Windows Server 2008 Active Directory Feature Components

Acronyms

Legend

Information, Important, Information Bullet, User, User Groups, Service Account, Client(s), User Tokens, User Application Wizard, User Credentials Cache, Microsoft Office Outlook User, Active Directory Object, Computer Credentials Cache, Password Replication Policy, Central Store, Group Policy, Firewall, Active Directory Forest, Replication Mechanism, Internet, RMS Protected Content, Restartable DS, RODC, Server/Client Tools, AD LDS Server, AD LDS Instance, Web Server, Web Server Farm, Domain Controller, DHCP Server, Federation Server, BitLocker, AD RMS Server, SQL Server

---

Active Directory Lightweight Directory Services
Product Scenario: Enterprise and Branch Office
Windows Server 2008

Active Directory Lightweight Directory Services (AD LDS) provides directory services for directory-enabled applications. AD LDS does not require or rely on Active Directory domains or forests. AD LDS was previously known as Active Directory Application Mode (ADAM).

AD LDS Usage Scenarios
- Application-Specific Directory Services Scenarios
- Application Development Scenarios
- Extranet Access Management
- X.500/LDAP Directory Store
- Deployment in Datacenters & Perimeter Networks (Branch Offices, DMZs)

AD LDS Tools
- ADSchemaAnalyzer – Helps migrate the AD schema to AD LDS, from one AD LDS instance to another, or from any LDAP-compliant directory to an AD LDS instance
- AD LDS Synchronizer – Command-line tool that synchronizes data from an AD forest to an instance set of an AD LDS instance
- Snapshot Browser – Uses LDAP client to bind to VSS snapshot (taken by NTDSUTIL) and view read-only instance of AD LDS database
- Active Directory Sites and Services – Assists in administrating AD LDS replication topology
- Install from Media (IFM) – IFM can also be used to install an AD LDS instance from backup media

AD LDS Users and Groups
- AD LDS authenticates the identity of users, who are represented by AD LDS user objects
- AD LDS allows the use of Windows Security principals from the local machine and AD for access control. Authentication process for these user principals is redirected to the local machine and AD respectively
- Four default groups: Administrators, Instances, Readers, and Users

AD LDS Platform Support
- AD LDS is a Windows Server 2008 role

AD LDS Access Control
- Uses ACLs on directory objects to determine which objects user can access

AD LDS Replication
- A configuration set is a group of AD LDS instances that replicate data with each other
- A single server machine can run multiple AD LDS instances
- One AD LDS instance can belong to just one configuration set

---

Active Directory Federation Services
Product Scenario: Security and Policy Enforcement
Windows Server 2008

Active Directory Federation Services (AD FS) provides Web single sign-on (SSO) technologies to authenticate a user to multiple Web applications over the life of a single online session. AD FS securely shares digital identity and entitlement rights, or "claims," across security and enterprise boundaries.

Federation Scenarios

Federated Web SSO with Forest Trust — Forests located in the DMZ and internal network. A federation trust is established so accounts in internal forest can access Web-based applications in perimeter network (including intranet or Internet access).

Web SSO — Users must authenticate only once to access multiple Web-based applications. All users are external, and no federation trust exists.

Federated Web SSO — Federation trust relationship established between two businesses. FS routes authentication requests from user accounts in "adatum" to Web-based applications that are located in the "treyresearch" network.

AD FS Authentication Flow

adatum.com (Account Forest)
- Authenticate users
- Map attributes

treyresearch.net (Resource Forest)
- Generate token based upon policies in federation server

1. Client tries to access Web application in treyresearch.net. Web server requests token for access.
2. Client redirect to Federation Server on treyresearch.net. Federation server has list of partners that have access to the Web application. Refers client to its adatum.com Federation Server.
3. Instruct client to get a token from adatum.com Federation Server.
4. Client is member of its domain. Presents user authentication data to adatum.com Federation Server.
5. Based on authentication, SAML token generated for client.
6. User obtains SAML token from adatum.com Federation Server for treyresearch.net Federation Server.
7. Redirects client to treyresearch.net Federation Server for claims management.
8. Based on policies for the claims presented by the adatum.com token, a treyresearch.net token for the Web application is generated for the client.
9. The treyresearch.net token is delivered to client.
10. Client can now present treyresearch.net token to Web server to gain access to the application.

- Security tokens assert claims
- Claims – Statements authorities make about security principals (e.g., name, identity, key, group, privilege, capability)

Active Directory Rights Management Services
Product Scenario: Security and Policy Enforcement
Windows Server 2008

Active Directory Rights Management Services (AD RMS) is information protection technology that works with AD RMS-enabled applications to safeguard digital information from unauthorized use – both online and offline – inside and outside of your organization's firewall.

Configuration Database stores:
- Data needed to manage account certification, licensing & publishing
- Primary key pairs for secure rights management

- Software-based key protection is the default for AD RMS. For added protection, AD RMS can store its keys in a hardware security module.

AD RMS Server
- License AD RMS-protected content
- Enroll servers and users
- Administer AD RMS functions

1. Author uses AD RMS for the first time - receives Rights Account Certificate (RAC) and Client Licensor Certificate (CLC). Happens once and enables user to publish online or offline and consume rights-protected content.
2. Using AD RMS-enabled application, author creates file and specifies user rights. Policy license containing user policies is generated.
3. Application generates content key, encrypts content with it. Online Publish – Encrypts content key with AD RMS server public key and sends to AD RMS server. Server creates and signs publishing license (PL). Offline Publish – Encrypts content key with CLC public key, encrypts copy of key with AD RMS server public key. Creates PL and signs with CLC private key. Append PL to encrypted content.
4. AD RMS-protected content file sent to Information Recipient. AD RMS-protected content may also be represented by e-mail.
5. Recipient receives file, opens using AD RMS-enabled application or browser. If no account certificate on the current computer, the AD RMS server will issue one (AD RMS document notifies application of the AD RMS server URL).
6. Application sends request for use license to AD RMS server that issued publishing license (if file published offline, send to server that issued the CLC). Request includes RAC and PL for file.
7. AD RMS server confirms recipient is authorized, checks for a named user, and creates use license for the user. Server decrypts content key using private key of server and re-encrypts content key with public key of recipient, then adds encrypted session key to the use license. This means only the intended recipient can access the file.
8. AD RMS server sends use license to information recipient's computer.
9. Application examines both the license and the recipient's account certificate to determine whether any certificate in either chain of trust requires a revocation list. User granted access as specified by information author.

Information Author — **Information Recipient**

AD RMS-Protected Content (XrML) — Each consumer of content receives unique license that enforces rules.

Group Policy
Product Scenario: Server Management
Windows Server 2008

Group Policy delivers and applies configuration or policy settings to targeted users and computers within an Active Directory environment. Windows Server 2008 supports a Central Store for centralized XML-based template storage, advanced logging, and enhanced Group Policy delivery and enforcement using Network Location Awareness.

Group Policy Delivery & Enforcement

Workstation / Member Server Delivery
- Workstation / Member Server Startup
- Processed every 90-120 minutes (randomized)
- Refreshes on NLA notifications (Windows Vista and Windows Server 2008)

User Delivery
- At user logon
- Processed approximately every 90-120 minutes (randomized)

Domain Controller Delivery
- Domain Controller Startup
- Processed approximately every 5 minutes

Network Location Awareness (NLA)
Using Network Location Awareness, Group Policy has access to resource detection and event notification capabilities in the operating system. This allows Group Policy to refresh after detecting the following events:
- Recovery from hibernation or standby
- Establishment of VPN sessions
- Moving in or out of a wireless network
- Removes the reliance on the ICMP protocol (PING) for assisting policy application across slow link connections
- Is used for bandwidth determination (applying GP over slow links)

Group Policy Central Store
Central Storage for Administrative Templates
1. Create Central Store on PDC Emulator
2. Central Store created for each domain
3. If Central Store available when administrating domain-based GPOs, the central store is used by default

Central Store Benefits
- Single point of storage
- Multilingual support
- Central Store hosted on Windows Server 2000, Windows Server 2003, & Windows Server 2008

Multiple Local Group Policy Objects
GPO Processing Order: MLGPO → Site → Domain → OUs

MLGPO Architecture
- Local Computer Policy
- Admin OR Non-Admin Group Policy
- Local User Account Policy

Group Policy Tools
Windows Vista, Windows 2008
- ☑ Manage new Windows Vista/Windows Server 2008 Policy Settings
- ☑ Manage Windows 2000, Windows Server 2003, and Windows XP Machine Policy Settings

Windows 2000, Windows Server 2003, Windows XP
- ☒ Cannot manage new Windows Vista/Windows Server 2008 Policy Settings
- ☑ Manage Windows 2000, Windows Server 2003 and Windows XP Machine Policy Settings

Group Policy Logging
- Windows Logs
- Applications and Services Log
- No "userenv.log" required
- XML-based event logs
- Report, filter, and create customized log views

Event Viewer Subscription — Collect copies of events from multiple remote computers and store them locally

---

Active Directory Management
Product Scenario: Server Management
Windows Server 2008

Active Directory Domain Services (AD DS) expands auditing capabilities to track changes in the Active Directory objects. Windows Server 2008 has password policy that removes the restriction of a single password policy per domain. AD DS has the capability to stop and restart the Active Directory Service.

Fine-Grained Password Policies
Fine-grained password policy removes the restriction of a single password policy per domain.

GlobalNames Zone
Resolution of single-label, static, global names for servers using DNS.
- All authoritative DNS servers for a domain must be running Windows Server 2008 to provide GlobalNames support for clients
- Implemented as a Regular Forward-lookup zone, which must be named "GlobalNames"
- The GlobalNames zone should be Active Directory integrated and replicated forest-wide
- The GlobalNames zone is manually configured with CNAME records to redirect from server's host name to Fully Qualified Domain Name

Restartable Active Directory Service
Active Directory Domain Services (AD DS) in Windows Server 2008 has the capability to start and stop the Active Directory Service via the MMC or command line.

Directory Service States
- AD DS Started
- AD DS Stopped (Ntds.dit offline)
- AD Directory Restore Mode

Audit Object Changes
Active Directory (AD DS and AD LDS) in Windows Server 2008 has the capability to log changes made to AD objects.

Audit Controls
- Global Audit Policy (Audit Active Directory Changes)
- Security Audit Entry on object
- Schema – Set per attribute to prevent change logging

Active Directory Read-Only Domain Controller
Product Scenario: Enterprise and Branch Office
Windows Server 2008

A Read-Only Domain Controller (RODC) allows organizations to easily deploy a DC in locations where physical security cannot be guaranteed. RODC hosts a read-only replica of the database in Active Directory Domain Services (AD DS) for any given domain.

Read-Only Partial Attribute Set — Prevent replication of sensitive information. Requires manual configuration.

Branch Office
- Read-only replica AD DB
- Unidirectional replication
- Credential caching
- Read-only AD-integrated DNS zone

- Universal group membership caching automatically enabled for site in which the RODC is deployed

Delegated Administration for RODC
RODC administrators can be different users from domain administrator users. Benefits include:
- Prevents accidental modifications of directory data existing outside RODC
- Delegated installation and recovery of RODC

Delegated Installation and Administration Process for RODC
(Note: Steps 1 and 2 are not necessarily performed from the same computer)
1. **Pre-Create and Delegate** — Domain Administrator uses AD Users and Computers MMC snap-in to pre-create RODC. Specifies RODC's FQDN and Delegated Administration group
2. **Promote RODC** — Delegated Administrator (non-DA) uses DCPROMO Wizard from server to configure as RODC. Replicates over network, with support for secure IFM. Reboots as RODC

RODC Deployment – Incremental Requirements
- Windows Server 2003 Forest Functional Mode
- Multiple Windows Server 2008 DCs per domain are recommended to load balance RODC replication

---

Authors: Martin McClean & Astrid McClean (Microsoft Australia)