Read more

Monday, June 10, 2013
8:17 PM

Active Directory Administrative Center - http://technet.microsoft.com/en-us/library/dd560651(v=ws.10).aspx
AD Powershell commands - http://technet.microsoft.com/en-us/library/dd378783(WS.10).aspx
AD Recycle Bin - http://technet.microsoft.com/en-us/library/dd391916(v=ws.10).aspx
NTDSUtil and DSAMain - http://technet.microsoft.com/en-us/library/cc753609(WS.10).aspx
AD FS - http://technet.microsoft.com/en-us/library/cc733115.aspx
AD CS - http://technet.microsoft.com/en-us/library/cc732625.aspx
Certificates - http://technet.microsoft.com/en-us/library/cc754122.aspx
Delegated Authentication - http://technet.microsoft.com/en-us/library/cc780217(v=WS.10).aspx
Authorization Manager - http://technet.microsoft.com/en-us/library/cc726036(WS.10).aspx
File Classification Infrastructure - http://blogs.technet.com/b/filecab/archive/2009/05/11/windows-server-2008-r2-file-classification-infrastructure-managing-data-based-on-business-value.aspx
Desktop Optimization Pack

Chapter 1. Planning Installation and Upgrade

Saturday, June 08, 2013
10:16 PM

Windows Server 2008 R2 comes with a Foundation edition, while Server 2008 doesn't.
New features of 2008 R2: AD Recycle Bin, Hyper-V Dynamic Memory, managed service accounts, AppLocker, DirectAccess, BranchCache, IIS 7.5, and AD CS in Server Core,

Windows Server 2008 R2 Standard

- Maximum 32GB of RAM and 4 sockets
- Licensed for a host and one VM
- Doesn't support AD FS
- Limited to 250 connections for RRAS and Remote Desktop Gateway
- Not all features of AD CS are supported

Windows Server 2008 R2 Enterprise

- Maximum 2 TB of RAM and 8 sockets
- Licensed for a host plus 4 VMs
- Supports Exchange 2010 with Database Availability Groups
- Supports MS SQL Server clustering
- Supports AD FS and all features of AD CS

Windows Server 2008 R2 Datacenter

- Maximum 2 TB of RAM and 64 sockets
- Unlimited number of VMs

Windows Web Server 2008 R2

- Maximum 32 GB of RAM and 4 sockets
- Supports IIS and DNS

Windows Server 2008 R2 for Itanium

- Supports 2 TB of RAM and 64 sockets
- Supports application servers and IIS

Windows Server 2008 R2 Foundation

- Aimed for companies with 15 users or fewer
- Supports AD RMS, IIS 7.5, NAP, Remote Desktop, and WDS
- Doesn't support Hyper-V, failover clustering, and BranchCache
- Doesn't support Server COre

Server Core

Windows Server 2008 Server Core doesn't support PowerShell directly.
Windows Server 2008 R2 Server Core supports PowerShell V2.

Upgrading to Windows Server 2008 and 2008 R2

You can upgrade from Standard Edition to Enterprise Edition
You can only upgrade Datacenter Edition to Datacenter Edition
You can upgrade Windows Server 2008 Server Core x64 to Server 2008 R2 Server Core
You cannot upgrade Server 2003 to Server 2008 Core.
You can upgrade Server 2003 to Server 2008 if SP1 is installed

Chapter 1. Server Deployment

Sunday, June 09, 2013
11:42 AM

The answer file is named **autounattended.xml**.
Windows System Image Manager (Windows SIM) is used to create XML files. It's included with WAIK.
If the answer file is located on a network share, boot the server into Windows PE, connect to the share and run the setup: **setup.exe /unattend:x:\autounattend.xml**

Steps to create an answer file:

1) Download and start Windows SIM
2) Copy the file \Sources\Install.wim from the DVD.
3) File -> Select Windows Image -> Select **Install.wim** file
4) Select a Windows Server 2008 R2 edition
5) Click Yes to create a catalog file
6) File -> New Answer File
7) Create the answer file, validate, and save it.

Windows Deployment Services

WDS Requirements: member of AD DS domain, DNS, DHCP, the operating system is stored on NTFS partition.
WDS doesn't support Server Core. WDSUtil.exe can be used to configure WDS from the command line.

PXE Server Initial Configuration

If the WDS is installed on a DHCP server, configure it not to listen on port 67, otherwise, there will be a conflict. Also, configure option 60 to advertise that this server supports PXE clients.
WDS can repond to the following clients:

- **Do not respond to any client computers**
- **Respond only to known client computers** - prestaged computer accounts are required
- **Respond to all client computers**
- **Respond to all client computer and require administrative approval -** new computers will be listed in Pending Devices node.

You must have at least one Install image and one Boot image. Images can be added upon completion of the wizard.

Other WDS Settings

- **Client Tab** - allows to specify the unattended file location for all architectures.
- **Multicast Tab** - used to configure Multicast addresses. Multicast Transfer settings:
    - Keep all multicast clients in the session at the same speed
    - Separate client into three sessions (slow, medium, fast)
    - Separate clients into two sessions (slow and fast)
    - Automatically disconnect clients below this speed - specify speed in Kbps.
- **AD DS Tab -** specifies where to store computer accounts:
    - Same domain as WDS server
    - Same domain as the user performing the installation - setup will ask for a valied user name and password
    - Same OU as the user performing the installation
    - The following location - specify
- **Boot tab -** configures boot options for known and unknown clients

    - Require the user to press F12 to continue the PXE boot
    - Always continue the PXE boot
    - Continue the PXE boot unless the user presses the ESC key

Multicast, Scheduled, and Automatic Deployment

- **Auto-cast -** starts installation automatically when a client requests the image. As other clients request the same image, they will be joined the already started transmission.
- **Scheduled-cast -** starts the transmission based on the following criteria:
    - Start when the number of clients that requested the image is - specify the number
    - Start at a later time - specify date and time - requires an answer file for automatic installation

WDS Image

- **Install image - Install.wim**
- **Boot image - Boot.wim**
- **Capture image** - boot image that starts the WDS capture utility. It can capture the reference computer's image prepared with Sysprep for deployment with WDS
- **Discover image** - used to deploy images on computers that are not PXE enabled.

Product Activation

- **MAK Proxy Activation** - uses centralized activation request on behalf of multiple clients using a single connection to Microsoft's activation servers. Use the Volume Activation Management Tool (VAMT).
- **MAK Independent Activation** - requires that each computer activates individually
- **KMS Activation**
    - Need to have at least 5 computers running Windows Server 2008 R2 or 25 computers running Windows 7 or Vista
    - KMS Server running on Windows 7 can't activate server operating systems
    - The same KMS key can be installed on up to 6 computers
    - All computers must reactivate every 180 days

Chapter 2. Planning IPv6

Tuesday, May 14, 2013
8:49 PM

Multiple interfaces can use the same unicast address, providing for load-balancing.

Global unicast address always begins with 001. The next 13 bits are allocated by the IANA and are known as the Top Level Aggregator. They are allocated to large ISPs. The next 8 bits are reserved for future expansion. Next 24 bits are the Next Level Aggregator (NLA), which identifies a specific customer site. The next 16 bits are the Site Level Aggregator (SLA), which is used to organize addressing and routing for downstream ISPs.

001	TLA ID	Reserved	NLA ID	SLA ID	Interface ID
3 bits	13 bits	8 bits	16 bit	8 bit	64 bit

Link-local addresses begin with fe80
Site-local addresses begin with fec0, followed by 32 zeroes and 16-bit subnet ID. Can be allocated through stateful address configuration (such as when using a DHCPv6 sever) or stateless configuration (using router advertisements).
IPv6 multicast addresses always begin with ff, followed by 4 bits of flags and 4 bits of scope, and then 112 bits of Group ID.
Multicast addresses begin with ff.

The IPv4 compatible address ::w.x.y.z is used by dual-stack nodes that are communicating with IPv6 over an IPv4 infrastructure. The IPv6 is encapsulated with an IPv4 header and sent to the destination using the IPv4 infrastructure.
The IPv4 mapped address ::ffff:w.x.y.z is used to represent an IPv4-only node to an IPv6 node
The Teredo address consists of a 32-bit Teredo prefix 2001::/32. It is followed by the IPv4 public address of the Teredo server. The next 16 bits are reserved for Teredo flags. The next 16 bits are obfuscated version of the external UDP port that corresponds to all Teredo traffic for the Teredo client interface. The final 32 bits store an obfuscated version of the external IPv4 address .
The ISATAP addresses are used to communicate between two nodes over an IPv4 network. It starts with a 64-bit prefix, followed by the ISATAP prefix 0:5efe. The final 32 bits are the IPv4 address. An ISATAP address can be link-local, site-local, global, or 6to4 global address. By default, Windows Server 2008 and 2008 R2 automatically configure the ISATAP address fe80::5efe:w.x.y.z for each IPv4 address that is assigned to a node.

In a **full-cone NAT**, all requests from the same internal IP address and port are mapped to the same external IP address and port. Any external host can send a packet to the internal host by sending a packet to the mapped external address.
In a **restricted cone NAT**, all requests from the same internal IP address and port are mapped to the same external IP address and port, but an external host can send a packet to the internal host if the internal host had previously sent a packet to the external host.
In a **port-restricted cone NAT**, the restriction includes port numbers. An external host with a specified IP address and source port can send a packet to an internal host only if the internal host had previously sent a packet to that address and port.

An ISATAP address starts with a 64-bit unicast, link-local, global or 6to4 global prefix. The next 32 bits are the ISATAP identifier 0:5efe. The final 32 bit have the IPv4 address. Examples
Link-local - fe80::5efe:w.x.y.z
Site-local - fec0:1111::5efe:w.x.y.z
Global - 3ffe:1a05:510:1111:0:5efe.w.x.y.z

6to4 - 2002:9b36:1:2:0:5efe:w.x.y.z
ISATAP address is automatically configured for each IPv4 address.

To check IPv6 address configuration, use **netsh interface ipv6 show address**
To set an IPv6 address, use the command **netsh interface ipv6 set address *connection ipv6_address***
To set an IPv6 DNS server, use the command **netsh interface ipv6 add dnsserver *connection ipv6_dns***
To check the contents of the neighbor cache, use **netsh interface ipv6 show neighbors**
To delete the neighbor cache, use the command **netsh interface ipv6 delete neighbors**
To show the destination cache, use the command **netsh interface ipv6 show destinationcache**
To clear the destination cache, use the command **netsh interface ipv6 delete destinationcache**

Stateless configuration doesn't include a host address - it's autoconfigured.
Stateful configuration specifies the host address.
IPv6 addresses of DNS servers are assigned by using DHCPv6 option 00023. DNS server addresses are not configured when router advertisements are used.

Chapter 2. Planning DNS

Wednesday, May 15, 2013
5:43 PM

IPv6 doesn't support WINS.
A partition is a data container in AD that holds data for replication. DNS zone data can be stored in either the domain, or an application directory partition, in which case you can specify which partition to use.
Conditional forwarding entries can be stored in AD DS and replicated to all DNS servers in the forest, all DNS servers in the domain, or all domain controllers in the domain.

DNS cache is flushed every 15 minutes.
Ipconfig /displaydns - shows the contents of the DNS cache
Nslookup ls -d <domain> - displays all the DNS records in the domain. Uses zone transfers

GlobalNames zone is supported in both Windows Server 2008 and 2008 R2.
GlobalNames zone can contain records for multiple forests, but you must use SRV records to publish the zone location. GlobalNames zone holds CNAME records that map a single-label name to an FQDN. AD DS integration of the GlobalNames zone and SRV records are required to support the zone across multiple forests.

WINS

WINS servers can be configured as either push or pull partners for replication. A push partner sends a message to its pull partners when its WINS database changes. A pull partner is a WINS server that requests new database entries from its push partners be requesting entries with a higher version number than the entries it received during the last replication. Pull replication can be configured to occur at specific intervals.

WINS Topologies

- **Centralized WINS topology -** single high availability WINS server or cluster. No replication, but no WINS database fault tolerance.
- **Full-mesh WINS topology -** multiple WINS servers
- **Ring WINS topology -** replication only occurs with specific neighbors, forming a circle. The topology needs to be created manually
- **Hub-and-spoke WINS topology -** distributed WINS design with a central server

Forwarding DNS queries requires that the DNS server is capable of making recursive queries.

A secondary zone server doesn't need to be a part of domain, except when it's configured as a RODC.

By default, DNS zones are replicated to all domain controllers in the domain.
Replicating to all domain controllers in the domain is recommended only if you have Windows 2000 domain controllers.

To create a reverse lookup IPv6 zone for subnet fec0::eefd/64, use the command:
Dnscmd . /ZoneAdd d.f.e.e.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa /DsPrimary

Chapter 3. AD DS

Monday, June 10, 2013
6:38 PM

New features in Windows Server 2008:

- RODC
- Fine-grained password policies
- Restartable AD DS Service, allows to perform operations such as defragmentation without restarting a DC
- AD DS Data Mining tool allows viewing AD data stored in snapshots
- Auditing allows to log old and new values when changes are made to an AD object

New features in Windows Server 2008 R2

- New domain and forest functional level
- AD Recycle Bin - forest level must be Windows Server 2008 R2
- AD can be managed using PowerShell
- Best Practices Analyzer for each server role
- Answer file can be exported when promoting a DC
- Simplified RODC installation
- Active Directory Administrative Center

The Active Directory Administrative Center

Active Directory Web Services must be installed on at least one DC to use ADAC. Requires TCP port 9389.
ADAC Features:

- Create new users, groups, computer accounts and OUs, and manage existing ones
- Connect to one or several DCs
- Filter AD data by using queries
- View domains that belong to the same forest or have a trust with the local domain

AD Module for PowerShell

Cmdlet	Description
Enable-ADAccount	Enables and AD account
Set-ADAccountControl	Modifies account properties
Set-ADAccountPassword	Changes or resets password
Set-ADComputer	Modifies a computer account
Get-ADComputerServiceAccount	Gets the service accounts that are hosted on a specified computer
Set-ADDefaultDomainPasswordPolicy	Modifies the default password policy
New-ADFineGrainedPasswordPolicy	Creates a new fine-grained password policy
Set-ADGroup	Modifies a group
Set-ADObject	Modifies an AD object
Enable-ADOptionalFeature	Enables AD optional features
New-ADServiceAccount	Creates a new service account

RODC

At least one writable DC must be running Windows Server 2008 or 2008 R2. The functional level of the domain and forest must be at least Windows Server 2003. **ADPrep /RODCPrep** command must be run on an infrastructure master role. To create an RODC, click the Domain Controllers container and choose Pre-create RODC account. You can delegate the RODC installation to a user or a group. When you delete an RODC account, you have an option of automatically forcing a password change on all accounts that were replicated to the RODC.

AD DS Installation Wizard

Advanced mode installation options:

- Select the source domain controller for replication
- Use backup media to reduce network traffic
- Create a new domain tree
- Change the default NetBIOS name when creating a new domain
- Set forest and domain functional levels when creating a new forest or domain
- Configure Password Replication Policy for an RODC
- Export settings to an answer file

Fine-grained Password and Account Lockout Policies

The Password Settings Container (PSC) object class is created under the System Container in the domain. It stores the Password Settings Objects (PSOs) for the domain. A PSO can be created by using ADSI Edit or LDIFDE.

Fine-grained password policies can only apply to users and groups, not computers. An exceptional PSO can be created to exclude users for another PSO. A PSO with a lower precedence number overrides PSOs with higher numbers.

Data Mining Tool

The data mining tool (dsamain.exe) makes it possible for deleted AD DS and AD LDS data to be preserved in snapshots taken by the VSS service and NTDSUtil. LDP.exe and ADUC can be used to view the read-only data in the snapshot.

AD DS Auditing

In Windows Server 2008 and 2008 R2, the Audit Directory Service Access global audit policy is enabled by default. You can audit DS access, DS changes (old and new values), and DS replication.

Domain and Forest Functional Levels

If the forest functional level is raised to Windows Server 2008 R2 and AD Recycle Bin has not been enabled, it's possible to roll it back to Windows Server 2008.

A default installation of the Windows Server 2008 R2 will create a domain with the Windows 2000 native functional level.

You should raise the domain functional levels on GC servers. When all domains are at the required domain functional levels, you should raise the forest functional level on a GC server in the root domain.

Domain Functional Levels

- Windows 2000 Native
    - All default AD features
    - Universal distribution and security groups
    - Group nesting
    - Group conversion
    - SID history

- Windows Server 2003
    - All default AD features
    - The domain management tool - netdom.exe
    - Logon time stamp update
    - Redirecting the Users and Computers containers
    - Selective cross-forest authentication
- Windows Server 2008
    - DFS replication support for SYSVOL
    - AES support for the Kerberos authentication protocol
    - Last interactive logon information
    - Fine-grained password policies
- Windows Server 2008 R2
    - Authentication mechanism assurance
    - Automatic SPN management

Forest Functional Levels

Windows 2000 is the default forest functional level. Windows NT 4 backup domain controllers can operate in an AD domain if the forest functional level is Windows 2000.

- Windows 2000
    - All default AD features
- Windows Server 2003
    - Forest trusts
    - Domain renaming
    - Linked-value replication
    - RODC deployment
    - Improved Knowledge Consistency Checker (KCC) and Intersite Topology Generator (ITG) algorithms
- Windows Server 2008
    - No additional features
- Windows Server 2008 R2
    - AD Recycle Bin

AD Recycle Bin

After all domain and forest functional levels have been raised to Windows Server 2008 R2, you can enable AD Recycle Bin by using PowerShell or ldp.exe. TCP/9389 needs to be open.
When AD Recycle Bin is enabled, every non-global catalog domain controller acts like an Infrastructure Master.

Forest-Level Trusts

A forest trust allows every domain in one forest to trust every domain in a second forest. Forest trusts can be one-way incoming, one-way outgoing, or two-way.

- **Shortcut Trust -** enables any domain in one forest to trust any domain in another forest.
- **External Trust -** typically used when migrating from Windows NT domain
- **Real Trust -** typically used between a Windows domain and UNIX realm

If users in Forest A require access to resources in Forest B, then Forest A is a trusted forest and Forest B is a trusting forest.

- One-way trust created in a resource forest is incoming trust
- One-way trust created in the trusted domain is an outgoing trust

To create a forest trust, open the AD Domains and Trusts snap-in. Connect the tool to a domain controller in the forest root domain. Right-click the root domain -> Properties -> Trust -> New Trust

wizard. If you know passwords for both domains, you can create both sides of the trust. If you only have a password for one domain, choose the This Domain Only option.

Selective Authentication provides AD administrators who manage the trusting forest more control over which groups or users ina trusted forest can access shared resources in a trusting forest. Both AD Domains and Trusts and Netdom.exe command can be used to enable Selective Authentication. The **Allowed To Authenticate** permission can be set on computer objects that represent member servers running Windows NT and higher.

Active Directory Federation Services

Enables organizations to allow limited access to their infrastructure to trusted partners. It operates like a cross-forest trust that operates over the Internet and extends the trust relationship to Web applications. It provides Web single sign-on technology.
New features in AD FS in Windows Server 2008 and 2008 R2:

- **Improved application support -** integrates AD FS with SharePoint Server 2007 and AD RMS
- **Improved installation -** includes server validation checks
- **Improved trust policy -** allows importing and exporting policies

Chapter 3. AD CS

Wednesday, June 12, 2013
7:03 PM

Types of CAs

- Enterprise - require access to AD. Uses Group Policy to propagate the certificate trust list to users and computers throughout the domain and publish CRLs in the AD. Enforce credential checks during the enrollment process. Certificate names are generated automatically from AD. Autoenrollment can be used
- Standalone - do not require AD. The certificate requestor must provide all relevant identifying information and manually specify the type of certificate needed. Standalone CA requests require administrator's approval. Do not use certificate templates.

If a domain administrators install the Standalone CA on a member server, the CA's information is added to the Trusted Root Certificate Authorities for all users and computers in the domain. The CA will be able to publish its CRL to AD.

CS Role-based Administration

- **CA Administrator** - grant the **Manage CA** permission using the Security tab of the Properties dialog box of the certificate server. Used to configure and maintain the CA itself. Users can start and stop certificate server, configure extensions, assign roles, renew CA keys, define key recovery agents, and configure certificate manager restrictions.
- **Certificate Manager -** grant the **Issue and Manage Certificates** permission. Users are responsible for approving certificate enrollment and revocation requests. Different users and groups can be configured with different permissions to different templates. Permissions are configured on the Certificate Managers tab.

Windows Server 2008 R2 Enhancements

- **Certificate Enrollment Web Service -** provides enrollment over HTTP
- **Support for certificate enrollment across forests**
- **Improved support for high volume CAs**

Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service

The web services act as a proxy between a client and a CA. Allows certificate enrollment over the Internet and across forests. The Enterprise CA needs to be running the Enterprise edition of Windows Server 2003, 2008, or 2008 R2. AD forests must have Windows Server 2008 R2 schemas, and all clients need Windows 7.

Certificate Enrollment Across Forests With Two-Way Trusts

Before Windows Server 2008 R2, CAs could only issue certificates to members of the same forest, and each forest had its own PKI. The forest functional level must Windows Server 2003 or greater, and all clients should be running Windows XP or greater. Doesn’t use HTTP.

Support for High-volume CAs

Doesn't store the issued certificates in the database. Certificate revocation is not possible.

Configuring Credential Roaming

Allows for storage of certificates and private keys within the AD. Also allows to remove all user

certificates and keys to be removed when the user logs off. Credential Roaming is supported on Windows XP SP2 or greater, and Windows Server 2003 or greater
Credential Roaming is enabled in User Configuration/Policies/Windows Settings/ Security Settings/Public Key Policies/Certificate Services Client - Credential Roaming
When a user logs on to a client in a domain with Credential Roaming enabled:

- If the certificates in the user's certificate store are up to date, no further action is taken
- If more recent certificates for the user are stored in the AD, they will be copied to the client
- If more recent certificates are storeed in the user's store, the certificates in the AD are updated

Configuring Autoenrollment

Certificate Managers can configure certificate templates in the Certificate Templates snap-in.
Level 1 certificates are supported on Windows 2000 and greater and can't use autoenrollment.
Level 2 certificates are supported on Windows Server 2003
Level 3 certificates are supported on Windows Server 2008 and greater. Level 2 and Level 3 certificates can use autoenrollment.
To configure automatic certificate enrollment, follow these steps:

1. Open the Certificate Templates snap-in
2. Right-click on a template you wish to modify and click Properties.
3. Configure the General, Request Handling, and Issuance Requirements
4. On the certificate's templates Security tab, select the group that you will allow to enroll certificates automatically.

Configuring Group Policy for Autoenrollment

1. Edit the Domain Default Policy GPO
2. User Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Certificates Service Client - Auto-Enrollment
3. Choose Enabled and configure expiration and update settings

- Renew expired certificates, update pending certificates, and remove revoked certificates - reduces the administration workload
- Update certificates that use certificate templates - the issued certificates will be updated if their template is revised or replaced
- Expiration notification - useful when automatic renewal is not configured

Configuring Web Enrollment Support

Supported on Internet Explorer 6 and later. Allows to:

- Request certificates and review existing certificate requests
- Access CRLs
- Perform smart card enrollment

Can be used to issue certificates to users who are not members of an AD domain. Users who don't use IE 6 or later, can request certificates by first creating a Public-Key Cryptography Standards (PKCS) #10 request.
The Certification Authority Web Enrollment role service needs to be added to the server role. If it's installed on a CA, no further configuration is required. If it's installed on a computer without AD CS, specify the CA.
Web Enrollment limitations:

- Only version 1 and 2 certificate templates can be used
- Computer certificates cannot be requested using Web enrollment from a Windows Server 2008 or 2008 R2 CA.

Configuring CRLs

The location of the CRL is included with the corresponding certificate.
The Extensions tab on the Certificate Server's Properties allows to add, remove, and modify the CRL

distribution points. Modifications do not apply retroactively. Only the Certificate Manager role can configure CRLs.
Delta CRLs can be published more frequently. When clients retrieve it, they add it to the cached copy of the full CRL. The Revoked Certificates node on the CA allows to configure the CRL and delta CRL publication intervals. The default CRL publication interval is one week, and one day for the Delta CRL.

Configuring Online Responders

CRL checks cannot be load balanced to another CA.
Online Resonders use Online Certificate Status Protocol (OCSP). Online Responder receives and responds only to requests about the status of individual certificates.
Windows Server 2008 and 2008 R2 features:

- Web proxy caching
- Support for nonce and no-nonce requests - prevent replay attacks. A **nonce** is a unique identifier in an OCSP request
- Advanced cryptography support - can use elliptic curve and SHA-256 cryptography
- Kerberos protocol integration
- Single point or responder array - for load balancing

Microsoft recommends installing the Online Responder service on a separate computer. It can provide revocation status data for certificates issued by one or several CAs. A single CA's revocation data can be distributed across multiple Online Responders. Online Responder is managed through the Online Responder snap-in.

Online Responder requirements

- IIS must already be installed
- An OCSP Response Signing certificate template must be configured on the CA and autoenrollment must be used to issue the certificate to the computer that will host the Online Responder Service. An Online Responder cannot provide status information for a certificate issued form a CA higher in the CA chain than the one that issued its signing certificate.
- The URL for the Online Responder must be included in the Authority Information Access (AIA) extension of the certificates issued by the CA.

Configuring Responder Arrays

One member in an Array is configured as the Array Controller and the rest are array members. To create an Online Responder Array, do the following:

1) Configure the CAs
2) Add the Online Responder service to all servers
3) Add the Online Responders to the array by opening the Online Responder console, selecting the Array Configuration Members node, and using he Add Array Members item.

Network Device Enrollment Service

Allows network devices to obtain certificates based on the Simple Certificate Enrollment Protocol (SCEP).

- Generates and provides one-time enrollment passwords to administrators of network devices
- Submits SCEP enrollment requests on behalf of network devices to a CA
- Retrieves issued certificates from the CA and directs them to the network device

Using Enterprise PKI to monitor CA health

Enterprise PKI is a custom snap-in that shows all certificate servers. Supports Windows Server 2003 and 2008.

- Question Mark - health status is being evaluated

- Green Indicator - CA is problem-free
- Yellow Indicator - CA has a non-critical problem
- Red Indicator - CA has a critical problem
- Red Cross over CA icon - CA is offline

Chapter 4. GPO Strategy

Friday, June 14, 2013
8:11 PM

If a GPO has no User or Computer settings, these unused parts can be disabled. Right-click the GPO in the GPME and disabled unconfigured settings.

Desktop Experience feature

The following features can be enabled after installing the Desktop Experience pack. To install it, use the Add Features dialog.

- Windows Media Player
- Desktop Themes
- Video for Windows (AVI support)
- Windows Slideshow
- Windows Defender
- Disk Cleanup
- Sync Center
- Sound Recorder
- Character Map
- Snipping Tool

Group Policy Tools

- GPOTool - included with Windows Server 2003 Resource Kit. Checks GPOs for consistency on each domain controller.

Chapter 4. Planning Group Policy Objects

Thursday, June 13, 2013
8:41 PM

Windows Server 2007 introduced Starter GPOs, which let you save baseline templates used for creating new GPOs. Starter GPOs can be exported to other domains. All Starter GPOs are stored in SYSVOL *domain*\StarterGPOs

Windows Server 2008 R2 introduced System Starter GPOs, which are read-only Starter GPOs that provide a baseline for specific scenarios. Four System Starter GPOs are created for Windows XP and four are created for Windows Vista, for both user and computer configurations

- Windows XP SP2 EC (Enterprise Client)
- Windows XP SP2 SSLF (Specialized Security Limited Functionality)
- Windows Vista EC (Enterprise Client)
- Windows Vista SSLF (Specialized Security Limited Functionality)

Only Administrative Templates are available in both User and Computer configuration. A new GPO can be created from a Starter GPO by clicking New GPO From Starter GPO. You can also create a new GPO and specify the Source Starter GPO.

Starter GPOs are not backed up when you back up the Group Policy Objects container. Instead, back them up separately. Restore a Starter GPO by right-clicking the Starter GPOs container and clicking Manage Backups.

ADMX files are not stored in individual GPOs. A central store location can be created. Custom ADMX files can be copied to that central store. After you create the central store, the Group Policy tools will use the ADMX files only in the central store, ignoring any locally stored versions.
ADMX language-neutral files - C:\Windows\SYSVOL\domain\policies\PolicyDefinitions
ADMX language-specific files - C:\Windows\SYSVOL\domain\policies\PolicyDefinitions\en-us

Chapter 5. Server Management Technologies

Saturday, June 15, 2013
12:22 PM

Server Manager Console

Not available on Server Core.
ServerManagerCmd.exe is the command-line tool. That can be used to add nad remove features and roles.

- **-query -** display a list of all roles, role services and features
- **-inputPath -** install or removes the roles, role services, or features specified in the answer file
- **-install *<id>* -** install the role, role service, or feature specified by ID.
- **-install *<id>* -allSubFeatures -** install all subfeatures
- **-remove *<id>* -** removes a specific role, role service, or feature
- **-restart -** restart automatically if it's required

OCList.exe and OCSetup.exe can also be used to install roles and features.
ServerManagerCMD.exe is deprecated in favor of Add-WindowsFeature

PowerShell

PowerShell 2.0 is included in Windows Server 2008 R2. It must be downloaded for Windows Server 2008.
To automatically import system modules, right-click the PS ison and choose Import System Modules.
The following modules are included when you install the RSAT console:

- Active Directory (**Import-Module ActiveDirectory**)
- AD RMS and ADRMSAdmin
- AppLocker
- BestPractices
- BitsTransfer
- FailoverCluster
- NetworkLoadBalancingClusters
- PSDIagnostics
- ServerManager (**Import-Module ServerManager**)

Emergency Management Services

Out-of-band connection through a serial or USB port using Telnet or other terminal emulator. Must be enabled on a server on hardware level. The Special Administration Console (SAC) is available if Windows is functioning normally. ISAC console is a subset of commands that are available when the OS is not operating.

Remote Desktop

Remote Desktop Users group on DCs doesn't give a right to log in using RDP. Edit the following policy:
Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/User Rights Assignment -> Log On Through Remote Desktop
RD Gateway works by using RDP over HTTPS.

Remote Server Administration Tools

PowerShell command **Add-WindowsFeature RSAT** if the ServerManager PS module is installed.
RSAT is available as a feature on Windows Server 2008 and 2008 R2 and can be downloaded for

Windows Vista SP1 Business/Enterprise/Ultimate and Windows 7 Pro/Ult/Ent. Windows XP and Server 2003 are not supported.

PowerShell Remoting

Allows executing PS commands against remote computers. Supported on Windows Vista/2008 and higher. To enable it, follow the steps:

1) Start an elevated PS session
2) **Set-Service WinRM -StartupType Automatic**
3) Enable PowerShell remoting **Enable-PSRemoting -force**
4) Use the **Invoke-Command** command.
   Example: **Invoke-Command -script {Import-Module ServerManager; Get-WindowsFeature}**
   -ComputerName DC

Telnet

Tlntadmn.exe can be used to configure Telnet server properties.

Event Logs

An event must exist already in the Event Log before you can attach a task to it.
To view events on a remote computer, enable the firewall exception Remote Event Log Management.
Custom views stored on the remote computer will be unavailable. Local custom views will be run against the remote event logs.

Collector-initiated subscriptions

1) On each source computer, **winrm quickconfig**
2) On each source computer, add the computer account of the collector computer to the Local Administrators or Event Log readers group
3) On the collector computer, **wecutil qc**
4) Open Event Viewer and click Subscriptions -> Create Subscription
5) Select computers and events to collect
6) Configure custom views if you want to view events for individual computers

Source-initiated subscriptions

1) Configure the collector-computer in the same manner
2) Configure source computers by using the Group Policy
   Computer Configuration/Policies/Administrative Templates/Windows Components/Event Forwarding
3) Configure the server address and refresh interval

A collector computer must run at least Windows Server 2003 R2 or Windows Vista
A source computer must run at least Windows XP SP2 or Windows Server 2003 SP1
A computer cannot be both a source and collector

Applications and Service Logs

Introduced in Windows Server 2008.

- **Admin logs -** describe a problem and suggest a solution

- **Operational -** provide information
- **Analytic -** only viewable when enabled. Indicate problems that cannot be solved easily
- **Debug -** used by developers for troubleshooting

Managing Event Logs

Event Logs can be saved to Event Files (*.evtx), XML, Tab-delimited Text, and CSV files.
Only *.evtx files can be opened in Event Viewer on another computer.
Wevtutil has the same functionality as the GUI Event Viewer. Allows to view, filter, and manage event log data from the command line. Can be used to automate log archiving.
PowerShell can also be used to manage event logs. Example:
Get-EventLog System | where {$_.EventID eq 1000 }

Chapter 5. Delegating Authority

Sunday, June 16, 2013
9:59 AM

The Delegation of Control wizard is the best tool to use for a small number of delegations. For large number, use dsacls.exe or PowerShell. Available delegations:

- Create, Delete, and Manage User Accounts
- Reset User Passwords and Force Password Changes at Next Logon
- Read All User Information
- Create, Delete, and Manage Groups
- Modify the Membership of a Group
- Manage Group Policy Links
- Generate Resultant Set of Policy (Planning)
- Generate Resultant Set of Policy (Logging)

The Restore Defaults button in the Advanced Security Settings (accessible after switching to Advanced Mode in AD) of a domain or OU allows to restore the default delegation policies. Another example:
Dsacls "OU=Delegation,DC=Contoso,DC=com" /resetDefaultDACL

Group membership management can be delegated by using the Managed By button in the group properties.

Delegated Authentication

Credential delegation, also known as delegated authentication, allows a computer to impersonate a user for the purposes of gaining access to resources that the user would normally be able to access. Requires the domain and forest functional levels to be set at Windows Server 2008. Delegated authentication occurs when a network service accepts a request from a user and assumes that user's identity to initiate a new connection to another network service.

The Delegation tab becomes available in the Computer's properties. The following options are available:

- Do not trust this computer for delegation
- Trust this computer for delegation to any service (Kerberos only)
- Trust this computer for delegation to specified services only

The computer trusted for delegation must be physically secure. Constrained delegation allows you to select specific services that can be requested through delegation. Domain Administrator accounts should be marked as sensitive and be prohibited from participating in delegation.

Authorization Manager

Provides an authorization model framework for mapplications that have been designed to use Authroization Manager. Can be started by running **azman.msc.** Support authorization stores in SQL Server, AD DS, AD LDS, and XML files. The domain level must be at least Windows Server 2003. Has two modes:

- Developer Mode - allows to create, deploy, and maintain applications, access all AM features, and create new authorization stores
- Administrator Mode - allows to deploy and maintain existing applications

Chapter 6. Presentation Virtualization

Sunday, June 16, 2013
5:32 PM

An RD Session Host provides a remotely accessible desktop to clients. All clients require a special license called RDS CAL. RDS CALs are managed by an RD license server, which uses the RD Licensing role service.

To backup an RD License Server, back up the System State data and the folder where the RD Licensing database is stored. If the server is later rebuilt and restored, unissued licenses will not be restored, and you will need to contact MS. Windows Server 2000 and 2003 TS License servers cannot issue licenses to Windows Server 2008 and 2008 R2. License Server running on Windows Server 2008 R2 can issue licenses for any version of Windows.

License Server Scope

The license server's discovery scope determines which RD Session Host servers and clients can detect the license server automatically. It's configured during the installation of the RD License Server role service.

- **This Workgroup** - not available if the computer is joined to the domain. RDSH and clients in the same workgroup can discover the license server
- **This Domain -** members of the same domain can discover the license server
- **This Forest -** clients and the RDSH can be located anywhere in the forest and can acquire RDS CALs automatically

RDS CALs

- **RDS Per-Device CAL -** gives a specific computer or device the ability to connect to an RDSH server. Per-Device CALs are reclaimed automatically after a random period between 52 and 89 days if the licenses are not used regularly. 20% of issued RDS Per-Device CALs for a specific operating system can be revoked using the RDS Licensing Manager Console.
- **RDS Per-User CAL -** gives a specific user account to connect to an RDSH server from any device. RDS Per-User CALs are not enforced by RD Licensing. The reports node of the RDS Licensing Manager console can be used to generate a report on number of licenses needed.

RDC License Server Activation

The RD License Server must be activated with Microsoft. During the activation process, a Microsoft-issued digital certificate is installed on the RD License Server. The server can be activated automatically using an SSL connection, by navigating to a web page, or by phone. If the License Server is not activated, it can only issue temporary CALs which are valid for 90 days. A License Server can be deactivated using the automatic method or by phone. A deactivated License Server cannot issue RDS Per-Device CALs, but it can still issue RDC Per-User CALs and temporary RDS Per-Device CALs. RD License Server can issue both Per-User and Per-Device CALs

Configuring RD Session Hosts Servers

Administrative Tools -> Remote Desktop Services -> Remote Desktop Session Host Configuration -> RDP-TCP -> Properties

- **General tab** - Security, encryption, and other settings. Security level: RDP Security Level, Negotiate (default), SSL (TLS 1.0). Network Level Authentication is not enabled by default
  Encryption:
  - Low (from client to server - 56-bit key, form server to client - no encryption)
  - Client Compatible (default)
  - High - 128 bits, requires at least RDP 5.2, Windows XP SP2 and higher

    - FIPS Compliant
- **Security tab -** specifies which users and groups can access the RDSH server and what level of control they have - Full Control, User Access, and Guest Access.
- **Sessions tab -** how long an RDSH session will last and how to treat idle and disconnected sessions
- **Remote Control tab -** allows an administrator to control user sessions. Can be set to require user's permission.
- **Network Adapter -** specifies which network adapter to use and the number of simultaneous connections
- **Client Settings -** used to set the maximum color depth, number of monitors to be used, and disable redirection of devices, printers, drives, and clipboard
- **Log on Settings -** whether credentials are requested or automatically provided

Server Properties

- **General tab -** all options are checked by default
    - Delete temporary folders on exit - after the session is complete
    - Use temporary folders per session
    - Restrict each user to a single session
- **User Logon Mode**
    - Allow all connections
    - Allow reconnections but prevent new logons
    - Allow reconnections but prevent new logons until the server is restarted
- **Licensing -** not specified, per device, per user. Allows to add License Servers

RDS Group Policies

Can be used to configure RDP-TCP connection settings and individual RDSH server properties. Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/RD Session Host

RD Web Access

Allows clients to connect to the RDSH server by navigating to its webpage. Clients need to be running at least Windows XP SP2 and Server 2003 SP1. Web Server (IIS) role and Windows Process Activation Service feature are required.

RD Connection Broker

Can work with DNS Round Robin or Network Load Balancing to distribute clients to RDSH servers. When configured with load balancing, the server with the largest amount of free resources is used first. When used with DNS Round Robin, clients are distributed evenly and the RD Connection Broker remembers where a client is connected. A disconnected session is reconnected appropriately, instead of starting a new session. RD connection broker requires Windows Server 2008 or 2008 R2. Clients must support at least RDP 5.2.

You can join an RDSH server to a farm by using the RDS configuration MMC. Specify the address of an RD Connection Broker, a farm name, a load balancing method, and the relative weight of the server based on its resources. More powerful servers should be configured with higher weight. You must also add the RDSH server computer account to the Session Directory Computers local group on the Connection Broker server.

Remote Desktop Virtualization Host

First become available in Windows Server 2008 R2.

Monitoring RDS

Performance Monitor has RDSH server-specific performance counters

- **Terminal Services** counters - active sessions, idle sessions, total sessions
- **Terminal Services Session** counters - various performance counters

Windows System Resource Manager

Can also be used to monitor and allocate resources.
Includes four default policies:

- Equal Per Process
- Equal Per User - useful when multiple sessions are allowed per user
- Equal Per IISAppPool
- Equal Per Session
- Weighted Remote Sessions

Chapter 6. Deploying Applications

Sunday, June 16, 2013
8:39 PM

When you publish an application, it can be installed by using the Add and Remove Programs. The application can also be associated with particular file extensions and then installed when a user opens that type of file.
When you assign an application, the application is installed to the computer the next time the computer boots. When you assign an application to a user, it's installed when the user logs on.

WebDAV

Web Distributed Authroing and Versioning (WebDAV) allows you to publish content through a firewall using HTTP or HTTPS. Can be used to move applications from internal development servers to production servers. WebDAV supports the same authentication methods as IIS. It's a role service in Windows Server 2008 R2, included with IIS Role.

FTP 7.5

FTP 7.5 now supports SSL. You can use IP host address and domain name restrictions to restrict which hosts can upload FTP content.

RDS RemoteApp

If multiple applications are executed from a single server, only one open session is used. RemoteApp applications can be associated with local file extensions. RemoteApp Manager is used to configure remote applications. RD Gateway allows users to access their applications when they are on the Internet.
RemoteApp users need to be members of the Remote Desktop Users group on the RDSH server. If RemoteApp is installed on a DC, modify the Allow Log On Through RDS policy.

Methods of deployment:

- Create an RDP shortcut and distribute it to users
- Create and distribute a Windows Installer package. This allows to associate the RemoteApp with a local file extension
- Get clients to connect to the RD WebAccess website and start the application

App-V

Part of the Microsoft Desktop Optimization Pack (MDOP). Creates a separate partitioned space called a **silo**, and the application executes within that silo. App-V can be used to deploy applications that are not compatible with RDS. Can be deployed using Windows Installer Packages.

MED-V

Allows to use applications in Windows XP Mode. Uses Windows Virtual PC running Windows XP SP3.

Chapter 7. Print Service Management

Wednesday, May 15, 2013
6:43 PM

A line printer remote (LPR) utility lets an application on one computer print to a spooler on a remote computer. The receiving utility is called a line printer daemon (LPD). The LPR/LPD combination was developed for UNIX computers but is widely used for many operating systems. Both utilities are included in Print Services for Unix.

XPS Document format is supported by Microsoft .NET Framework 3.0 in Windows XP/2003 and higher.

Web Services on Devices (WDS) - a set of protocols for accessing and controlling services on network-connected devices.

The View Server permission allows a user to view the print server and is given to Everyone. The Manage Server permission lets users create and delete print queues (with already installed drivers), add or delete ports, and add or delete forms. A Standard user with this permission is called a **delegated print administrator.**
Permissions configured at the printer level override permissions inherited from the print server configuration.

Standard forms cannot be deleted from the Print Management console.

The location of the printer spooler folder can be changed. By default, informational notifications for network printers are shown on remote computers.

Printer filters are used to display only those printers that meet specified criteria. The two default filters are:

- Printers Not Ready
- Printers With Jobs

Group Policy Settings

Computer Configuration/Policies/Administrative Templates/Printers

- Automatically publish new printers in AD
- Allow printers to be published

Chapter 7. File Servers

Wednesday, May 15, 2013
7:46 PM

File permissions override folder permissions.
By default in Windows Server 2008 and 2008 R2, File Sharting is enabled and Public Folder Sharing is disabled.
The default standard shared folder permission in Windows Server 2008 is to grant administrators full access and all other users reas-only access.
The default standard shared folder permission in Windows Server 2008 R2 is all users have read-only access.

Share and Storage Management snap-in is installed by default when you install the File Server role service.
The File Server Resource Manager role service can apply quotas, actively screen files, and generate storage reports.

Shared Folders snap-in allows to create file shares, set permissions, and view and manage open files and users connected to file shares on the computer.

Storage Explorer snap-in allows to view and manage the Fibre Channel and iSCSI fabrics that are available in your SAN. It displays information about servers connected to the SAN, host bus adapters, FC switches, and iSCSI initiators and targets.

Right-click Share and Storage Management and you can manage sessions and open files.
Access-Based Enumeration is enabled by default and lets you hide files and folders from users who do not have access to them.

You can install the old FRS service on Windows Server 2008. Server 2008 R2 uses only DFSR and doesn't allow installation of FRS.
DFSN allows to group shared folders on different servers into one or more logically structured namespaces.
DFSR allows synchronizing folders on multiple servers across LAN or WAN.

Windows Server 2003 File Services role services includes Indexing Service, which was used in earlier versions of Windows. Windows 2008/2008 R2 uses Windows Search Service instead. Windows Search is compatible with Windows Vista/7, and is available for Windows XP with Windows Desktop Search installed.

The default standard shared folder permission in Windows Server 2008 R2 is All Users Have Read-Only Access.
In Windows Server 2008, the default is to grant administrators full control and all other users read-only access.

Services for NFS

Includes Server for NFS and Client for NFS. Improvements in Server 2008 R2:

- Active Directory Lookup - allows Windows -to-Unix account mappings
- Unmapped accounts
- Enhanced server performance - file filter driver reduces file access latencies
- Enhanced UNIX support - including Sun Solaris 9, Red Hat 9, IBM AIX, and HP UX 11i.

File Classification Infrastructure

File classification classifies files based on their business value. Can be used to:

- Identify sensitive data on public servers
- Configure automatic expiration of stale data
- Use custom scripts. For example, move low-business-value files to cheaper storage
- Integrate with thrid-party storage solutions and backup software

Files can be classified:

- Manually
- By LOB applications
- Based on location, owner, content, file size, and extension

Removable Storage

Can be used to track removable storage media and manage the libraries that contain them. Removable Storage labels, catalogs, and tracks media, controls library drives, slots, and doors, and provides drive-cleaning operations. It makes possible sharing the same storage media resources to different programs. It also moves media between media pools to provide the amount of data storage that applications require.
Removed Storage Manager is removed from Windows Server 2008 R2.

Shadow Copies

Uses the Volume Snapshot Driver (volsnap.sys) to create shadow copies. The storage space used for shadow copies is called Diff Area. A snapshot represents the differences between the current content and content from a previous point in time.

Folder Redirection

Configured in Group Policy User Configuration. Enhancements in Server 2008 R2:

- Ability to redirect new folders, such as Contacts, Downloads, Favorites, Links, Music, Saved Games, Searches, and Videos
- Ability to apply settings for redirected folders to clients running earlier versions of Windows
- Option to have the Music, Pictures, and Videos folders follow the Documents folder
- Ability to redirect the Start Menu folder to a specific path for all users

Offline Files

New features and improvements in Server 2008 R2:

- Fast first logon - Windows will synchronize files after the user's logon
- Offline support with background sync
- Exclusion list
- Transparent caching - not enabled by default

BranchCache

A role service that can be installed as a part of File Services server role in Windows Server 2008 R2. Caches content from web and file servers. It supports IPv4, IPv6 and end-to-end encryption with SSL or IPSec. Clients must be running Windows 7 Ultimate or Enterprise and have the BranchCache feature enabled. Servers must be running Windows Server 2008 R2 with the BranchCache for Network Files role service. It can be enabled in shared folders -> Properties -> General -> Offline Settings -> Enable BranchCache. The minimum size of content for BranchCache is 64 KB.

Windows Storage Server 2008 R2

Includes Workgroup, Standard, and Enterprise editions. Provides file deduplication feature and iSCSI functionality. Supports dual-node, highly available storage clusters. Enterprise edition provides

automated two-node failover cluster setup.
Single Instance Storage (SIS) reduces the amount of storage used by data by using logical links to a single source copy. Storage Server enables file access using SMB and NFS protocols. It uses DFS and DFSR to implement a unified namespace and file replication. Can be administered from IE using an ActiveX control and from other clients using a Java Remote Desktop Protocol.

Quotas

Quotas based on a specific template can be updated automatically when you edit the template. Specified quotas can be excluded from the update. Default quota templates:

- **100 MB Limit -** emails the user and administrators if the 100% quota limit has been reached. Makes an entry in the Event Log
- **200 MB Limit Reports to User -** generates a report, sends an email and writes to event log
- **200 MB Limit with 50 MB Extension -** applies the 250 MB Extended Limit tempalte when the user reaches the quota
- **250 MB Extended Limit -** sends an email and logs the event
- **Monitor 200 GB Volume Usage -** can only be applied to a volume. Soft quota
- **Monitor 500 MB Share -** used for monitoring
- New templates based on existing ones can be created

Chapter 8. Security Policies

Wednesday, June 19, 2013
6:34 PM

Auditing Categories

Category	Effect
Account Logon	Logon attempts by a local account on a computer. If the user account is a domain account, the event will also appear on the domain controller
Account management	Records the creation, modification, and deletion of user accounts and groups. Also records password changes and resets
Directory Service Access	Records access to objects in the AD
Logon/Logoff	Attempts to log on to workstations and servers
Object access	Attempts to access files, folders, registry keys, or printers
Policy change	Records any changes to user rights assignment, audit, account, or trust policies
Privilege use	Logs when a user exercises a user right
Process tracking	Records application behavior
System	Records computer system event, such as startup and shutdown, and events that affect system security or the security logs

Audit Policy settings can be configured by using Local Security Settings or Group Policy

Policy Violations

- Creation of user accounts outside of proper process
- Use of administrative privileges without proper authorization
- Use of service accounts for interactive logons
- Deletion of user files
- Execution of unapproved programs
- Attempts to access files to which a user doesn't have permission

Chapter 8. Server Security

Wednesday, June 19, 2013
8:40 PM

WSUS 3.0 SP2 cannot be installed on Server Core.
Requirements:

- IIS 6.0 or later
- Microsoft .NET Framework 2.0 or later
- MMC 3.0
- Microsoft Report Viewer 2008 or later - must be downloaded manually
- Microsoft SQL Server 2005 SP3 or 2008, or Windows Internal Database

The installation of WSUS creates two local groups:

- **WSUS Administrators**
- **WSUS Reporters -** can create reports on the WSUS servers

BITS Peer Caching allows one computer on a local subnet to download an update from a WSUS server and then share it with other compatible clients on the same subnet.

New features in WSUS 3.0 SP2

- The only version of WSUS that can be installed on Windows Server 2008 R2
- Supports Windows 7
- Supports BranchCache
- Auto-approval rules specify the approval deadline
- If you want an update to be installed immediately, set the deadline to a past date

When a downstream server configured in a Replica Mode, all approvals, settings, computers, and groups from the upstream servers are used on the downstream server. The downstream server cannot be used to approve updates.
Autonomous mode allows for a local WSUS administrator to configure update approval settings but still retrieves updates from the upstream server.

WSUS computers can be assigned to multiple groups. With **server-side targeting**, a WSUS administrator can manually move the computers between groups.
Group Policy or registry settings can be used to simplify this process. Computer Configuration / Policies/Administrative Templates/Windows Components/ Windows Updates/**Enable Client-side targeting.**

GPO policies

- Enable Windows Update power management to automatically wake up the system to install updates - only works on Windows Vista and 7.
- No auto-restart with logged-on users for scheduled automatic updates installation - the user is notified that the computer needs to be restarted. If not configured, restart happens 5 minutes after the updates installation
- Reschedule automatic updates scheduled installation - if disabled, the updates will be installed during the next scheduled installation

WSUS Reporting

- **Update Status Summary Report** - shows basic information about update deployment, including the number of computers the update is installed on, needed on, or failed to install on, and for which WSUS has no data.

- **Update Detailed Status** - returns a list of computers and their update status on an update-per-page status
- **Update Tabular Status** - provides data in a table on a per-update basis.
- **Update Tabular Status for Approved Updates** - summary of the update status in a tabular form
- **Computer Status Summary** - provides information on a per-computer basis in a summary form
- **Computer Detailed Status** - provides details about the status of specific updates for a particular computer
- **Computer Tabular Status -** provides a table of update status information with individual computers as rows
- **Synchronization Results**

The Microsoft Baseline Security Analyzer (MBSA) can integrate with WSUS to check whether approved updates are missing from a target computer.
System Center Essentials 2010 can manage up to 50 servers, physical and virtual. Requires Microsoft SQL Server 2008 SP1.

Chapter 9. Remote Access

Thursday, May 16, 2013
6:01 AM

To reset RRAS configuration, type **netsh ras set conf confstandard=disabled & net stop "Routing and Remote Access"** in the command prompt.

When you use DHCP to assign addresses to remote clients, the RAS server will lease blocks of 10 addresses.
DHCP Servers running Windows Server 2008 and 2008 R2 have a predefined user class **Default Routing and Remote Access Class**, which can be used to assign specific options only to RRAS clients.

Authentication

- EAP-TLS requires AD and supports authentication with certificates and smart cards. Not supported on standalone VPN servers.
- MS-CHAPv2 provides mutual authentication and encryption. It's the default protocol
- CHAP provides only authentication using MD5. Doesn't support encryption
- Microsoft Secure Password (EAP MS-CHAPv2) - requires a computer certificate to be installed on the RADIUS server. Client computers should trust the CA that issued the computer certificate. Clients authenticate using domain credentials.

PPTP connections can be authenticated using MS-CHAP, MS-CHAPv2, EAP and PEAP. Uses MPPE for encryption. Provides data confidentiality, but no data integrity or data origin authentication. Often used with non-Microsoft clients.

L2TP connections are encrypted by IPSec. Provides per-packet data origin authentication, data integrity, replay protection, and data confidentiality. Uses computer-level authentication by using certificates and user-level authentication. Deployed when clients have Windows XP.

SSTP - new to Windows Server 2008 and Windows Vista SP1. Encapsulates PPP traffic over HTTPS. Requires that the VPN server has an SSL certificate, which should be trusted by clients. The SSL certificate must be installed on the VPN server before the installation of RRAS. Doesn't support tunneling through web proxies that require authentication and site-to-site tunnels. Can use EAP-TLS and Smart Cards.

IKEv2 - new to Windows Server 2008 R2 and Windows 7. Supports IPv6, VPN Reconnect. Supports PEAP, EAP-MSCHAPv2, smart cards or other certificates. Doesn't support PAP, CHAP, or MS-CHAPv2 (without EAP). Uses UDP port 500. All Windows 7 editions support IKEv2 with VPN Reconnect.

DirectAccess connection methods

Public IPv6 address	Public IPv6 address
Public IPv4 address	6to4
NAT	Teredo
Firewall blocks	IP-HTTPS

1. Only domain-joined computers running Windows 7 Ultimate/Enterprise can use DirectAccess
2. When configuring DirectAccess, add the client's domain computer account to a special security group
3. The client needs a computer certificate from AD CS

4. The server must be a domain member and have Windows Server 2008 R2
5. Two network adapters are required, one of the adapters should have a direct connection to the Internet and be assigned to consecutive public IPv4 addresses.
6. Add the DirectAccess Management Console in Features.
7. The internal Intranet address must have a web server and certificate installed
8. Ensure that all internal network resources available to DirectAccess clients support IPv6.
9. ISATAP can be used to tunnel IPv6 traffic from intranet resources over an IPv4 intranet
10. NAT-PT device allows hosts that support only IPv4 addresses to be accessible to DirectAccess clients using IPv6.
11. Firewall ports on intranet resources:
    - Echo-Request - ICMPv6-in
    - Echo-Request - ICMPv6-out
12. Firewall ports on the external firewall:
    - UDP port 3544 - Teredo
    - IPv4 protocol 41 - 6to4 traffic
    - TCP port 443 - IP-HTTPS traffic
    - IPv4 protocol 50 - ESP traffic

If a RADIUS server is used to centralize remote access policies management, it must be a member of the domain. RADIUS clients can be standalone computers.

NPS Accounting data can be recorded to a SQL Server 2005 SP1, 2008, or 2008 R2 database.

RD Gateway Server

1. Install the RD Gateway Role Service in the DMZ. RD Gateway uses port 443.
2. Obtain an SSL certificate, which must match the name that clients use to connect to the server. Use the RD Gateway Manager to map the certificate.
3. Configure RD Connection Authorization Policies and RD Resource Authorization Policies

Connection Authorization Policies

RD-CAPs specify which users are allowed to connect through the RD Gateway server. Usually done with groups, which can include computer and user accounts. RD-CAPs also specify whether remote clients can use password or smartcard authentication. RD-CAPs can be used in conjunction with NAP.

Resource Authorization Policies

RD-RAPs specify which resources on the internal network are accessible to the RD Gateway clients. You can specify a group of computers that you want to grant access to and the group pf users that you will allow this access to. To be granted access to internal resources, a remote user must meet conditions of at least one RD-CAP and at least one RD-RAP.

Chapter 9. Firewalls and NAP

Thursday, May 16, 2013
5:54 PM

Domain Isolation connection security rule forces domain member computers to accept incoming communication requests only from domain computers. Isolated computers can initiate communication with external hosts. Server Isolation connection security rule applies to servers.

System Health Agents (SHAs) and System Health Validators (SHVs) validate a computers' health against a configured set of benchmarks. The SHV specifies which benchmarks the computer must meet. SHA components are installed on all clients, and SHV on a computer running NPS.
An Enforcement Client (EC) enforces limited network access for non-compliant computers.
Most NAP Enforcements require Windows XP SP3 and later.

IPSec NAP Enforcement works by applying IPSec rules. It can be applied on a per-IP address, per-TCP port number, or per-UDP port number basis. For example, only healthy computers can manage a web server, but all other computers can view web pages. The network must have a Windows Server 2008 or 2008 R2 Health Registration Authority and a Windows Server 2008 or 2008 R2 CA. Clientd mudt be running at least Windows XP SP3

802.1x NAP Enforcement uses Ethernet switches or WAPs by applying IP packet filters or VLANs. The health status of clients is assessed constantly.

VPN NAP Enforcement is used on VPN clients. Uses packet filters. Health status of connected clients monitored continuously.

DHCP NAP Enforcement is only applied when a client lease is obtained or renewed. DHCP Server must be running Windows Server 2008 or 2008 R2.

RD Gateway NAP Enforcement - only for Windows Vista/2008 and later clients. Clients connecting to an RD Gateway must meet health requirements before the RD Gateway allows connection to RDP servers on the internal network.

1. Enable NAP health policy checking on the RD Gateway server by configuring the RD Gateway server to request the clients to send a statement of health.
2. Remove any existing RD-CAPs
3. Edit the properties of the Windows SHV in the NPS console on the RD Gateway Server.
4. Create NAP Policies on the RD Gateway Server using the Configure NAP Wizard. Two health policies need to be created - one for compliant and one for noncompliant computers
5. Create a connection request policy
6. Create three network policies for compliant, noncompliant, and non-NAP-capable computers

DirectAccess NAP Enforcement - similar to IPSec NAP Enforcement. Configure DirectAccess server GPO to require health certificates.

Chapter 10. Provisioning Data

Friday, June 21, 2013
5:59 PM

RAID 1+0 - a stripe of mirrors - create mirrored sets and then stripe data across them
RAID 0+1 - a mirror of stripes - create a strpied set across multiple disks and then use the same amount of disks to mirror that content

You can create a DFS namespace when installing the DFS Management role service. Windows Server 2008 Standard only supports one namespace, while Enterprise and Datacenter editions support multiple.

- **Domain namespace** uses a domain as its namespace root, such as \\contoso.com\shares\
  Can be hosted on multiple servers, and its metadata is stored in the AD.
- **Standalone namespace** uses a namespace server as its namespace root, such as \\Server1\Shares.
  Hosted on only one server, but can be hosted on a failover cluster to increase availability.

Namespace Modes

- Windows 2000 Namespace mode
- Windows 2008 Namespace mode - supports access-based enumeration, can contain up to 5,000 DFS folders. The domain needs to be at least at Windows Server 2008 functional level, the forest needs to be at least at Windows Server 2003 functional level, and all namespace servers should run at least Windows Server 2008. To enable ABE, edit the Properties of a namespace -> Advanced -> Enable ABE

Target Priority

A referral is an ordered list of targets that a client receives from a domain controller or namespace server when a user accesses a namespace root or any folder. Targets can be reordered by setting target priorities.
Expand the namespace in the DFS Management console, click the relevant folder, right-click the folder target and click Properties. Choose one of the following:

- **First among all targets -** users are always referred to this target if it's available
- **Last among all targets -** users are never referred to this target unless all other targets are unavailable
- **First among targets of equal cost**
- **Last among targets of equal cost**

DFS Replication

The New Replication Group Wizard in the DFS Management console can be used to create a replication group. The New Member Wizard adds a member. The New Replicated Folder Wizard adds a replicated folder to a replication group.
Replication filters can be configured to exempt certain file types from replication.
Replication topologies can be cnfigured in the DFS Management Console. Right-click the replication group and then click New Topology:

- **Hub and Spoke -** requires three or more members. For each spoke, choose a required hub member and an optional second hub member for redundancy. When two hubs are specified, they have they have a full-mesh topology between them.
- **Full-mesh -** every member replicates with all other members. Works when there are less than 10 members in the replication group.

Offline Data Access

The default setting is **Only the files and programs that users specify are available offline.** When this option is selected, you can enable BranchCache.
To change Indexing options on a server, open the Indexing Options in the Control Panel. You can choose whether to index encrypted files, indexed file types, and location of the index.

Chapter 10. Storage

Friday, June 21, 2013
8:06 PM

The **Provision Storage Wizard** in the Storage Manager for SANs console, allows you to create a LUN on a Fibre Channel or iSCSI disk storage subsystem. The storage subsystem must support Virtual Disk Service (VDS) and you need to install the VDS hardware provider for the storage subsystem.
The LUN size can be extended using the Storage Manager for SANs. When you unassign a LUN, you make the LUN invisible to the server or cluster but retain the data stored in the LUN.
VDS allows to manage SANs without using tools provided by the hardware vendor.

Storage Manager for SANs

Installed as a feature in Windows Server 2008 and 2008 R2. Includes three nodes:

- **LUN Management -** lists all LUNs created with Storage Manager. Allows to create new LUNs, extend the size of existing LUNs, assign and unassign LUNs, and delete LUNs. Can also be used to configure iSCSI and FC connections
- **Subsystems -** lists all of the Storage subsystems discovered within the SAN environment
- **Drives -** lists all the drives in the storage subsystems. You can identify drives that you are working with by making the drive light blink.

FC LUNs are assigned directly to a server or cluster
iSCSI LUNs are assigned to logical entities called targets. An iSCSI Initiator is used to connect to a target. iSCSI Initiators can use one or more network adapters.

MPIO

Path Failover times can be configured through the Microsoft iSCSI Initiator driver or by modifying the Fibre Channel HBA driver parameter settings. MPIO load balancing features:

- **Failover -** no load balancing is performed. Specify a primary path and a group of standby paths.
- **Failback -** same as failover, but I/O will switch back to the preferred path automatically when it's available
- **Round-robin -** all available paths are used
- **Round-robin with a subset of paths -** a set of preferred paths is specified for I/O and a set of standby paths is specified for failover. The set of preferred paths will be used until all paths fail.
- **Dynamic Least Queue Depth -** I/O is directed to a path with the least number of outstanding requests
- **Weighted Path -** each path is assigned a weight. The path with the least weight is chose for I/O

Storage Explorer

Used to manage iSCSI and FC fabrics on the SAN. Can display detailed information about servers that are connected to the SAN, host bus adapters, FC switches, iSCSI Initiators, and iSCSI targets. Can be used to configure iSCSI security, iSCSI target portals, add iSNS servers, and manage Discovery Domains. To view and manage an iSCSI fabric, enable the WMI exception in Windows Firewall on each server that is a part of the fabric.

Chapter 11. DNS Round Robin and NLB

Saturday, June 22, 2013
9:28 AM

Both DNS Round Robin and NLB are supported on all editions of Windows Server 2008 and 2008 R2. These technologies require that the content on both servers is the same. DNS Round Robin and NLB cannot be used with file servers.

DNS Round Robin

Provides different IP responses from a DNS Server to requests with the same host name. The capacity for the number of servers is almost unlimited. DNS Round Robin is not aware when one of the member servers fails. Can be used with non-Microsoft operating systems. Configure a short TTL on DNS host records to quickly update DNS records if a server fails. DNS Round Robin is not session friendly. When a server TTL expires, client with an established session can start using another server that doesn't have the session information.

Netmask Ordering

Takes the client's IP address into account when providing a response. Will try to return the IP address on the same subnet. If the querying client is not on same subnet as any of the DNS Round Robin records, the Round-Robin process functions as normal. DNS Round Robin and Netmask Ordering are enabled by default.

Creating DNS Round Robin Entries

Create multiple A or AAAA records associated with the same host name. Example:

```
Dnscmd /RecordAdd Contoso.com www A 10.10.111.111
Dnscmd /RecordAdd Contoso.com www A 10.10.111.222
```

Network Load Balancing

When an NLB Cluster is created, it creates a virtual network address and adapter, with traffic to this address distributed across a number of hosts. Windows Server 2008 R2 supports up to 32 nodes, but no more than 8 is recommended. Build mutiple clusters with 8 nodes each and then use DNS Round Robin. NLB automatically reconfigures as nodes join or fail out of the cluster. You can add or remove nodes through the NLB Manager uinterface or by using command line. It's possible to use different operating systems with NLB clusters.

Servers within an NLB cluster constantly communicate with each other. This process is known as heartbeat and convergence. The heartbeat is sent every second to all nodes. If a cluster node fails to transmit five consecutive heartbeats, the cluster reconfigures itself through a convergence process. Convergence can be triggered by the changes in network, hosts returning online,or manually by adding or removing nodes from a cluster. It also happens when port rules are modified.

Cluster Operation Mode

All servers within a cluster must operate in the same mode.

- **NLB Unicast Mode -** the MAC address of the virtual network adapter is shared among the participants within the cluster. If the cluster nodes have only one NIC, this virtual MAC address replaces the physical MAC address and the server will respond to network traffic sent to the virtual address. The server still retains its original IP address, but it will resolve to the virtual MAC address. You can still connect to the server's original IP address if you are on the same subnet. If two NICs are installed on each node, one NIC participates in the cluster, and the second is used for management and inter-server communication.

- **NLB Multicast Mode -** more suitable for servers with one NIC. The server retains its original MAC address in addition to the virtual address. Network devices such as switches and routers must support multicast MAC addressing. Can be used for management from remote subnets.
- **IGMP Multicast Mode -** enhances network performance by limiting switch flooding. Enabling IGMP support means that multicast traffic passes through only switch ports that service the NLB cluster. The switch hardware must support IGMP.

Managing NLB Clusters

User the NLB Manager console in Administrative Tools. Use the console to alter port rules, change cluster operation mode, add or remove hosts, block incoming connections on a node, and stop and start the NLB cluster.

- **Start -** start a cluster node that has been stopped
- **Stop -** stop a cluster node and terminate any active connections
- **Drainstop -** stop a cluster node from receiving new connections but maintain existing connections
- **Suspend -** pause the cluster node
- **Resume -** resume the cluster node after it has been suspended

NLB Port Rules

Allows to control how NLB Clusters deal with traffic to a specific port. Created on the Port Rules tab of the Cluster Properties dialog box. When port rules are configured on a cluster level, all nodes are configured automatically. A node will be unable to join a cluster if it has different port rules. The default port rule is to redirect all traffic in a balanced way to all nodes.

To create a port rule,
NLB Console -> right-click the cluster -> Cluster Properties -> Port Rules -> Add
When creating a cistom port rule, choose a filtering mode. It allows to specify whether only one node, some nodes, or all nodes respond to requests from a single client during the session. Some applications require that all session traffic occurs only between a single host and the client.

- **Single Host -** a single node handles all traffic sent to the cluster matching the port rule
- **Disable port range -** configures the cluster not to respond to traffic on specific ports
- **Multiple Host Filtering -** allows traffic to be redirected to several nodes in the cluster. Affinity settings:
    - **None -** all requests are distributed equally across the cluster, even if a client has an established session
    - **Network -** similar to netmask ordering. Directs clients to the closest node
    - **Single -** after a client established a session, all subsequent requests in the session will be directed to the same node in the cluster. This is the default filtering mode on port rules.

Chapter 11. Clustering

Saturday, June 22, 2013
11:17 AM

Failover Clustering is only available on Windows Server 2008 and 2008 R2 Enterprise and Datacenter Editions.
Supports two types of applications:

- **Single-instance application -** can run on only one server at a time. The application is operating on one node, while the other nodes are standby.
- **Multiple-instance application -** applications can share data between different nodes. Examples - database and email servers.

Application requirements to run on a cluster

- The cluster application must use an IP-based protocol
- Application must allow you to configure where its data is stored, ie local disks or SAN
- Application must be able to reestablish the failed sessions after a failover

Cluster Requirements

- If Windows Server 2008 is used, the same processor architecture (x86 or x64) is required
- Unlike Windows Server 2003, Server 2008 and Server 2008 R2 no longer support direct SCSI connections to shared storage. Only FC, SAS and iSCSI are supported.
- All servers must be members of the same domain and be running the same operating system

Cluster Quorum Models

Quorum determines the number of failures a cluster can tolerate before it stops running. It exists as a database in the registry and is maintained on the winess disk or witness share. The witness disk or share keeps a copy of this configuration so that servers can join the cluster at any time. One server manages the quorum data, but all other servers have a copy.
Four quorum models:

- **Node Majority -** suits failover cluster deployments with odd number of cluster nodes. A Node Majority cluster retains quorum if the number of available nodes exceeds the number of failed nodes. Example: if four nodes in a seven-node cluster fail, the cluster will shut down.
- **Node and Disk Majority -** suits clusters with even number of cluster nodes. As long as the witness disk is available, the cluster keeps running even if up to half of its nodes fail. In the case of a witness disk failure, a majority of the nodes needs to keep running for the cluster to keep running.
- **Node and File Share Majority -** similar to the Node and Disk Majority model but the quorum is stored on a network share.
- **No Majority: Disk Only -** not recommended in production because the disk becomes a single point of failure. The cluster can sustain if all but one node fails as long as the quorum is available. If the quorum fails, the cluster fails even if all of its nodes are still running.

The Create Cluster Wizard wil lsuggest the most appropriate configuration.

Failover Cluster Validation

1) Validate the configuration of all computers by using the Validate A Configuration Wizard
    - **Cluster Configuration -** checks that the cluster-level components are compatible with the proposed configuration
    - **Inventory Test -** creates an inventory of components and settings in the node
    - **Network Test -** ensures that network settings are appropriate for cluster
    - **Storage Test -** ensures that storage is compatible with clustering

- **System Configuration Test -** validates system settings across servers

2) Remove all SPOFs, or you will receive a warning
3) Parallel SCSI cannot be used for storage. NTFS is recommended for cluster partitions. NTFS is required for the witness disk

Creating a Failover Cluster

1) **Add-WindowFeature Failover-Clustering**
2) Administrative Tools -> Failover Cluster Manager -> Create Cluster Wizard
3) Select servers used for clustering. The wizard wil suggest the most appropriate quorum configuration
4) Choose whether to run validation checks
5) In the Access Point for Administering the Cluster dialog box, enter a cluster name and an IP address

Configuring Servers for High Availability

1. Use the High Availability Wizard to configure services and applications for HA. Failover Cluster Manager -> Actions -> Configure a Service or Application. Services that support HA:
   - **DFS Namespace server**
   - **DHCP Server**
   - **Distributed Transaction Coordinator -** provides support for distributed applications that are used to perform transactions
   - **File Server**
   - **Internet Storage Name Servers (iSNS) -** provides a directory of iSCSI targets
   - **Message Queuing -** used by distributed applications for messaging
   - **Print Server**
   - **Remote Desktop Connection Broker**
   - **Hyper-V**
   - **WINS Server**
2. On the Client Access Point Page, specify the address that clients will use to access the highly available service
3. On the Select Storage page, select the storage volumes that will be assigned to the service

Managing a Failover Cluster

Cluster.exe command can be used to manage clusters from the command line.
Failover Cluster Manager console can be used to:

- Pause and resume nodes
- Take the server or application offline for maintenance
- Bring the server or application online
- Move the service or application to another cluster node - perform maintenance on the passive node first, then transfer the application to the passive node, and perform maintenance on the previously active node

Chapter 12. Performance.

Thursday, May 16, 2013
7:15 PM

Performance Monitor Properties

In Performance Monitor, each line on the graph appears in different colors. To maker it easier to see, select it and press Ctrl+H.

- **General -** how frequently the graph updates, sample duration, and what data is shown on the graph
- **Source -** whether to display current activity, or load it from a log file
- **Data -** add and remove counters, adjust their appearance
- **Graph -** change the graph view (line, histogram, or report), adjust scales, whether to show grids, and whether the graph can be scrolled or wrapped
- **Appearance -** change graph background, fonts, and borders

Data Collector Sets

Data Collector Sets (DCSs) gather system information, including configuration settings and performance data. You can use Performance Monitor to examine the data, or generate a report with summary.
Built-in DCSs:

- **System Performance** - logs processor, disk, memory, and network performance counters. 10 minutes by default.
- **System Diagnostics** - used for troubleshooting reliability problems, such as problematic hardware, driver failures, or STOP errors. Logs all the information included in the System Performance DCS, plus detailed system information. 1 minute by default.
- **Active Directory Diagnostics** - available only on DCs. 5 minutes by default.

After running a DCSs, summary of the collected data is available in Performance Monitor Reports node. The most recent report is available when you click Latest Report.
DCSs can be used to monitor performance counters, creating an alert when a certain condition occurs. Alerts can start a batch file, send an email or call on a pager.

Creating a Custom DCS

1. Performance Monitor -> Data Collector Sets -> right-click User Defined -> New -> Data Collector Set
2. Specify a name and choose whether to create a DCS from a template or create manually
3. Choose which template to use (AD Diagnostics, Basic, System Performance, or System Diagnostics)
4. Specify where to save the data
5. Select one of the options and click Finish:
    - Open properties for this DCS
    - Start this DCS now
    - Save and close
6. You can start a DCS manually, or start and stop it on schedule

Types of Data Collectors

To add a Data Collector to a DCS, right-click it and choose one of the following:

1) **Performance Counter Data Collector -** collects performance statistics. Useful to set baselines and analyze trends
2) **Event Trace Data Collector -** enables to collect information about system events and activities
3) **Configuration Data Collector -** stores information about registry keys, and the system state
4) **Performance Counter Alert -** enables to configure an alert when a performance counter exceeds

or drops below a specified value

Command Prompt tools

- **Logman create counter -** creates a Performance Counter data collector
- **Logman create trace -** creates an Event Trace data collector
- **Logman create config -** creates a Configuration Data collector
- **Logman create alert -** creates an Alert Data collector
- **Perfmon /report -** generates and displays an up-to-date system diagnostic report
- **Perfmon /rel -** opens Reliability Monitor

Kernel paged memory - the amount of virtual memory the kernel is using
Kernel nonpaged memory - the amount of RAM used by the kernel

Reliability Monitor

Measure the compuer's reliability over 28 days. The hidden RACTask must be enabled before data collection begins. Can be opened by running **perfmon /rel.** The stability index is only calculated when the computer is on. Until Reliability Monitor has 28 days, the line will be dotted. Reliability Monitor maintains up to a year worth of data. Software updates and service packs may reduce the stability index if a restart is required.
An information icon indicates a successful event. A warning icon indicates a failure.

Application Log events can be Error, Warning, and Information.
System Log events can be Critical, Error, Warning, and Information.

Chapter 13. Backups

Sunday, June 23, 2013
3:55 PM

Shadow Copies

To enable Shadow Copies of Shared Folders, open Computer Management, right-click Shared Folders node -> All Tasks -> Configure Shadow Copies. Shadow Copies are configured on a per-volume basis. The default schedule is to make shadow copies every weekday at 7:00 AM and 12:00 PM. The Settings button allows configuring schedule, where the shadow copies are stored, and the maximum size of shadow copies. Maximum of 64 shadow copies can be stored.

Windows Server Backup in Server 2008

- Cannot write to tape drives
- Cannot write to network locations or optical media during a scheduled backup
- The smallest object you can back up is a volume
- Only local NTFS volumes can be backed up

Windows Server Backup in Server 2008 R2

- The ability to back up or exclude individual files, file types, and folders
- Older incremental backups are automatically deleted
- Scheduled backups can be stored on a network share (but only one version), or volume

When another volume is used for scheduled backups, all data from it will be removed and the volume will be hidden from the OS. A volume can store up to 512 backups. If removable media is used for a backup, it's possible to span the backup across multiple DVDs. Only manual backups can be saved on DVDs.

By default, scheduled backups occur at 9:00 PM. Only Administrators can manage scheduled backups. The VSS Settings tab allows to configure VSS Full Backup and VSS Copy Backup. If multiple destination volumes for scheduled backups are selected, multiple copies of the backup data will be written.

WBAdmin tool

Available on both the standard and Server Core installations. The Windows Server Backup console is not available in Server Core.

- **Wbadmin enable backup -** allows to create and manage scheduled backups
    - **Include** - specify multiple files, folders, or volumes
    - **Exclude -** specify the comma-delimited list of items to exclude
    - **SystemState -** add the System State backup
    - **vssFull | vssCopy**
    - **User -** specify the user name
    - **Password -** specify the password
- **Wbadmin start systemstatebackup -** manual system state backup
- **Wbadmin start backup -** start a single manual backup. If no backup parameters are specified, it uses the settings configured for scheduled backups
- **Wbadmin get versions -** view details of backups
- **Wbadmin get items -** view what is contained in a backup
- -**backuptarget:\\Share\Folder -** save a backup to a share
- **-quiet -** won't wait for a user's input

Examples:

Wbadmin start backup -backuptarget:\\BackupServer\Share -include:E:,F:,G: -user:Admin@contoso.com -password:P@ssword

Use Scheduled Tasks with *.bat files to schedule network backups in Server 2008. The scheduled task must be run using the local Administrator account.
Windows Server 2008 and 2008 R2 can be used to backup computers remotely. Wbadmin cannot bse used to manage backups of remote computers.
Backup Operators cannot schedule backups. They can only perform unscheduled backups.

System Center Data Protection Manager

- Protection for Windows clients, even if they are offline
- Users can restore their own data using Windows Explorer or Microsoft Office
- DBAs can restore their databases through a self-service restore utility
- Byte-level backups reduce the amount of space needed
- Point-in-time database backups provide zero data loss restoration of Exchange, SQL Servers, and Sharepoint
- Supports backups to FC and iSCSI SANs

Chapter 13. Disaster Recovery

Sunday, June 23, 2013
6:17 PM

Even if a backup was taken at the volume level, you can restore individual files and folders.

When you do an application recovery, you have the option of rolling forward the application database. This option enables a full recovery of the database by first restoring it from a backup and then running transaction logs. The roll-forward option is only available when you perform a restore from the most recent backup.

The Operating System Recovery is similar to Full Server Recovery, but only critical volumes are recovered. Use the Windows Complete PC Restore option in System Recovery Options to do the recovery. Clicking the Advanced button allows to install drivers for other storage devices and search for backups on the network.

System State Recovery

1) **Wbadmin get versions -** note the backup version identifier
2) **Wbadmin start SystemStateRecovery -version:MM/DD/YYYT-HH:MM**
3) Reboot the server when the process completes

Recovering Active Directory

AD is recovered non-authoritatively when you recover system state data on a DC. It also recovers server roles and role services. Authoritative restores are not necessary when there is only one domain controller. To reboot into DSRM, type the command: **bcdedit /set safeboot dsrepair.** When finished, type **bcdedit /deletevalue safeboot.** Also, MSConfig can be used to boot into DSRM.
PowerShell command **Restore-DOBject** can be used to recover deleted objects.

Resetting the DSRM Password

1. Log in to a DC as the domain admin
2. **Ntdsutil**
3. **Set dsrm password**
4. At the Reset DSRM password command prompt, do one of the following:
    - **Reset password on server null -** if resetting the password on the local DC
    - **Reset password on server *servername*** - if resetting the password on another DC
5. Press **q** twice to exist

Authoritative Restore

When the system state recovery is complete, use the **ntdsutil** to enter Authoritative Restore Mode. To restore an object, type **Restore Object,** and then the object's DN. To restore a container and everything located under it, type **Restore Subtree** and then the container's DN. After restoring the container, you need to restore all objects in contained.
If you want to perform an authoritative restore of SYSVOL, perform the system state recovery with the **-AuthSYSVOL** option. Deleted GPOs must be recovered using the GPMC -> Manage Backups

AD DS Database Mounting Tool

The Dsadmin.exe tool enables to create and view data stored within AD DS without needing to restart the DC in DSRM. It can be used to compare the state of AD DS as it exists in different snapshots. Use the **ntdsutil** to mount the snapshot and then use **dsadmin** to view and modify the snapshot.

Introducing Windows Server 2008 R2

Tuesday, June 25, 2013
7:40 PM

System Center Data Protection Manager (DPM 2010) provides ability to back up to tape.

Microsoft .Net Framework 3.5.1 is required to support AD Web Services. ADWS is needed for PowerShell and ADAC. ADWS uses port TCP 9389.
.Net Framework 3.5.1 can run on Server Core in Windows Server 2008 R2.

If the forest functional level is set to Windows Server 2008, you can raise the domain functional level to Windows Server 2008 R2 and then lower it back down to Windows Server 2008.

Adprep /forestprep must be run on the schema master role
Adprep /domainprep must be run on the infrastructure operations master role

Raise the domain functional level on a PDC. Raise the forest functional level on
The schema master.

MDOP

Tuesday, June 25, 2013
7:47 PM

MDOP includes:

- App-V
- MED-V - Windows XP Mode plus control and management features. Can also customize and automate setting up VMs. Requires no dedicated infrastructure or management servers.
- Advanced Group Policy Management - provides accounting and auditing. Change management, and version control. Check out a GPO out of the archive, change it, and check it back into the archive. GPO Administrators can have one of the three roles:
    - Reviewer - can view and compare GPOs, but cannot edit or deploy
    - Editor - can edit, but cannot deploy. Affect only the archive, not production GPOs.
    - Approver - can review and approve
- Microsoft BitLocker Administration and Monitoring - used for Bitlocker andf Bitlocker To Go
- Diagnostic and Recovery Toolset (DaRT) - used for troubleshooting. Can edit registry, reset local account passwords, analyze crash dumps, recover deleted files, repair volumes, MBR, or partitions, wipe disks, uninstall hotfixes, remove spyware and rootkits.
  Provides the following tools: System Information, Autoruns, Event Viewer, Disk Management, Services and Drivers, TCP/IP Config, SFC Scan, Standalone System Sweeper.
- Asset Inventory System - provides comprehensive view of an organization's desktop software environment. Shows how many copies of an application are installed, where they are installed, and whether you need to increase or decrease the number of licenses.

Other notes

Wednesday, June 26, 2013
7:27 PM

Credential roaming - allows to sycnhronize certificates and provate keys on a local computer with the AD DS. Certificates are erased when the user logs off.

Server Core supports the following roles:
- AD Certificate Services
- AD Domain Services
- AD LDS
- BranchCache Hosted Cache
- DNS
- DHCP
- File Services
- Hyper-V
- Print and Media Services
- Streaming Media Services
- IIS

Server Core supports these features:
- Failover Clustering
- Multipath I/O
- Network Load Balancing
- Quality of Service
- Removable Storage Management
- SNMP
- Telnet client
- Windows BitLocker Drive Encryption
- Windows Powershell
- Windows Server Backup