (ACL).

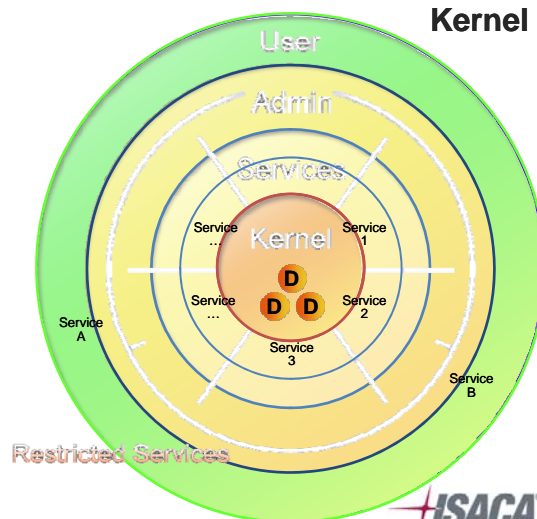


Integrity Levels

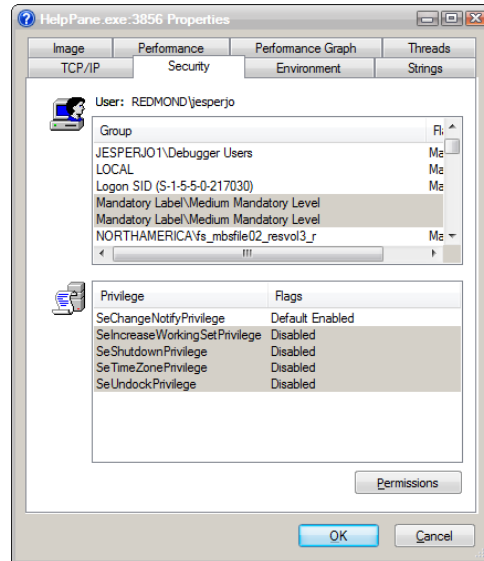
Defense-in-Depth: Factoring and Profiling of Windows Kernel

- Reduce size of high risk layers
- Segment the services
- Increase number of layers

- Kernel Drivers
- User-mode Drivers



Integrity Levels in Token



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

CONVERGENCE

ISACA
San Francisco Chapter

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

<http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>
<http://support.microsoft.com/Default.aspx?kbid=943729>

ISACA
San Francisco Chapter

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>



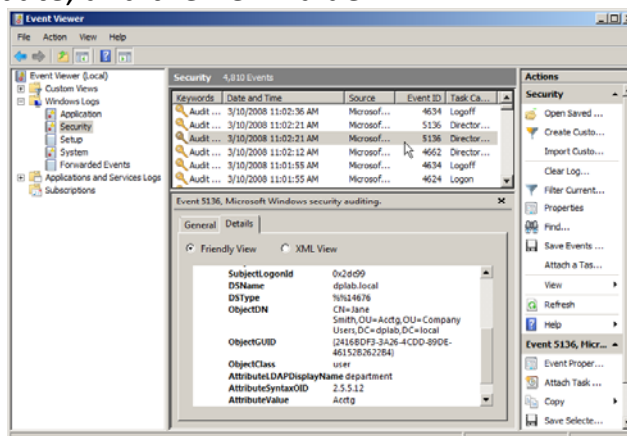
Audit Logs

- 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



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

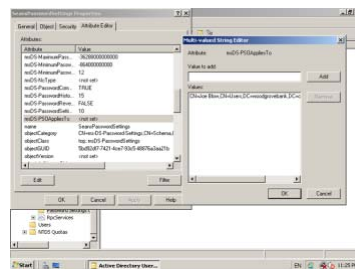
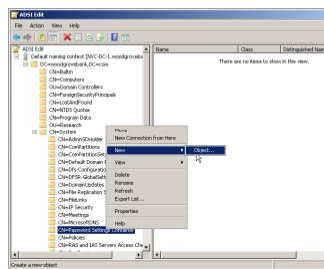
- PSO settings include attributes for the following password and account settings:
 - Enforce password history
 - Maximum password age
 - Minimum password age
 - Minimum password length
 - Passwords must meet complexity requirements
 - Store passwords using reversible encryption
 - Account lockout duration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



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
```

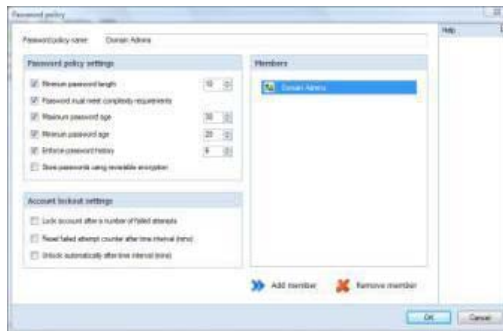
- To import:

```
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://dmitryshotnikov.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



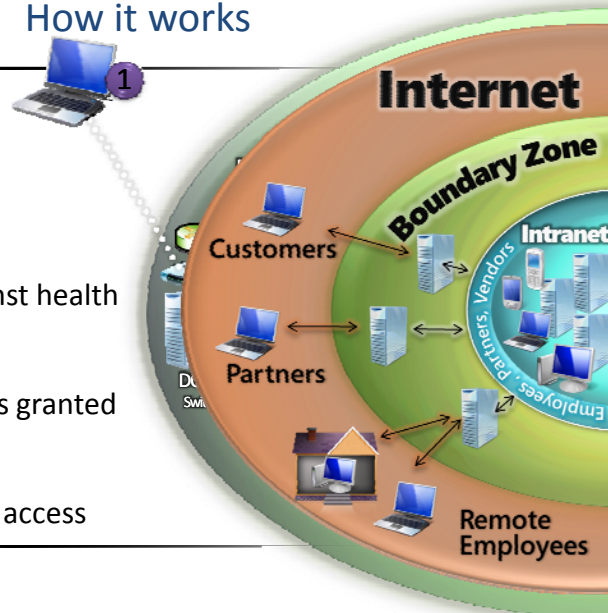
CONVERGENCE

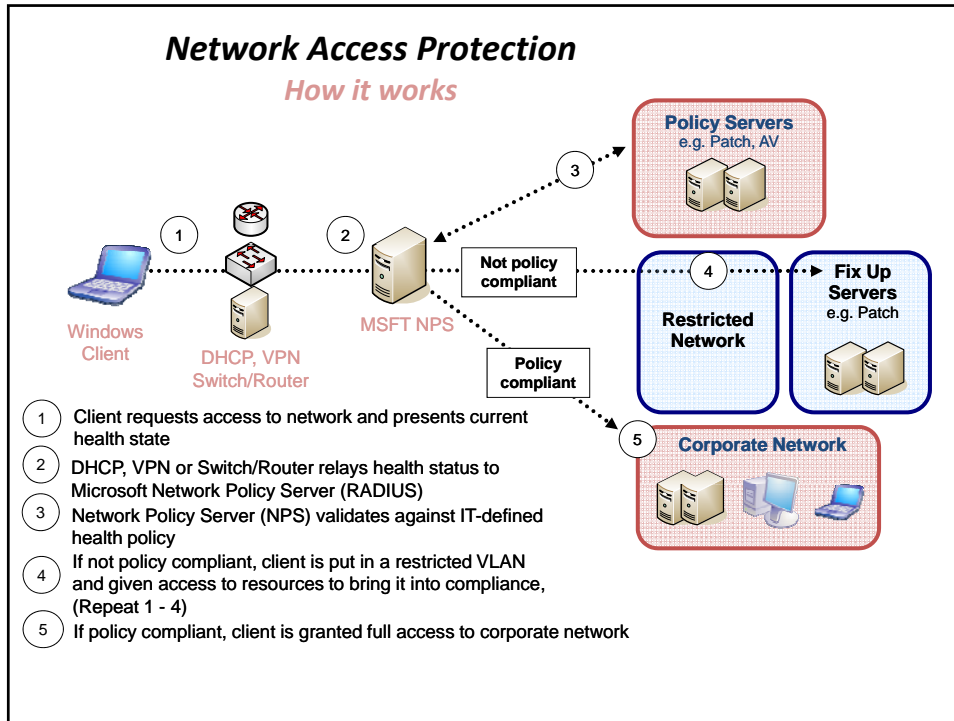
ISACA
Setting IT Governance Professionals
San Francisco Chapter

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
- 4 Modes
 - 802.1x NAP enforcement
 - Enforcement on the switch/router level
 - VPN NAP enforcement
 - Enforcement for remote connections
 - Enforcement by packet filtering
 - DHCP NAP enforcement
 - Only applied when a client lease is obtained or renewed
 - Avoid configuring long leases
 - Can be circumvented by static IP assignment
 - Terminal Services Gateway NAP enforcement
 - RDP (Remote Desktop Protocol) session will not be

NG TCP/IP

Next Generation TCP/IP in Vista and Server 2008 “Longhorn”

- A new, fully re-worked replacement of the old TCP/IP stack
- Dual-stack IPv6 implementation, with now obligatory IPSec
 - IPv6 is more secure than IPv4 by design, esp.:
 - Privacy, tracking, network port scanning, confidentiality and integrity
- Other network-level security enhancements for both IPv4 and IPv6
 - Strong Host model
 - Windows Filtering Platform
 - Improved stack-level resistance to **all known** TCP/IP-based denial of service and other types of network attacks
 - Routing Compartments
 - Auto-configuration and no-restart reconfiguration
- Read:
www.microsoft.com/technet/community/columns/cableguy/cg0905.msp



TCP/IP protection

- Enhancements:
 - Smart TCP port allocation
 - SYN attack protection is enabled by default
 - New SYN attack notification IP Helper APIs
 - Winsock self-healing

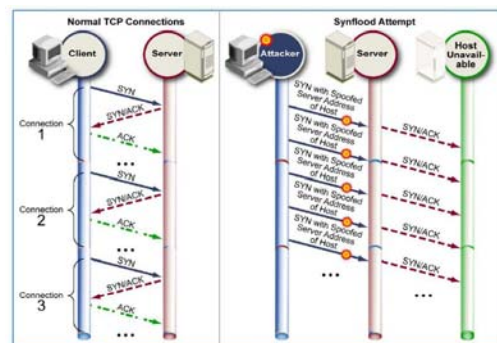
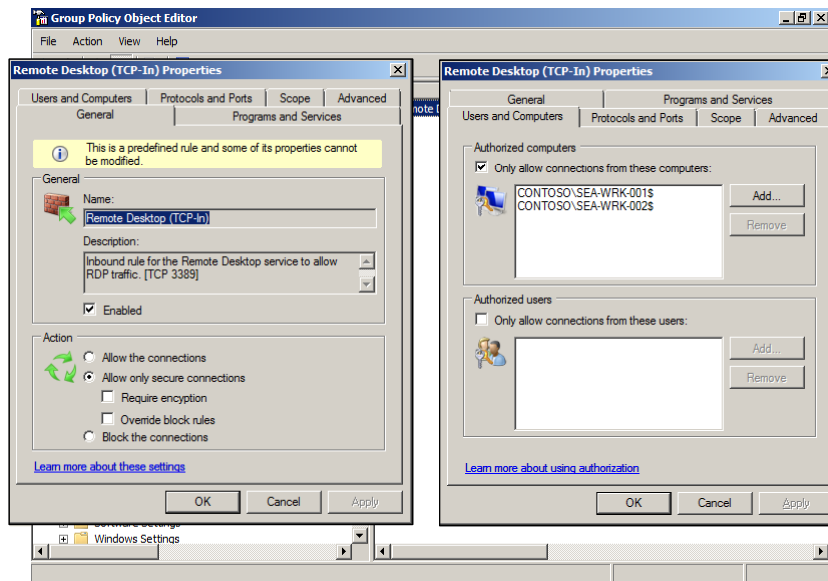
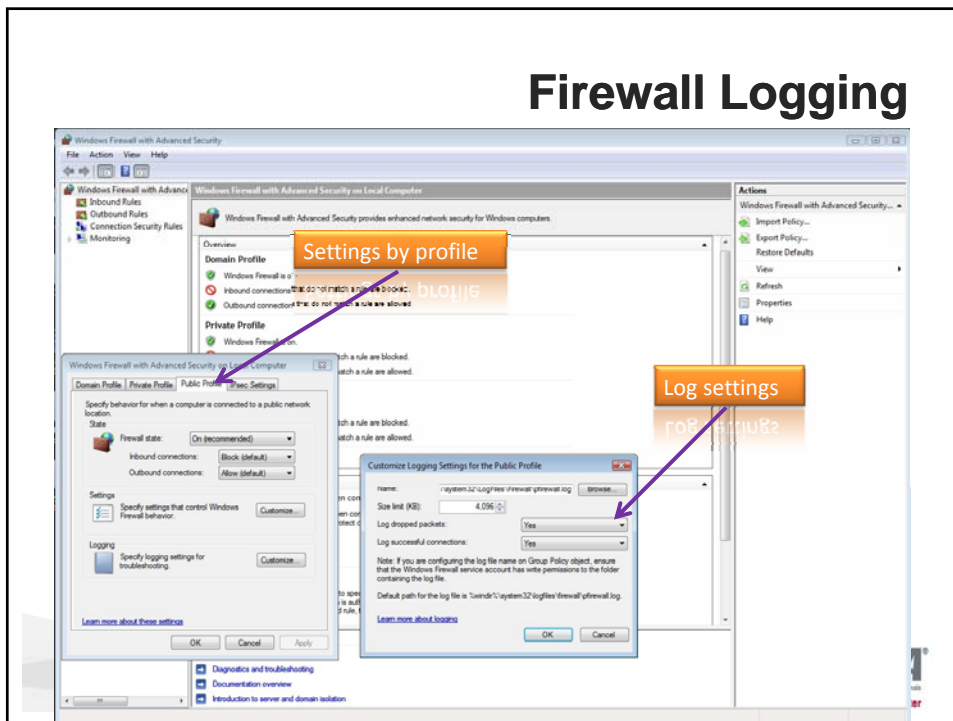


Figure 4-4. Synflood Attack

Windows Firewall w/ Advanced Security



Firewall Logging



Inbound & Outbound Rules

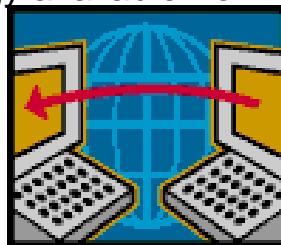
The screenshot displays the Windows Firewall with Advanced Security console. The left pane shows the tree view with 'Inbound Rules' selected. The main pane shows a list of rules. The 'Microsoft Office Groove' rule is highlighted in blue. Callout boxes are present:

- 'Specific Rules' points to the 'Microsoft Office Groove' rule.
- 'MS Office 2007 added needed rules' points to the 'Microsoft Office Groove' rule.
- 'Inbound & Outbound Rules' points to the 'Inbound Rules' group in the left pane.

Name	Group	Profile	Enabled	Direction	Action	Local Address
AirSync Protocol HTTP Port	Any	Any	Yes	Allow	No	Any
AirSync Protocol HTTP Port	Any	Any	Yes	Allow	No	Any
AirSync Protocol HTTP Port	Any	Any	Yes	Allow	No	Any
hpsync.dll.exe	Private	Private	No	Allow	No	C:\Users\...
hpsync.dll.exe	Private	Private	No	Allow	No	C:\Users\...
Internet Explorer	Domain	Domain	Yes	Allow	No	C:\Program...
Internet Explorer	Domain	Domain	Yes	Allow	No	C:\Program...
Legacy Status Port	Any	Any	Yes	Allow	No	Any
Legacy Status Port	Any	Any	Yes	Allow	No	Any
Legacy Status Port	Any	Any	Yes	Allow	No	Any
Legacy Sync Channel Port	Any	Any	Yes	Allow	No	Any
Legacy Sync Channel Port	Any	Any	Yes	Allow	No	Any
Legacy Sync Channel Port	Any	Any	Yes	Allow	No	Any
Microsoft Office Groove	Private	Private	Yes	Allow	No	C:\Program...
Microsoft Office Groove	Domain	Domain	Yes	Allow	No	C:\Program...
Microsoft Office Groove	Domain	Domain	Yes	Allow	No	C:\Program...
Microsoft Office Groove	Private	Private	Yes	Allow	No	C:\Program...
Microsoft Office OneNote	Domain	Domain	Yes	Allow	No	C:\Program...
Microsoft Office OneNote	Private	Private	Yes	Allow	No	C:\Program...
Microsoft Office OneNote	Domain	Domain	Yes	Allow	No	C:\Program...
Microsoft Office OneNote	Private	Private	Yes	Allow	No	C:\Program...
Microsoft Office Outlook	Domain	Domain	Yes	Allow	No	C:\Program...
Microsoft Office Outlook	Domain	Domain	Yes	Allow	No	C:\Program...
Sync Services Port	Any	Any	Yes	Allow	No	Any
Sync Services Port	Any	Any	Yes	Allow	No	Any
Windows Live Messenger 8.1 (Phone)	Any	Any	Yes	Allow	No	%System... Any
Windows Live Messenger 8.1 (Phone)	Any	Any	Yes	Allow	No	%System... Any
Windows Mobile-based device connecti...	Any	Any	Yes	Allow	No	%System... Any
Windows Mobile-based device connecti...	Any	Any	Yes	Allow	No	%System... Any

SSL VPN (VPN over SSL)

- Secure Socket Tunneling Protocol (SSTP)
- More accessibility
- Firewall port friendly
- Old technology available from 3rd parties



Data Protection

- BitLocker
- ADRMS



CONVERGENCE

ISACA
Serving IT Governance Professionals
San Francisco Chapter



Windows Vista / Server 2008 Security

BITLOCKER™ DRIVE ENCRYPTION

BitLocker™

- Over 600,000 laptops are stolen a year
- BitLocker ensures that data stored on a computer running Windows Vista / Server 2008 remains encrypted even if the computer is tampered with when the operating system is not running
- BitLocker is designed to offer a seamless user experience



BitLocker



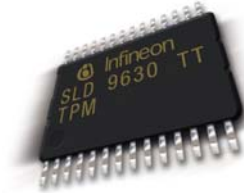
- Preventing off-line modifications
- Entire drive encryption
- TPM (Trusted Platform Module) to store key
- Can use additional protection factors such as a USB dongle, PIN or password
- Data recovery strategy must be planned carefully!
- Single digit performance hit (overhead)



Trusted Platform Module

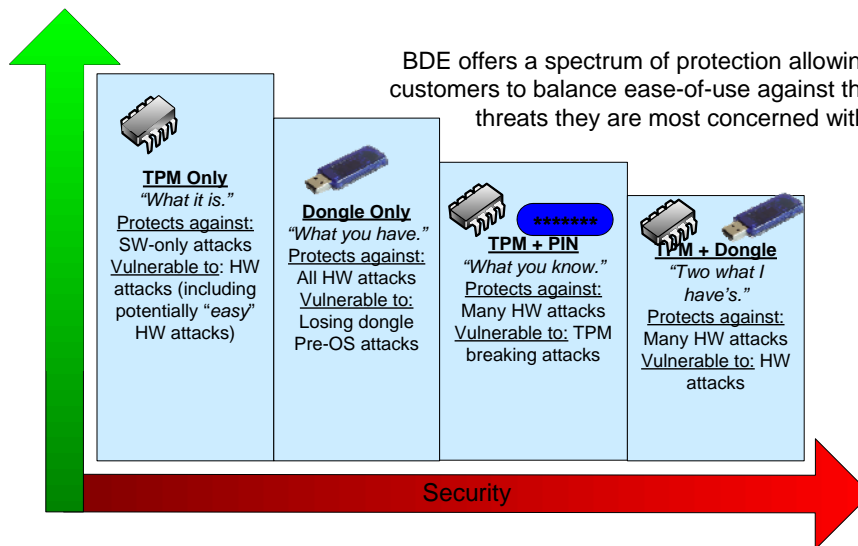
TPM Chip Version 1.2

- Hardware present in the computer, usually a chip on the motherboard
- Securely stores credentials, such as a private key of a machine certificate and is crypto-enabled
 - Effectively, the essence of a smart smartcard
- TPM can be used to request encryption and digital signing of code and files and for mutual authentication of devices
- See www.trustedcomputinggroup.org



Spectrum Of Protection

BDE offers a spectrum of protection allowing customers to balance ease-of-use against the threats they are most concerned with.



Deployment Options

- Dongle Only: If you don't have TPM you can deploy BitLocker with the key on a USB device
- TPM only: You can use BitLocker with TPM
- TPM & PIN: you can use a PIN number in addition for added security
- TPM & Dongle: For the greatest protection



Hardware and Software requirements

- A computer that meets the minimum requirements for Windows Vista / Server 2008.
- A TPM microchip, version 1.2, turned on.
- A Trusted Computing Group (TCG)-compliant BIOS
- Two NTFS drive partitions, one for the system volume and one for the operating system volume. The system volume partition must be at least 1.5 gigabytes (GB) and set as the active partition
- A BIOS setting to start up first from the hard drive, not the USB or CD drives.



Partitioning a Hard Disk for BitLocker

- 1st partition, system volume, (label “S” for example) contains unencrypted boot information
- 2nd partition, operating system volume (label “C” for example) contains encrypted user data and operating system



BitLocker Disk Layout and Key Storage



Recovery Password

- During the setup process you can save the recovery password in the following ways.
 - Save the password on a USB drive
 - Save the password in a folder
 - Print the password
 - In Active Directory
- The password is so important that it is recommended that you make additional copies of the password stored in safe places to assure you access to your data



Tampering & Recovery

- You BitLocker will enter recovery mode, and you will need a recovery password to regain access to the data if,
 - The TPM is missing or changed
 - Or if the startup information has changed
- Recovery happens so early in the startup process, the accessibility features of Windows are not available.
- BitLocker Drive Encryption Recovery Console



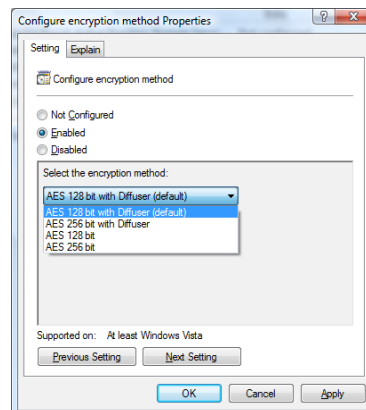
BitLocker & TPM: GPO

- You can configure these settings in the following location within the Group Policy Object Editor:
 - **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption**
- You can configure these settings in the following location in the Group Policy Object Editor:
 - **Computer Configuration\Administrative Templates\System\Trusted Platform Module Services**



Performance & Security

- 4 levels of AES encryption
- 128 & 256 bit
- the diffuser is a new unproven algorithm
- diffuser runs in about 10 clock cycles/byte
- Combination with AES-CBC for performance & security



Server Core



CONVERGENCE

ISACA
San Francisco Chapter



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

CONVERGENCE

ISACA
San Francisco Chapter

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



CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

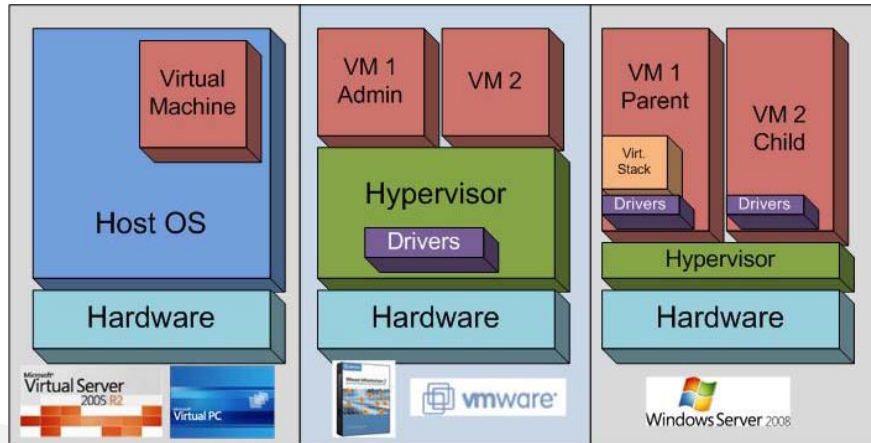
Features

- 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 SP 1 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

CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

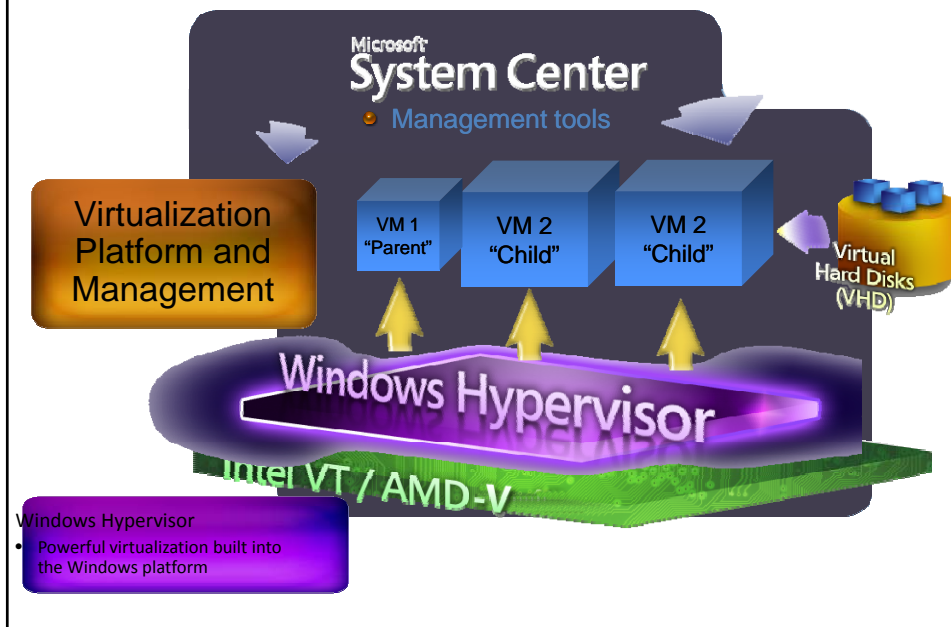
Server/Machine Virtualization



CONVERGENCE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Hyper-V Overview



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

Terminal Services Changes



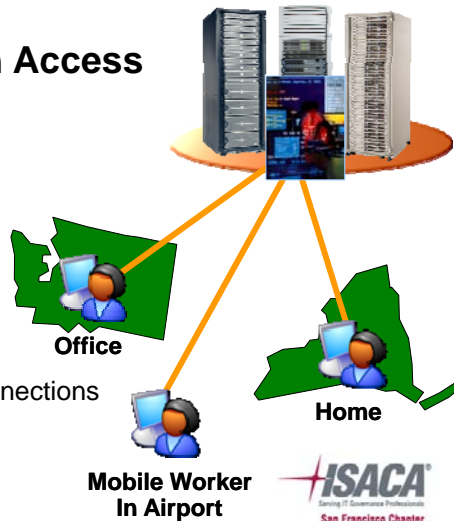
Terminal Services Enhancements

- **Centralized Application Access**

- App Deployment (“app virtualization”)
- Branch Office
- Secure Anywhere Access

- **New features**

- TS Gateway
- TS Remote Programs
- SSO for managed clients
- NAP enforcement for client connections



CONVERGEMERGE

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)

CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

High Availability

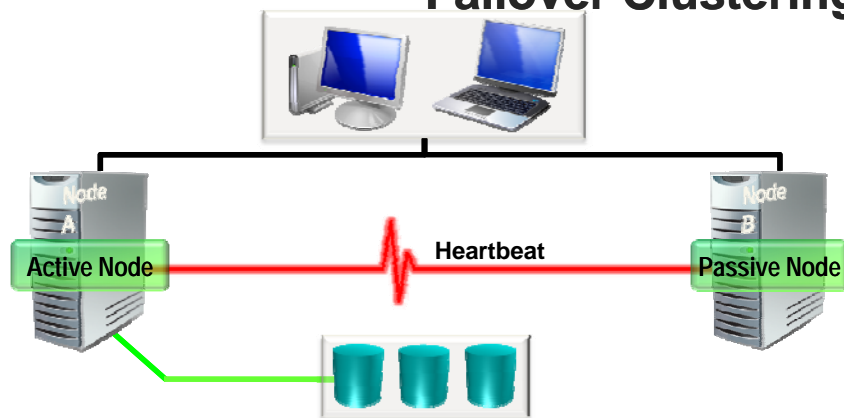
- Failover Clusters (formerly known as Server Clusters)
- Still have NLB (Network Load Balancing)



CONVERGENCE

ISACA
Setting IT Governance Professionals
San Francisco Chapter

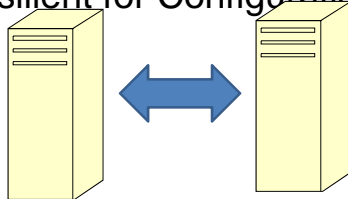
Failover Clustering



- 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

Cluster Security Improvements

- No More Cluster Service User Account
- The Cluster runs with Local System Account with low privileges
- No Account Password Management
- More Resilient for Configuration Issues

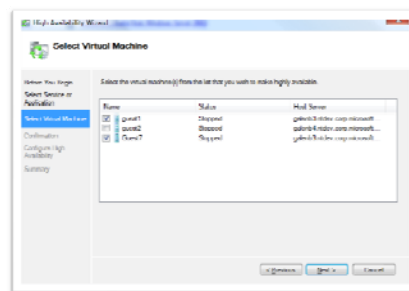
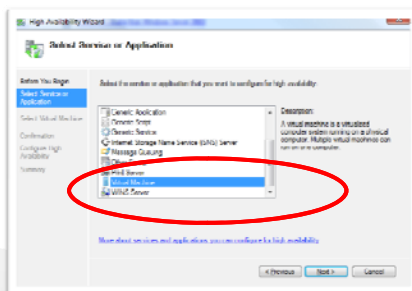


CONVERGENCE

ISACA
Setting IT Governance Professionals
San Francisco Chapter

Virtual Machine Clustering

- Tight integration of Hyper-V with Clustering
 - Wizards for creating highly available VM's
 - New resource type to enable Quick Migrations
 - No more clunky scripts



CONVERGENCE

ISACA
Setting IT Governance Professionals
San Francisco Chapter

Geographically Dispersed Clusters

- No More Single-Subnet Limitation
 - Allow cluster nodes to communicate across network routers
 - No more having to connect nodes with VLANs!
- Configurable Heartbeat Timeouts
 - Increase to Extend Geographically Dispersed Clusters over greater distances
 - Decrease to detect failures faster and take recovery actions for quicker failover

Questions

Donald E. Hester
CISSP, CISA, CAP, MCT, MCITP, MCTS⁴,
MCSE Security, MCSA Security, MCDST,
Security+, CTT+

Blog
www.LearnSecurity.org
LinkedIn
<http://www.linkedin.com/in/donaldehester>



Windows Server 2008 R2 & Windows 7 Security Features



The graphic features a large grey arrow pointing right. On the left, the Windows 7 logo is above the text "Windows 7". In the center, the word "CONVERGEMERGE" is written in large, bold, black letters. Above it, "Windows Server 2008 R2" is written in black and red. A circular diagram with arrows connects the text "KNOWLEDGE", "CONTROLS", "STRONGER", "WITH YOUR PEERS", "2009 FALL CONFERENCE", "MORE MARKETABLE", and "BETTER NETWORKED". The text "SF ISACA" is at the top of the circle. Below the arrow, the dates "September 21, 2009 – September 23, 2009" are listed. The ISACA logo is in the bottom right corner.

Windows 7

Windows Server 2008 R2

KNOWLEDGE

CONTROLS

STRONGER

WITH YOUR PEERS

2009 FALL CONFERENCE

MORE MARKETABLE

BETTER NETWORKED

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows 7

- AppLocker
- BitLocker
- Direct Access
- User Account Control
- Windows Filtering Platform (WFP)
- Biometrics Support
- SmartCard Support
- System Restore
- Windows Defender
- DNSSEC Support
- Action Center



CONVERGEMERGE



Windows 7 Goals

- Fundamentally Secure Platform
 - Windows Vista Foundation
 - Streamlined UAC
 - Enhanced Auditing
- Protect Users & Infrastructure
- Secure Anywhere access
- Protect Data for Unauthorized Viewing

CONVERGENCE

71

ISACA
Serving IT Governance Professionals
San Francisco Chapter

The screenshot displays the Windows 7 AppLocker configuration console. On the left, the navigation tree shows the path: Console Root > Local Computer Policy > Computer Configuration > Security Settings > Application Control Policies > AppLocker. The right-hand pane is titled "AppLocker provides access control for applications" and contains three sections: "Getting Started" with introductory text and links; "Configure Rule Enforcement" with a warning icon and instructions on enforcing rules; and "Overview" which lists three rule collections: "Executable Rules", "Windows Installer Rules", and "Script Rules", each showing "Rules: 0" and "Enforcement not configured: Rules are enforced".

Windows Filtering Platform (WFP)

- group of APIs and system services that allow third party vendors to tap further into Windows' native firewall resources
- The idea is that third parties can take advantage of aspects of the Microsoft Windows Firewall in their own products. Microsoft says "third-party products also can selectively turn parts of the Windows Firewall on or off, enabling you to choose which software firewall you want to use and have it coexist with Windows Firewall"



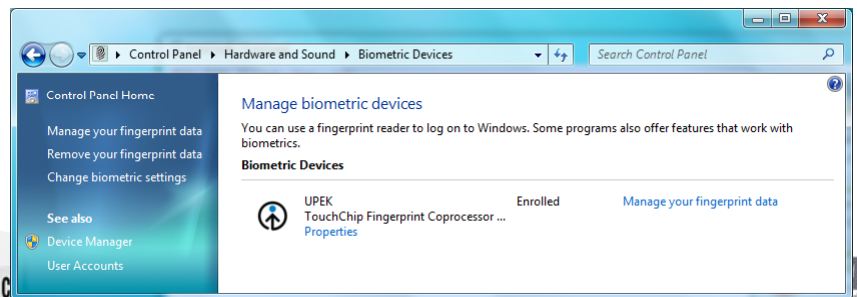
Multiple Active Firewall Policies

- Windows 7 and WFP in particular permit multiple firewall policies, so IT professionals can maintain a single set of rules for remote clients and for clients that are physically connected to their networks
- Only one profile at a time with Vista
- Multiple profiles, each connection has its own profile
 - Connect to home network then start a VPN which policy is applied?

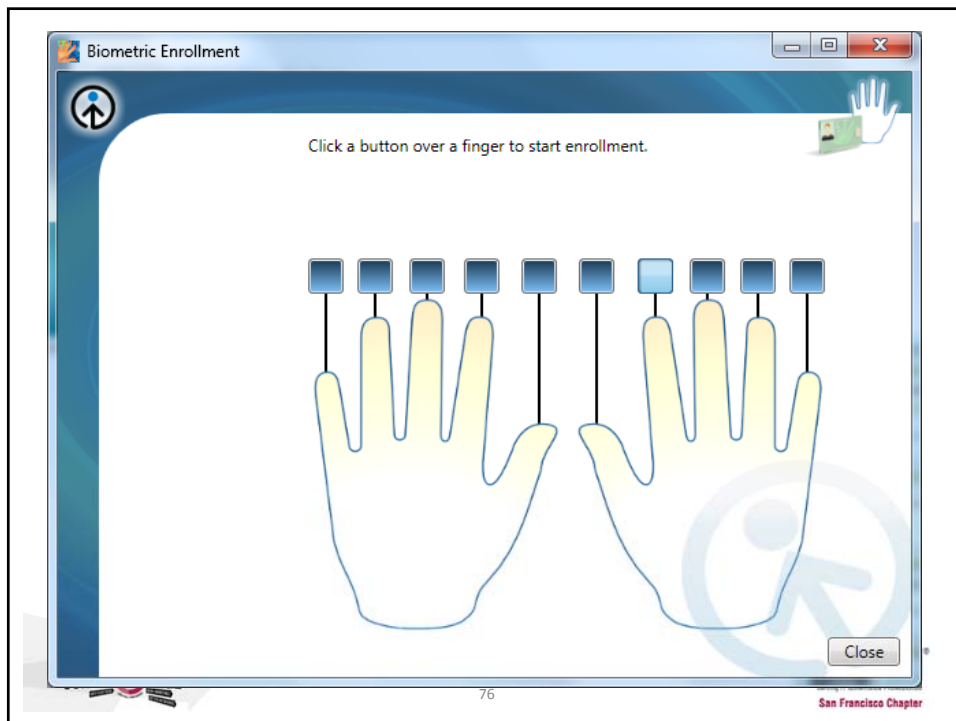


Biometrics Support

- Biometrics enhancements include easier reader configurations, allowing users to manage the fingerprint data stored on the computer and control how they log on to Windows 7



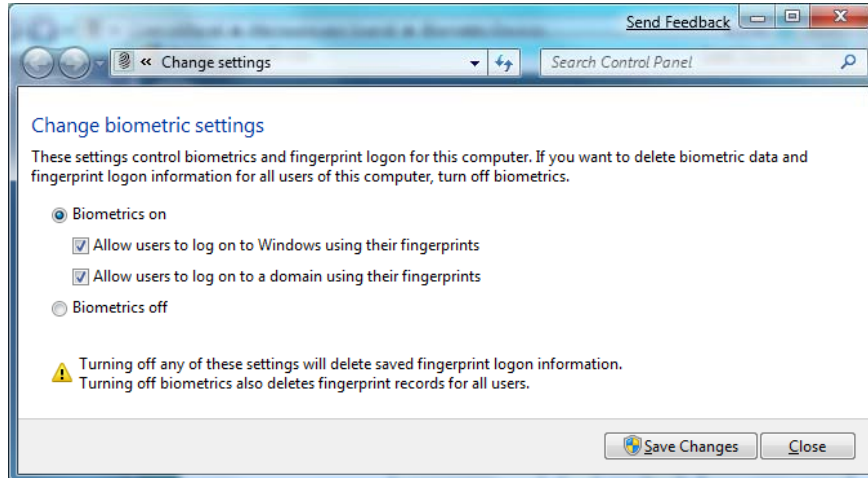
San Francisco Chapter



76

San Francisco Chapter

Biometric Settings



77



Smart Card Support

- Windows 7 extends the smart card support offered in Windows Vista by automatically installing the drivers required to support smart cards and smart card readers, without administrative permission.



System Restore

- System Restore includes a list of programs that will be removed or added, providing users with more information before they choose which restore point to use
- Restore points are also available in backups, providing a larger list to choose from, over a longer period of time



System Restore

- First, System Restore displays a list of specific files that will be removed or added at each restore point.
- Second, restore points are now available in backups, giving IT professionals and others a greater list of options over a longer period of time



BranchCache

- Microsoft recommends that users run Windows 7 clients in conjunction with Windows 2008 R2 servers in order to get the benefit of BranchCache, a caching application that makes networked applications faster and more responsive

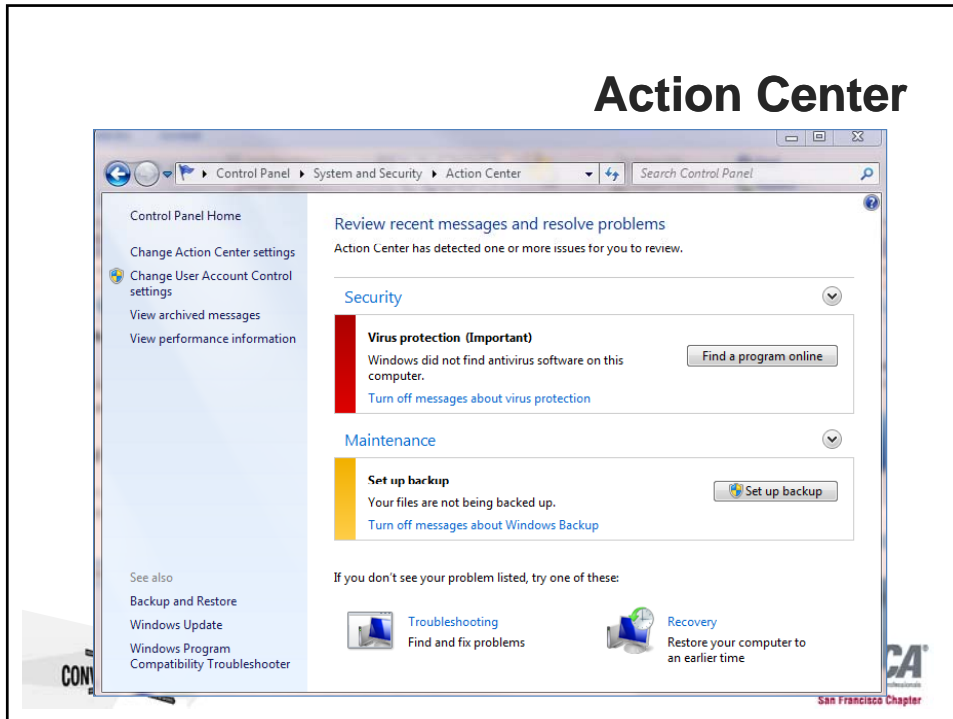


Action Center

- Action Center includes alerts and configuration settings for several existing features, including:
 - Security Center
 - Problem, Reports, and Solutions
 - Windows Defender
 - Windows Update
 - Diagnostics
 - Network Access Protection
 - Backup and Restore
 - Recovery
 - User Account Control

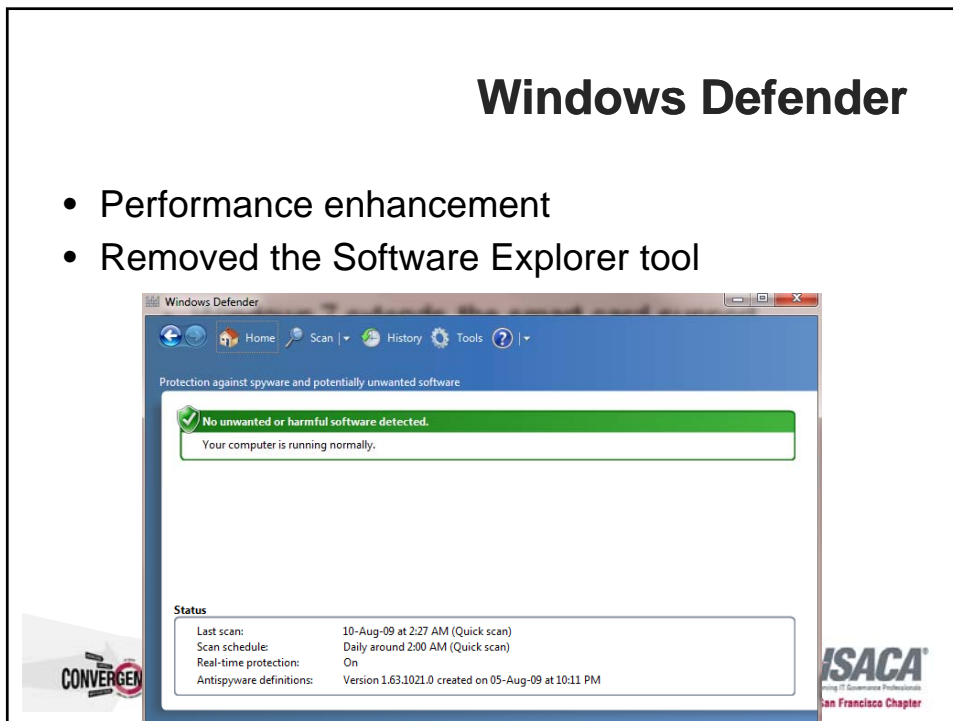


Action Center



Windows Defender

- Performance enhancement
- Removed the Software Explorer tool



DNSSEC

- Windows 7 also supports Domain Name System Security Extensions (DNSSEC), newly established protocols that give organizations greater confidence that DNS records are not being spoofed



Name Resolution Policy

Overview

The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and Direct Access on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).

[Learn more about DNSSEC on the Web](#)

Description

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

Create Rules

To which part of the namespace does this rule apply?

Suffix:

Certification authority: (Optional)

DNSSEC | **DNS Settings for Direct Access**

Enable DNSSEC in this rule

DNSSEC settings

Validation:

Require DNS clients to check that name and address data has been validated by the DNS server



IPsec:

Use IPsec in communication between the DNS client and DNS server

Encryption type:

Name Resolution Policy Table

Namespace	CA	DNSSEC (V...)	DNSSEC (I...)	DNSSEC (I...)	Direct Acce...	Direct Acce...	Direct Acce...	Direct Acce...



Event Auditing

- Windows 7 also makes enhancements to event auditing
- Regulatory and business requirements are easier to fulfill through management of audit configurations, monitoring of changes made by specific people or groups, and more-granular reporting.
- For example, Windows 7 reports why someone was granted or denied access to specific information.



Advanced Audit Policy Configuration

Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.

[More about Advanced Audit Configuration](#)

[Which editions of windows support Advanced Audit Configuration?](#)

A summary of the settings is provided below:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured



Vista / Windows 7

- Kernel Patch Protection
- Service Hardening
- Data Execution Prevention
- Address Space Layout Randomization
- Mandatory Integrity Levels

CONVERGENCE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

IE 8

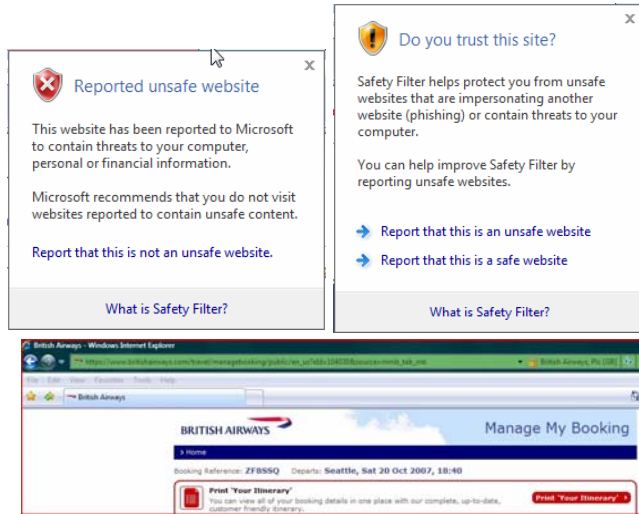


Internet Explorer 8 security features target three major sources of security exploits: social engineering, Web server, and browser-based vulnerabilities

CONVERGENCE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

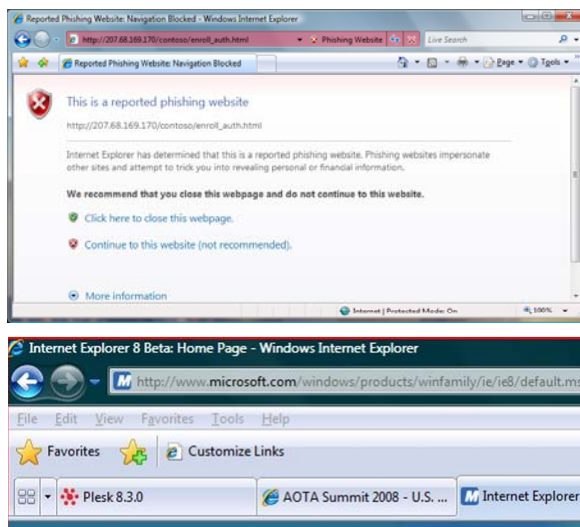
Internet Explorer 7 Contribution to Building Trust



Phishing Filter
Over 1M phishing attempts blocked per week

Extended Validation Certificates
Over 5000 issued to date

What's New in Trust in Internet Explorer 8?



SmartScreen™
Expanding scope to incorporate new threats



Domain Name Highlighting
Helps the user identify real domain name

Internet Explorer 8 Management



Group Policy (over 1300 in IE8)

- Control browser features, ex : Turn on/off Phishing Filter
- Configure browser features, ex : home page, favorites
- Enforce security settings, ex: trusted sites
- New features exposed through group policy



Support Infrastructure

- Pay per incident support available to everyone
- Support agreements for Windows OS include support for Internet Explorer
- Professional support organization provides issue resolution

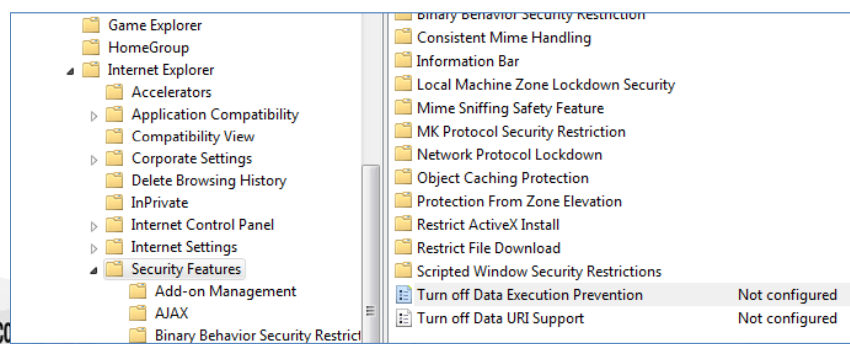


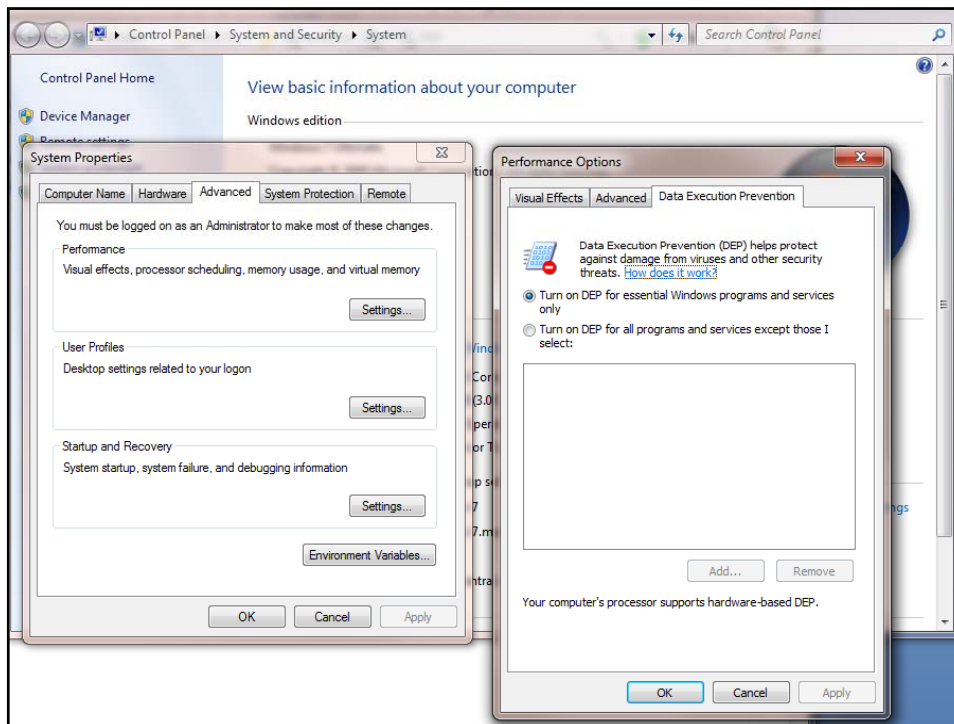
New in IE8 – Crash Recovery

- Tabs isolated into separate processes – one tab crashing does not bring down the browser
- Crash recovery reloads tabs when they crash

IE 8 DEP

- Internet Explorer 7 on Windows Vista introduced an DEP off-by-default
- DEP enabled by default for IE 8 on Windows Server 2008 and Windows Vista SP1 and later





6 Reasons You (Should) Care About the Browser

Customer Connection

- Your company has a website and does business on the web

Customer Trust

- Your business on the web relies on customer trust that the web is a safe place to do business

Security

- You care about the integrity of your business data, infrastructure and PCs

Compatibility & Standards


- Your company uses internal web apps and is building or buying more

Supportability

- Your users probably spend 2 hours or more in the browser every day

Manageability

- Keeping up to date with browser patches and updates is hard




Windows Server® 2008 R2

CONVERGEMERGE

KNOWLEDGE
CONTROLS
WITH YOUR PEERS
SF ISACA
2009 FALL CONFERENCE
STRONGER
MORE MARKETABLE
BETTER NETWORKED

September 21, 2009 – September 23, 2009



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows Server 2008 R2

- BitLocker
- Virtual Accounts
- Managed Service Accounts
- Hyper-V R2
- Cluster Failover
- Live Migration



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Managed Service Accounts

- Services sometimes require network identity e.g. SQL, IIS
- Before, domain account was only option
 - Required administrator to manage password and Service Principal Names (SPN)
 - Management could cause outage while clients updated to use new password
- Windows Server 2008 R2 Active Directory introduces Managed Service Accounts (MSA)
 - New AD class
 - Password and SPN automatically managed by AD like computer accounts
 - Configured via PowerShell scripts
 - Limitation: can be assigned to one system only



Virtual Accounts

- Want better isolation than existing service accounts
 - Don't want to manage passwords
- Virtual accounts are like service accounts:
 - Process runs with virtual SID as principal
 - Can ACL objects to that SID
 - System-managed password
 - Show up as computer account when accessing network
- Services can specify a virtual account
 - Account name must be "NT SERVICE\<<service>"
 - Service control manager verifies that service name matches account name
 - Service control manager creates a user profile for the account
- Also used by IIS app pool and SQL Server



Migration

- Quick Migration
 - Pauses the virtual machine
 - Moves the virtual machine
 - Resume the virtual machine
- Live Migration
 - Move virtual machine without stopping
- Cluster Fail Over
 - Automatic failover for virtual machines



The screenshot displays the Failover Cluster Manager interface. The left-hand tree view shows the cluster hierarchy, including nodes (PTSIBMR2N1, PTSIBMR2N2), storage, and networks. The main pane is titled 'Services and applications' and contains a table with the following data:

Name	Status	Type	Current Owner	Auto start
CSV-VM1	Online	Virtual Machine	PTSIBMR2N2	Yes
CSV-VM2	Online	Virtual Machine	PTSIBMR2N2	Yes
PTD1	Online	Virtual Machine	PTSIBMR2N1	Yes
Regular	Online	Virtual Machine	PTSIBMR2N1	Yes

Below the table, the '4 Services and applications. 1 item selected.' section shows details for 'CSV-VM1':

- Status: Online
- Auto Start: Yes
- Preferred Owners: <none>
- Alerts: <none>
- Storage: <none>
- Current Owner: PTSIBMR2N2
- Client Access Name: <none>
- Capacity: Total: 0 Bytes, Free Space: 0 Bytes, Percent Free: 0%
- IP Addresses: <none>
- Other Resources: 2

The right-hand pane shows the 'Actions' menu for 'CSV-VM1', including options like 'Connect to virtual mac...', 'Start virtual machines', 'Turn off virtual machines', 'Shut down virtual mac...', 'Save virtual machines', 'Live migrate virtual ma...', 'Cancel in-progress live...', 'Quick migrate virtual ...', 'Manage virtual machine', 'Move virtual machine(...)', 'Show the critical even...', 'Add storage', 'Add a resource', 'Disable auto start', 'Show Dependency Re...', 'Delete', and 'Properties'.

Live Migration

The screenshot shows the Hyper-V Manager interface. A context menu is open over a virtual machine, with the option 'Quick migrate virtual machine(s) to another node' selected. The menu also includes options like 'Live migrate virtual machine to another node', 'Move virtual machine(s) to another node', and 'Show the critical events for this application'. The background shows a table of virtual machines with columns for Name, Status, Type, and Current Owner.

Services and applications	Name	Status	Type	Current Owner
CSV-VM1	Virtual Machine	PTSIBMR2
CSV-VM	Virtual Machine	PTSIBMR2
PTD1	Virtual Machine	PTSIBMR2
Regular	Virtual Machine	PTSIBMR2



No Lost Connection

The screenshot shows the Hyper-V Manager interface during a live migration. A 'Verifying settings' dialog box is open, indicating 'Detecting VM(s) state'. In the background, the 'Summary of Regular' window shows the virtual machine's status as 'Online' and 'Auto Start: Yes'. A command prompt window is also visible, showing the execution of a ping command to the virtual machine's IP address (157.58.38.54).

```

Administrator: C:\Windows\system32\cmd.exe - ping ptsib...
Pong 157.58.38.54: bytes=32 time<1ms T...
Pong 157.58.38.54: bytes=32 time<1ms T...
Pong 157.58.38.54: bytes=32 time<1ms T...
Pong 157.58.38.54: bytes=32 time<1ms T...
  
```

The screenshot shows the Hyper-V Manager console. The virtual machine 'Virtual Machine Reg...' is shown with a status of 'Running (Migrating, 43% ...)'. Below it, another virtual machine is shown as 'Online'.



PowerShell

Administrator: Windows PowerShell Modules

Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

```
PS C:\Windows\system32> Get-Cluster "hypercluster" | Move-ClusterVirtualMachineRole -Name "CSV-VM2" -Node "PTSI1BMR2N2"
```

Get-Cluster "*name*" for the name of the cluster

Move-ClusterVirtualMachineRole -Name "*name*" for the name of the virtual machine

-Node "*destination name*" for the location to move it to

Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

```
Move-ClusterVirtualMachineRole
Performing live migration of virtual machine 'CSV-VM2'.
[.....]
```

Progress (above) and Result (below)

Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

```
PS C:\Windows\system32> Get-Cluster "hypercluster" | Move-ClusterVirtualMachineRole -Name "CSV-VM2" -Node "PTSI1BMR2N2"
```

Name	OwnerNode	State
CSV-VM2	ptsibmr2n2	Online

PS C:\Windows\system32> _

Cluster Fail Over

hypercluster.ptsdomain.local

- Services and applications
 - CSV-VM1
 - CSV-VM2
 - PTD1
 - Regular
- Nodes
 - PTSIBMR2N1
 - PTSIBMR2N2**
- Cluster Shared Volumes
- Storage

Name	Status
CSV-VM1	Pending (Starting VM)
CSV-VM2	Pending (Starting VM)
PTD1	Pending
Regular	Pending

Name	Status	Type
CSV-VM1	Online	Virtual
CSV-VM2	Online	Virtual
PTD1	Pending (Starting VM)	Virtual
Regular	Pending (Starting VM)	Virtual

CONVERGEMET

ISACA
Saving IT Governance Professionals
San Francisco Chapter

Notes

- <http://blogs.techrepublic.com.com/10things/?p=488>
- <http://www.microsoft.com/windows/internet-explorer/default.aspx>
- <http://technet.microsoft.com/en-us/library/dd367859.aspx>
- <http://blogs.msdn.com/vijaysk/archive/2009/02/13/goodbye-network-service.aspx>
- <http://www.neowin.net/news/main/09/01/11/windows-7-problem-steps-recorder-overview>
-



Resources

Microsoft
tech·ed
Online

www.microsoft.com/teched
Sessions On-Demand & Community

Microsoft | **Learning**

www.microsoft.com/learning
Microsoft Certification & Training Resources

Microsoft **TechNet**

<http://microsoft.com/technet>
Resources for IT Professionals

msdn

<http://microsoft.com/msdn>
Resources for Developers

www.microsoftlearning.com
Microsoft E Learning Resources