Active Directory Management
A quick guide for IT professionals

White Paper

Contents

Introduction

Microsoft's Active Directory offers a centralised way for IT system administrators to manage user accounts and devices within an IT infrastructure network. Changes in Active Directory are generally made by IT administrators centrally for consistency across the IT infrastructure environment.

With the right Active Directory management in place, users can enjoy benefits such as being able to log onto devices and into applications with the same username and password; use their settings and files across all devices that are members of relevant Active Directory groups; have peace of mind knowing that when a device is lost, defective or stolen, they can remain productive on another Active Directory-managed device.

Active Directory and its Components

Now we have defined what Active Directory is, here are some of the key components that make up this useful IT Administration tool set:

Domain Controllers

On Microsoft Servers, a domain controller (DC) is a server which responds to security authentication requests (log in, checking permissions, etc.) within the Windows Server domain. These are Windows Server installations equipped with the Active Directory Domain Services Server Role.

Domain Controllers can be physical hosts and virtual machines. The most important elements of Domain Controllers are:

The Active Directory Database: The Active Directory database and its supporting files contain the definition of objects and the configuration of objects. Examples of objects are Containers, Org Units, user accounts and computer accounts.

Read/write Domain Controllers: These Domain Controllers allow changes to their Active Directory databases and System Volumes from Active Directory members and can be used to bring changes to other Domain Controllers.

Read-only Domain Controllers: Are Domain Controllers that only allow read-access to their Active Directory databases and System Volumes. Changes are brought in by Read/write Domain Controllers.
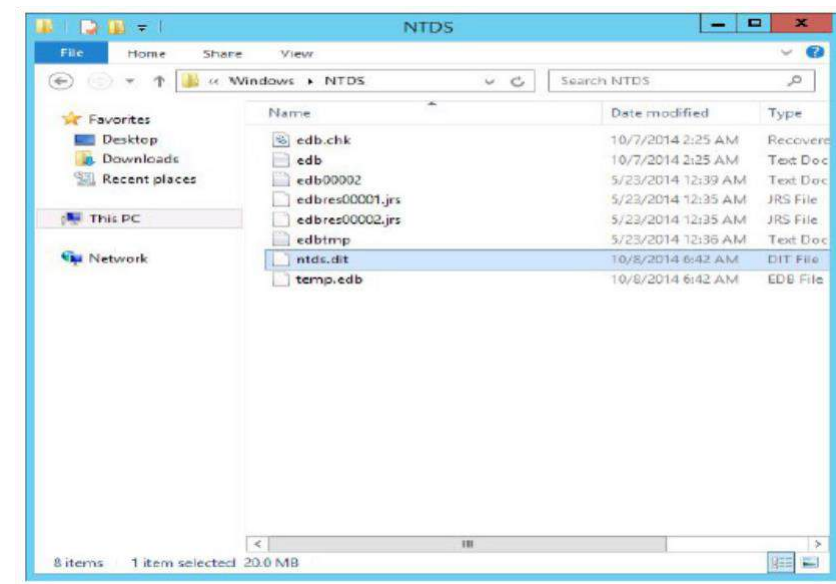

Figure 1 : Active Directory Database Example

Grouping of Domain Controllers

Domain Controllers are generally grouped into sites, domains and forests. An Active Directory site, typically, represents a geographical site of high-speed connectivity. Active Directory sites govern replication between Domain Controllers configured in Active Directory sites.

By default, authentication traffic from within an Active Directory site is directed to a Domain Controller in that site. A Domain Controller can only be part of one Active Directory site at a time. Active Directory domains are containers of replication.

Additionally, all Domain Controllers in a domain can receive changes and replicate those changes to all other Domain Controllers in it. Each domain in Active Directory is identified by a Domain Name System (DNS) domain name.

An Active Directory forest is a collection of one or more Active Directory domains that share a common Active Directory schema. Most Active Directory environments exist with one Active Directory domain in its own Active Directory forest.

Inside the Active Directory database

The Active Directory database consists of two types of data:
The Active Directory schema Objects are defined in the schema. This way, their behaviour and relationships are shaped.

For example, the fact that a user account object can have a last name where a computer object cannot, is defined in the Active Directory schema.

The Active Directory configuration. The objects themselves and the information in their properties (called attributes) are stored in the configuration part of the Active Directory database

Objects

Each object within the Active Directory configuration is identified with a security identifier, the SID. The security identifier consists of two parts: The domain identification part and the relative identifier, relative to the domain. In the screenshot to the right you can see the properties for the Ronnie Properties user object (after the Advanced Features were enabled in the View menu of the Active Directory Users and Computers management tool).

The Security Identifier for the user object used by Ronnie is S-1-5-21-2225613072-2737155430-3758491199- 1128.Its relative identifier is 1128. Although, strictly speaking, every object is a container in the world of Active Directory, only true container objects have objects under them. Organizational Units (OUs) and Containers (CNs) in the configuration part of the Active Directory database are represented in the Active Directory management tools as folders.

The differences between OUs and CNs is that the first can be used to deploy settings (through Group Policy Objects). The special thing about CNs is that you cannot delete them using standard tooling. Containers that are available in a default Active Directory environment are Built-in, Users and Computers. The Exchange Users, New Users, Security and Distribution Grroups and Domain Controllers Org Units (OUs) are clearly distinguishable from the containers by their icons.
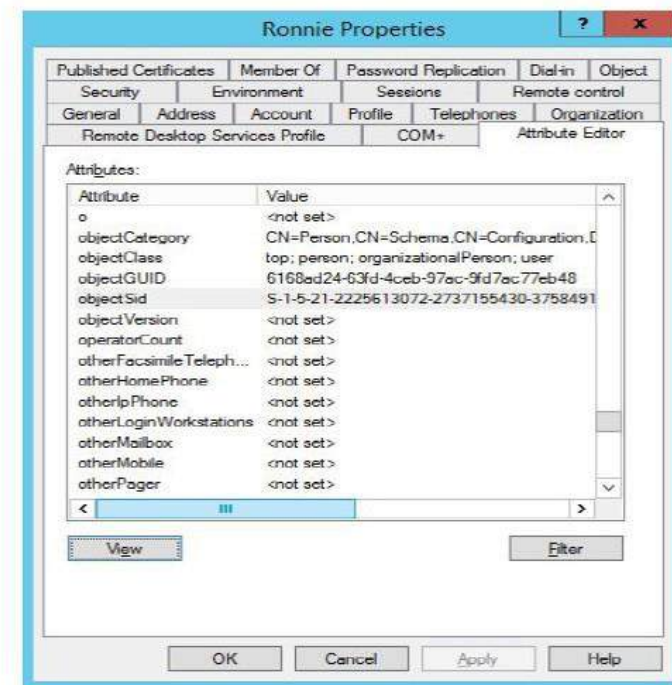

Figure 2 – Example of a user object

Attributes

Objects have properties based on the Active Directory schema.
These properties are called attributes. Some attributes contain a single value such
as the password last set attribute for a user object. Other attributes may contain
multiple values such as the members attribute of a group object.

In the screenshot of Active Directory Users and Computers below,
you can see the Organizational Units and Containers for an Active Directory
domain based on Windows Server 2012 R2 Domain Controllers:
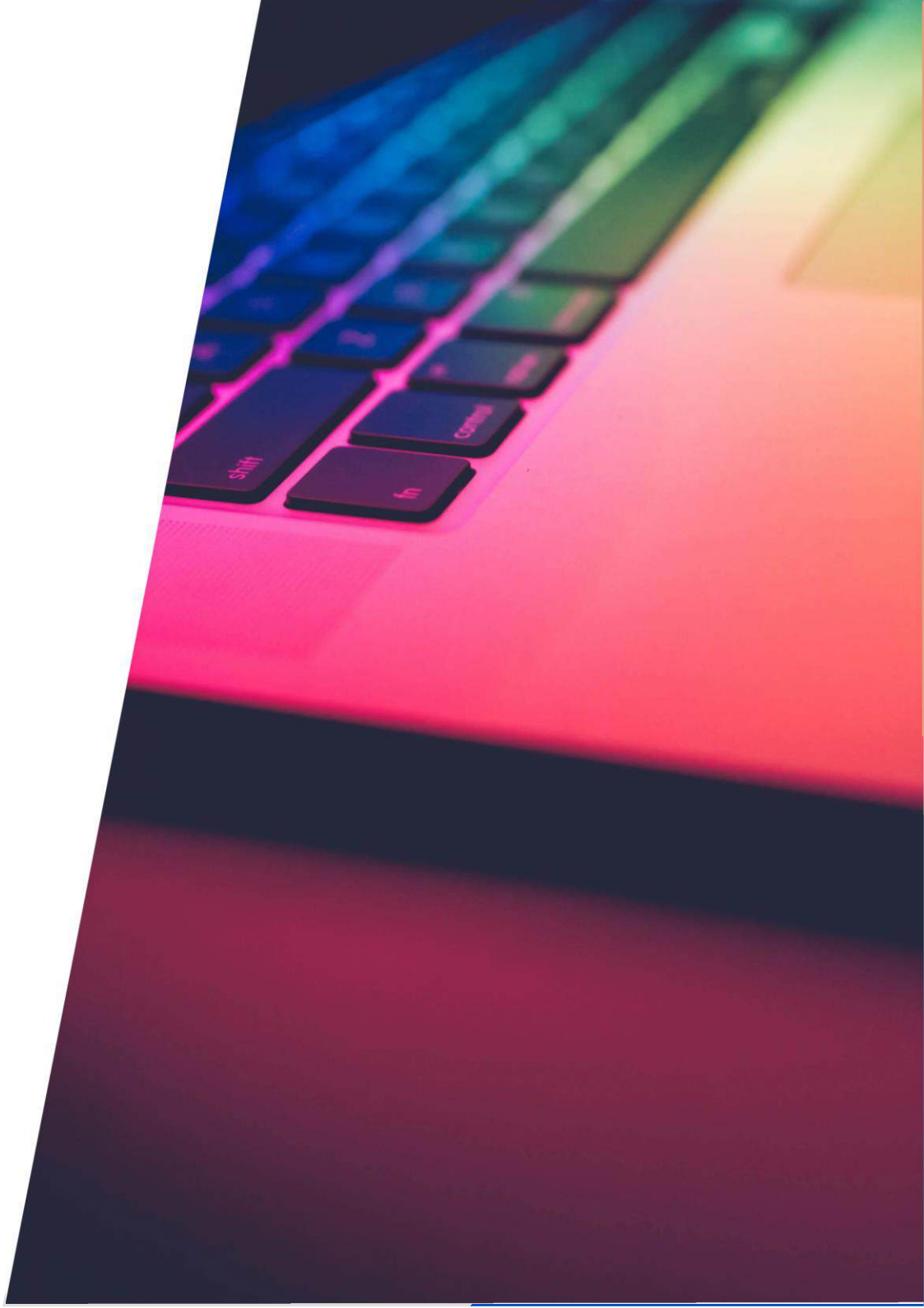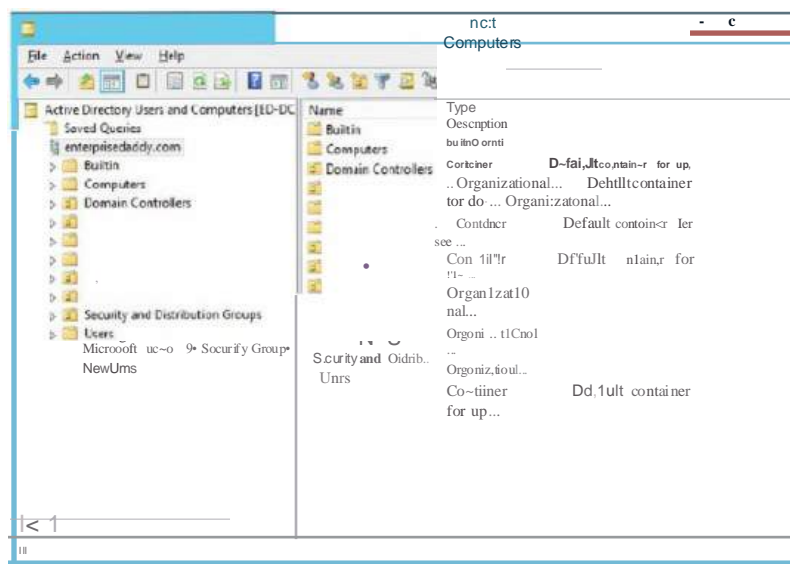
Replication and High Availability

Active Directory High Availability is not based on Failover Clustering (like Hyper-V) or Log shipping (like Exchange and SQL Server). In its place, Domain Controllers all offer the Active Directory database and System Volume (SYSVOL) to whoever needs the information in it.

When IT Administrators deploy at least two Domain Controllers for an Active Directory domain, they gain redundancy and High Availability for that Active Directory domain. This means a mechanism to keep the contents of this database in sync between Domain Controllers is needed.

Active Directory uses replication between Domain Controllers to keep things in sync. Replication synchronizes changes that are made on one Domain Controller with all other Domain Controllers in scope of replication. Data integrity is maintained by tracking changes on each Domain Controller and updating other Domain Controllers systematically.

Active Directory replication uses a connection topology that is created automatically by the Knowledge Consistency Checker (KCC) to reduce administrative effort, but can alternatively be modified manually.

Intrasite and intersite replication

Going back to the previously mentioned Active Directory sites, two types of replication exist:

Intrasite replication - Within an Active Directory site, replication is based on pull replication. After being notified of changes, a Domain Controller will ask the Domain Controller with the change what changes it has seen. To reduce network chatter, intrasite replication is setup by default as a two-way ring topology. This avoids Domain Controllers within a site to communicate to each of the other Domain Controllers. Instead, the ring topology allows it to communicate to two of its site siblings.

Intersite replication between Active Directory sites - Replication is schedule-based and between frontline servers. After the default schedule time-out (15 minutes by default), the Domain Controller for a site asks the other Domain Controller in the other site for the changes it has seen. The main Domain Controller then replicates the changes to the Domain Controllers in its site using intrasite replication.

Replication is also where the schema and configuration parts of the Active Directory database come into play. The schema is replicated and used throughout an Active Directory forest, where larger parts of the configuration is only replicated among Domain Controllers of a domain.

Global Catalogue servers

The Active Directory databases of Domain Controllers configured as Global Catalogue servers maintain all objects within a forest. These types of Domain Controllers store all attributes for all objects for the domain it is a Domain.

Controller for, but only the most important attributes for objects in the other domains in the forest. This allows for approval within the Active Directory forest. E.g. The ability to add a group from another domain in a forest to the access control list of a file share in your domain.

Flexible single-master operations

When it comes to replication, a couple of areas that will hinder progress come to light. Since all Domain Controllers are able to commit to the database simultaneously, replication collisions may occur. Therefore, Active Directory replication works with five Flexible Single Master Operations (FSMO) roles:

The Primary Domain Controller emulator

The Domain Controller in the domain with the Primary Domain Controller emulator (PDCe) Flexible Single Master Operations (FSMO) role, is commanding for the replication of password changes, group policy changes and Distributed File Services (DFS) changes. A Domain Controller will replicate these changes to the PDCe first, which then replicate it to the other Domain Controllers.

This way, when a colleague changes the password for a user object in a site across the globe, and the new password is used at another site, the PDCe will be able to tell the IT Administrator that the new password is correct even though the Domain Controller at site has not received the change yet. The Domain Controller with the PDCe FSMO role also serves as the default time server for all other Domain Controllers in the domain.

The RID pool master

SIDs, and RIDs (as they are commonly known), are used to create new objects. The Domain Controller with the RID pool Flexible Single Master Operations (FSMO) role is responsible for avoiding RID-based object creation collisions. It hands out 500-object RID pools to Domain Controllers within the Active Directory domain. When a Domain Controller depletes its 500-object RID pool, all it has to do is ask for a new pool.

The infrastructure master

The Domain Controller with the Infrastructure Master Flexible
Single Master Operations (FSMO) role is responsible for updating references
from objects in its domain to objects in other domains. The infrastructure
master compares its data with that of the previously mentioned Global
Catalogue servers.

Domain Controllers configured as Global Catalogue servers receive
regular updates for objects in all domains through replication, so the Global
Catalogue data will always be up to date. If the infrastructure master finds data
that is out of date, it requests the updated data from a global catalogue. The
infrastructure master then replicates that updated data to the other Domain
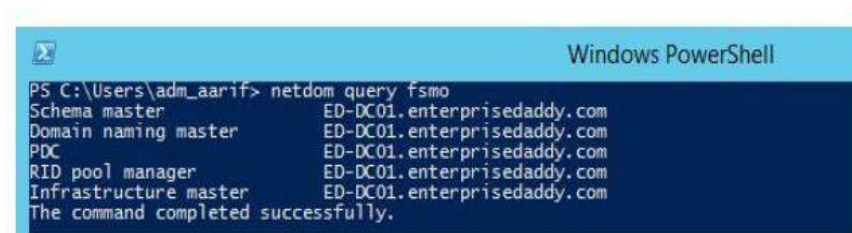Controllers in the domain.

The schema master

The Domain Controller with the Schema Master Flexible Single
Master Operations (FSMO) role is responsible for the integrity of the
Active Directory schema. Since schema changes impact all objects
on all Domain Controllers within an Active Directory forest, changes
to the Active Directory schema occur on the Domain Controller
with the Schema Master Flexible Single Master Operations (FSMO)
role and replicated from there.

The domain naming master

The second forest-wide Flexible Single Master Operations (FSMO) role is the Domain Naming Master role. The Domain Controller holding this role is authoritative for the Active Directory domains within an Active Directory forest. When an IT Administrator adds or removes a domain to a forest, the change originates from the Domain Controller holding the Schema Master Flexible Single Master Operations (FSMO) and replicates from there.

Using the netdom query fsmo command, IT Administrators can quickly find out the Domain Controllers holding the Flexible Single Master Operations (FSMO) roles in an Active Directory environment:

Figure 3 – Example of Flexible Single Master Operations (FSMO) roles in an Active Directory environment

Functional levels

Active Directory domains and forests are configured with a functional level. These levels govern the minimum Windows Server Operating System (OS) version for Domain Controllers. Raising these levels unlock new functionality.

When IT Administrators raise the Active Directory Domain Functional Level (DFL), they remove the ability to run and promote Windows Servers below that version in the Active Directory domain. IT Administrators can only upgrade when all Domain Controllers with earlier Windows Server versions are removed from the domain or upgraded.

After all Active Directory domains in an Active Directory forest have their Domain Functional Level (DFL) raised to a certain version, IT Administrators can raise the Active Directory Forest Functional Level (FFL) for the forest.

Active Directory and its networking services - DNS

Active Directory relies heavily on the Domain Naming System (DNS). First of all, each Active Directory domain is represented by a DNS domain name. Within an Active Directory forest, multiple domains may share a common DNS name tree or have separate DNS domain names. Secondly, Active Directory-joined devices use DNS to locate Active Directory services like Domain Controllers.

DNS Domain Names

The Domain Naming System (DNS) is a hierarchical naming system. Its highest level is the root. Beneath the root, IT Adminstrators find top level domains (TLDs), like .com, .net and .org. Then, there's the domain name portion, which can be registered: EnterpriseDaddy. com is a registered domain name for the company named Enterprise Daddy.

When an Active Directory domain is created, a DNS domain name must be specified. Microsoft's best practice is to register a domain name on the internet and use that, or an internal sub-domain beneath it, as the Active Directory DNS domain name. This provides the best interoperability and connectivity to the outside world.

DNS Zones

For each of the hierarchical layers in the Domain Naming System (DNS), two corresponding DNS zone types exist:

Forward Lookup Zones - DNS Forward Lookup Zones contain information on DNS records that allow you to convert a DNS name to IPv4 and IPv6 addresses.

Reverse Lookup Zones - DNS Reverse Lookup Zones perform the reverse job of Forward Lookup Zones. It allows for DNS clients to get a DNS name for a specific IPv4 or IPv6 address.

DNS Records

DNS Zones contain DNS Records. In DNS Forward Lookup Zones, A and AAAA records contain information on the IPv4 and IPv6 addresses associated to certain hostnames, like www.DNS Forward Lookup Zones used by Active Directory typically contain a lot of SRV records to point to IPv4 and IPv6 addresses for Active Directory functionality like Domain Controllers configured as Global Catalog servers. In DNS Reverse Lookup Zones, PTR records contain DNS names for certain IPv4 and IPv6 addresses.

DNS Servers

The Domain Naming System (DNS) is offered through DNS Servers. These are the servers that are queried by domain-joined devices. While you can use stand-alone DNS Servers, Active Directory offers Active Directory integration for DNS.

This way, Domain Controllers double as DNS Servers and the information in the DNS zones are replicated between them in the same way the Active Directory configuration is replicated. This offers some benefits:

Traditional DNS Servers - changes can only be made on Primary DNS Servers. Changes are then transferred to Secondary DNS Servers. Information in Active Directory-integrated DNS Zones can be modified on each of the Domain Controllers acting as DNS Servers.

On traditional DNS Servers, changes in DNS Zones are transferred by transferring the entire DNS Zones. Information in Active Directory-integrated DNS Zones is replicated on a per-record basis, vastly reducing the amount of network traffic and time required for DNS updates.

DHCP

Although the Dynamic Host Configuration Protocol (DCHP) is not a requirement for Active Directory, it is commonly used in Active Directory environments for its flexibility. Through the Dynamic Host Configuration Protocol (DHCP), devices on a network can automatically configure their IPv4 and IPv6 addressing information by negotiating this information with DHCP Servers.

DHCP is used extensively in environments with and without Active Directory. Your Internet Service Provider (ISP) uses it to configure your router without Active Directory. However, using DHCP within an environment with Active Directory offers several benefits:

DHCP Authorization - In an Active Directory environment, domain-joined devices acting as DHCP servers need to be authorized in Active Directory. Without this authorization, DHCP will not offer addressing information.

This is helpful to protect against devices that offer addressing information that point devices to other routers and DNS Servers than DHCP Servers.

DHCP and Dynamic DNS Authorized DHCP Servers offer automatic registration and updating of DNS records within Active Directory; integrated DNS Zones, both Forward Lookup Zones and Reverse Lookup Zones. This way, information in DNS is kept up to date without administrative effort.

Active Directory in the networking infrastructure

Device-independent productivity - Every colleague with a user account in Active Directory is able to sign into every domain-joined device with the credentials and authentication methods associated with that user account. Servers are not considered standard devices and IT administrators can further limit the scope of devices for colleagues. When a device is lost, defective or stolen, users can simply sign into another Active Directory-managed device and be productive on it.

Single Sign-On - Once signed into a domain-joined device with an Active Directory user account, colleagues benefit from Single Sign-On (SSO) into Active Directory-integrated applications, files and services. When a colleague signs into a device, their credentials are sent to the Local Security Authority Subsystem Service (lsass. exe). This service is responsible for providing the Single Sign-On experience for the colleague.

LSASS hosts a number of plug-ins representing the protocols that Windows supports including NTLM authentication, Digest authentication and Kerberos.

Credentials are presented to each of these plugins, producing one-way hashes and tickets in the memory space of LSASS, which would remain there for the duration of the user session. During this session, the colleague benefits of Single Sign-On to all Active Directory integrated applications, files and services.

Using Group Policy Objects (GPOs) - IT administrators can govern settings on domain-joined devices. Administrators can centrally configure settings for applications and services, and also settings that govern how Windows looks and feels.

Additionally, the functionality offered by Group Policy Objects (GPOs), Group Policy Preferences (GPPs) can be used to replace legacy startup, shutdown, logon and logoff scripts.

Consistent user experience - User profiles, Home folders and Folder redirection can be used to synchronize files and settings between devices and file servers. This way, all these settings are backed up automatically on the file server and protected against data loss on the device level.

Additionally, on any new domain-joined device a colleague logs on, these files and settings are automatically synced back from the file server, offering a consistent user experience.

Distributed File System for optimized access to files -
The Distributed File System (DFS) File Server Role Service can be used in conjunction with Active Directory sites to synchronize files and folders between file servers located in different Active Directory sites and pointing domain-joined devices to the file server located in their Active Directory site.

The System Volume (SYSVOL) file share on Domain Controllers is the most prominent example of the Distributed File System (DFS) model, exposing the data in it to domain-joined devices efficiently, based on Active Directory sites.

Best practices when deploying Active Directory

With Active Directory present in every major aspect of networking infrastructures, there's an urgency to deploy Active Directory and Domain Controllers correctly. Below is Wanstor's list of key considerations to achieve this outcome:

+ Create at least two (equal) Domain Controllers per domain

+ Implement Role Separation. Do not misuse a Domain Controller as an Exchange Server or SQL Server, unless it's a Windows Small Business Server

+ Take time to understand server dimensions in terms of hardware and software. Use RAID and separate spindles for storage of Active Directory-related data when possible. Use the Infrastructure Planning and Design (IPD)

+ Use hardware and software still covered by the vendors guarantee, support, and/or life cycle policy for the period in which you need to rely on the Domain Controller. Additionally, Wanstor strongly recommends Windows Server 2012 as the Operating System for newly deployed Domain Controllers.

+ When the server is a virtual machine, have the correct procedures in place. Always run sysprep.exe when working with Windows Server templates. Before you install Windows Server, run the Memory Diagnostics from the windows Server DVD. Possible memory corruption issues show early this way and this will minimize issues further on in the lifetime of the server.

+ Document the passwords for the DSRM accounts on each Domain Controllers on the password list for your organisation. IT Admins will need these passwords in disaster recovery scenarios. Implement Information Security measures (anti-malware and UPS client software) according to the best practices of the manufacturer for Domain Controllers. Make exclusions for the Active Directory database and supporting files

+ To promote Domain Controllers, use answer files. IT Administrators should write them, get them checked, signed off and then use them. Include them in your documentation after they have been used them since the passwords will be stripped by the server after usage.

+ After promotion, check dcpromo.log, dcpromoui.log and event viewer for issues.

+ Run Windows Update after promotion. IT Administrators will only be offered Active Directory-specific updates after promoting a Windows Server installation to a Domain Controller.

+ Configure system state backups to run periodically. Don't forget to configure regular separate backups of GPOs and Starter GPOs through the Group Policy Management Console since these won't be as easy to recover granularly.

+ Run the Active Directory Best Practices Analyser regularly.

Active Directory

Practical Management Solutions

What is ADManager Plus?

What is ADManager Plus?

ADManager Plus is a simple, easy-to-use Windows Active Directory Management and Reporting Solution that helps IT administrators and Help Desk Technicians with their day-to-day activities. With a centralized and intuitive web-based user interface, the software handles a variety of complex tasks like Bulk Management of User accounts and other AD objects, delegates Role-based access to Help Desk Technicians, and generates various AD Reports as an essential requirement in satisfying Compliance Audits. This tool also offers mobile AD apps empowering performance of important user management tasks right from mobile devices at any location with an internet connection.

What problems does ADManager Plus address?

+ Eliminates repetitive, mundane and complex tasks associated with AD Management

+ Automates routine AD Management and Reporting activities for AD Administrators

+ Facilitates Creation, Management and Deletion of AD objects in Bulk

+ Provides 'on the move' AD user management capability through its mobile apps

+ Acts as an essential resource during Compliance Audits like PCI, GDPR and ISO

What features does it offer?

+ Single and bulk user management	+ Group Computer Management	+ Help Desk Delegation
+ O365 Management & Reporting	+ Active Directory Automation	+ Active Directory Cleanup
+ Active Directory Reports	+ Real Last Logon Reports	+ Exchange Management

Key Features of AD Manager Plus

Every IT administrator faces the challenge of managing Active Directory objects including users, groups, computers, OUs and more daily. Manually performing complex tasks such as configuring user properties is extremely time consuming, tiresome and prone to error. AD Manager Plus enables automation and simplification of many of these tasks, with key features including:

MANAGEMENT

+ Create users in AD, Exchange, Office 365, Google Apps, and Skype for Business (Lync) in a single step
+ Create or modify AD objects (users, groups, contacts, OUs, computers) in bulk via CSV import
+ Perform tasks like password reset, account unlock, clean up and more
+ Streamline management of AD objects such as users and OUs with customizable templates
+ Assign, replace, or revoke Office 365 licenses in bulk
+ Manage shared, remote, room, equipment mailboxes

REPORTING

+ Generate and schedule more than 150 preconfigured, granular reports on AD, Exchange, Office 365, and Google Apps
+ View inactive users, locked out users, disabled computers, and more in just few clicks
+ Perform management tasks for specific users within reports
+ Export to various formats: HTML, PDF, XLS, XLSX, CSV, CSVDE
+ Mention specific users or computers in a CSV file for generating their important details
+ Generate compliance reports to meet regulatory standards such as PCI, GDPR, ISO and more

OU & ROLE-BASED HELP DESK DELEGATION

+ Delegate AD tasks to help desk technicians granularly within specific OUs
+ Delegate tasks like password reset and user creation
+ Delegate without elevating technicians' AD privileges

iOS & ANDROID APPS

+ Manage users from anywhere - reset passwords; unlock, enable, disable and delete accounts
+ Report on locked out, disabled, password, expired, inactive users
+ View, manage, and execute AD workflow requests

AD AUTOMATION & WORKFLOW

+ Automate routine tasks such as AD clean up
+ Manipulate automated tasks via workflow with automation Configure
+ review-approval workflows to execute AD tasks with a structured flow

Other   Active   Directory Tools

Features & Benefits

ManageEngine
ADSelfService Plus

ADSelfService Plus is an IT self-service solution designed for Windows environments. It is a feature rich IT self service solution which can be implemented independently or integrated seamlessly with company websites.

+ Self-service password management for on-premises Active Directory and cloud applications
+ Notify users (email & SMS) on impending password & account expiration
+ Enforces granular password policies across AD and connected on-premises and cloud applications
+ Automatically syncs Active Directory password in real-time across multiple applications
+ Offers Active Directory-based single sign-on (SSO) for cloud applications

ManageEngine
ADAudIt Plus

In real-time, IT administrators can ensure critical resources in the network like Domain Controllers are audited, monitored and reported on with information on Users, Groups, GPO, Computer and OU changes, with 200+ detailed event specific reports and instant email alerts.

+ Web-based, Active Directory tool to track all domain events, including user, group computer, GPO, and OU changes
+ Audits Windows files servers, failover clusters, NetApp for doc changes to files and folders, audit access
+ Monitors every user logon and logoff, including every successful and failed logon event across network workstations
+ Tracks Windows member servers, FIM, printers, and USB changes with events summary; tracks application, policy, and system events
+ Brings 150+ ready-to use audit reports with instant email alerts to ensure security and meet IT Compliance requirements

ManageEngine
Exchange Reporter Plus

ManageEngine Exchange Reporter Plus is a comprehensive web-based analysis & reporting solution for Microsoft Exchange, providing over 100 different reports on every aspect of the Microsoft Exchange Server environment.

+ Web-based change auditing/ reporting solution for MS Exchange environments
+ Track / monitor enterprise ActiveSync infrastructure & inventory of related smart devices
+ Report on Outlook Web Access usage, mailbox traffic, mailbox growth
+ Supports customized reports that use data filters, automatic scheduling, and multi-format report generation
+ Provides audit feature to enable investigation of unauthorized mailbox logons and other critical changes

ManageEngine
RecoveryManager Plus

Empowers IT teams to backup changes made to AD objects as separate versions, providing an Exchange Online backup solution for numerous Exchange functions & data

+ Automated incremental backup of Active Directory objects
+ Simple and granular restoration down to the attribute level
+ Change tracking to undo changes
+ Detailed version management of each attribute change
+ Provision to roll back Active Directory to an earlier state

ManageEngine SharePoint Manager Plus

ManageEngine SharePoint Manager Plus is a tool that helps IT administrators to manage, audit and report on both on-premises and Office 365 SharePoint environments. It also allows monitoring, tracking and analysis of all activities in a SharePoint infrastructure, which facilitates informed, timely and accurate decision-making and management.

+ Web-based tool to manage and audit SharePoint on-premise servers and Office 365 configurations
+ Provides complete infrastructure visibility into both on-premise and online SharePoint server components
+ Includes out-of-the-box reports for monitoring SharePoint components such as farms, content databases, web applications, site collections, sites, lists and document libraries
+ Performs component level and security level auditing. Tracks permission changes, group changes and new role changes instantly with alerts
+ Meet compliance requirements by archiving audit log data for flexible time period

ManageEngine DataSecurity Plus

ManageEngine DataSecurity Plus is agent-based, real-time file auditing & reporting software that delivers complete visibility into Windows file server environments, showing IT administrators the 'who, what, where and when' behind every access event while also perform storage analysis. This helps to improve organisational Windows file server data security and information management, in a simple yet efficient and cost-effective way.

+ Web-based, real-time Windows file server access auditing & storage analysis tool helping meet data security, information management & compliance needs
+ Track & analyze access to files & folders by inspecting anomalies, recording access patterns & examining share & NTFS permissions
+ Optimize storage space by isolating old, stale & non-business files, gain insight into disk space usage & viewing file and folder properties
+ Actively respond to security breaches with instant email alerts. Detect & counter ransomware with mass access alerts & response automation
+ Stay compliant with SOX, HIPAA, FISMA, PCI, GLBA, GDPR, and other regulatory mandates

ManageEngine O365 Manager Plus

Providing exhaustive preconfigured reports on Office 365 & helping IT administrators perform complex tasks including bulk user & mailbox management, secure delegation and more. Monitor Office 365 services 24/7 and receive instant email notifications about service outages. O365 Manager Plus eases compliance management with built-in reports, offering advanced auditing & alert features to keep Office 365 setups secure.

+ An Office 365 reporting, monitoring, management and auditing tool
+ Utilize out-of-the-box reports Exchange Online, Azure Active Directory, OneDrive for Business and Skype for Business, as well as reports on security, compliance management and licences for Office 365
+ Monitor Office 365 service health around the clock, and receive instant email notifications on service outages
+ Effortlessly oversee your Office 365 setup with a wide range of Exchange Online and Azure Active Directory management features
+ Track even the most granular user activities in Exchange Online, Azure Active Directory, OneDrive for Business, Sway, and other services
+ Audit critical activities and changes in your Office 365 environment with custom alerts for each Offices 365 service
+ Delegate Office 365 administration tasks granularly to help desk staff and other non-IT users through role-based delegation