

[Click Here](#)



























Active Directory (AD) is an essential component for managing networked systems within many business environments. At its core, AD provides a centralized platform for organizing, managing, and securing network resources, including computers, user accounts, and other assets. Developed by Microsoft, AD is a cornerstone of many enterprise-level Windows network environments, offering a range of features that facilitate efficient management of IT resources. This trial is designed for beginners, aiming to provide a fundamental understanding of Active Directory's structure and capabilities, as well as hands-on guidance for basic tasks. Understanding AD is crucial for anyone aspiring to work in network administration or IT support. As a directory service, it serves as a centralized database that stores information about objects within the network, such as users, groups, computers, and printers. This allows administrators to manage permissions and access to network resources effectively. If you want to learn AD and get hands-on experience in our free IT labs, then sign up to our free AD course at the link below! This free course will teach you the fundamentals of Active Directory. You'll learn how to create and...10 Lessons! Quizzes! Labs! Hr One of the significant advantages of using AD is its ability to streamline the management of a large number of resources and users. Administrators can create and manage user accounts, assign and enforce security policies, and automate tedious administrative tasks. Additionally, AD's hierarchical structure makes it scalable, suitable for organizations of various sizes, from small businesses to large corporations. In this tutorial, we'll cover the basics of Active Directory, including its key components, how to access and navigate its interface, manage users and groups, and organize resources using Organizational Units. Whether you are new to network administration or looking to broaden your IT skills, this guide will provide a comprehensive introduction to the world of Active Directory. Active Directory (AD) is a directory service created by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Primarily, AD stores information about objects on the network and makes this information easy for administrators and users to find and use. Understanding its basic components is crucial for effective AD management. Key Components of Active Directory: Domain: A domain is a central part of AD's structure. It's a logical group of network objects, like users, computers, and devices, that share the same AD database. A domain is managed by a domain controller. Domain Controller (DC): A server that responds to security authentication requests within a Windows Server domain. It stores domain information, authenticates users, and enforces security policies for a domain. Organizational Unit (OU): These are containers within a domain that can hold users, groups, computers, and other OUs. They provide a way to organize directory objects into logical hierarchies, offering more granular control over the management of these objects. Global Catalog (GC): This is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multi-domain AD forest. It helps in locating objects from any domain without needing their domain name. Schema: The schema is a component of AD that defines all the objects and attributes that the directory service can manage. It determines the kinds of objects that can be stored in the directory and the attributes of those objects. Understanding these components is vital for anyone starting with Active Directory. They form the backbone of AD's structure and functionality. As we proceed, we'll explore how these components interact and how they can be managed effectively. In addition to these components, AD uses Lightweight Directory Access Protocol (LDAP) for directory services and Kerberos and NTLM for authentication protocols. These protocols are essential for ensuring secure and efficient communication within the network. As a beginner, familiarizing yourself with these terms and their functions within AD will lay a solid foundation for your journey into network administration. In the following sections, we will delve into accessing and navigating Active Directory, managing users and groups, and organizing resources efficiently. Nine times out of ten, when someone says "Open Active Directory", they really mean open the Active Directory Users and Computers console as shown in the image below: Active Directory Users and Computers This article will focus on this part of Active Directory since it is by far the most common. If you want to learn more about Active Directory including a hands-on lab, consider taking our free Active Directory Fundamentals course: This free course will teach you the fundamentals of Active Directory. You'll learn how to create and...10 Lessons! Quizzes! Labs! Hr To effectively manage your network's resources using Active Directory, you first need to know how to access it. There are two primary methods for accessing AD: through a Domain Controller or using Remote Server Administration Tools (RSAT). Logging into a Domain Controller: A Domain Controller (DC) is a server that manages all security-related aspects regarding users and computer authentication within the Windows domain. By logging into a DC, you gain direct access to the Active Directory Domain Services (AD DS). This method is straightforward - once you're logged into the server, you can start managing AD immediately. However, it's vital to ensure that your access to the DC is secured and limited only to authorized personnel to maintain network security. Using Remote Server Administration Tools (RSAT): RSAT allows administrators to manage Windows servers and desktops remotely. It includes various tools, including Active Directory Users and Computers (ADUC), which is particularly useful for AD tasks. To use RSAT: Download and install RSAT from the official Microsoft website here. Enable the AD DS and AD LDS Tools. Once installed, you can access ADUC from your own workstation. You can learn more about using RSAT in this official Microsoft learn article by clicking here. Real-Life Application: Consider a situation where a new employee joins the company. As an administrator, you need to create a user account for them in AD. If you're using a Domain Controller, you would directly log into the server and create the account. Alternatively, with RSAT, you could remotely connect to AD from your workstation, create the new user account, and set up their permissions without needing physical access to the DC. This flexibility is particularly beneficial in larger organizations or when managing multiple domains across different locations. Accessing AD via RSAT is generally more convenient and secure, as it reduces the number of direct interactions with the Domain Controller, minimizing security risks. Additionally, RSAT allows administrators to manage their network from virtually anywhere, provided they have the necessary credentials and network access. This approach not only enhances efficiency but also allows for more flexibility in managing network resources. In the next section, we will explore the Active Directory interface and how to navigate through its various components to manage your network effectively. Once you've accessed Active Directory, either through a Domain Controller or using RSAT, the next step is to familiarize yourself with its interface. The primary tool for this is Active Directory Users and Computers (ADUC), a Microsoft Management Console (MMC) snap-in that you use to administer and publish information in the directory. Understanding ADUC: ADUC is where you'll spend most of your time managing AD objects like users, groups, and computers. Its interface is divided into several sections: The left pane (Console Tree): On the left side, you'll find the console tree which displays the AD domains, organizational units (OUs), and other containers. Details Pane: The middle section shows the contents of whatever is selected in the console tree, such as user accounts in a selected OU. Action Pane: On the right, the action pane offers quick access to common tasks relevant to the selected object. See the image below: The Active Directory Users and Computers Console Understanding Organizational Units (OUs): Organizational Units (OUs) are an essential aspect of the Active Directory structure. They are containers used to organize and group different types of objects within a domain, such as users, groups, and computers. Think of OUs as folders in a file system, where you can categorize and store related objects for easier management and application of policies. For instance, you might have an OU for the HR department, containing user accounts and computers specific to that department. This structure not only simplifies management by grouping relevant objects together but also helps in applying specific policies to those groups. Using the 'Find' Feature to Search for AD Users: A common task for administrators is locating specific user accounts within the Active Directory. The 'Find' feature in ADUC is a powerful tool for this purpose. Here's how to use it: Open ADUC and click on the 'Find' button in the toolbar, or right-click on the domain or OU and select 'Find'. In the 'Find' dialog box, ensure 'Users, Contacts, and Groups' is selected, and most important in the in field, make sure it shows your current domain or Entire Directory: Enter the criteria for your search. For example, you can search by the user's name, display name, or email address. Click 'Find Now' to execute the search. The results will be displayed in the dialog box. Active Directory Find Search Results This feature is particularly useful when dealing with a large number of users or when you need to quickly locate a specific account for tasks such as resetting passwords or updating user information. One of the primary functions of Active Directory (AD) is to manage user accounts and groups. This management includes creating, modifying, and removing accounts, as well as organizing users into groups for easier administration. Creating User Accounts: Creating a user account in AD is a straightforward process: Navigate to the Correct OU: In Active Directory Users and Computers (ADUC), locate the OU where you want to create the new user account. New User Wizard: Right-click on the OU and select 'New' > 'User'. This opens the New User Wizard, where you'll enter the user's details, such as their name and user logon name. Set Initial Password: Towards the end of the wizard, you'll set an initial password for the account and can choose whether the user must change the password at the next login. Managing Groups: Groups in AD are used to collect user accounts, computer accounts, and other groups into manageable units. Working with groups is similar to working with individual user accounts: Create a New Group: Right-click on the OU where you want the group and select 'New' > 'Group'. Name the group and define its scope and type. Add Members to the Group: Once the group is created, you can add members by opening the group's properties and navigating to the 'Members' tab. Practical Example: Imagine a scenario where a new marketing team is formed in your company. You would first create individual user accounts for each team member. Then, you would create a group called "Marketing Team" and add all the marketing team's user accounts to this group. This setup simplifies processes like assigning permissions or sending emails to the entire team, as you can now apply actions to the group instead of each user individually. Importance of Regular Maintenance: Regularly updating user information, resetting passwords, and cleaning up inactive accounts are critical for maintaining the security and efficiency of your AD environment. For instance, when an employee leaves the company, their user account should be disabled or removed to prevent unauthorized access. Organizational Units (OUs) are crucial for structuring and organizing resources within Active Directory (AD). They provide a means to group objects, such as users, groups, and computers, in a way that aligns with your organization's internal divisions, such as departments or geographical locations. OUs are not just for organization; they also play a key role in the delegation of administrative tasks and the application of group policies. Creating and Managing OUs: Decide on the Structure: Before creating OUs, plan a structure that mirrors your organization's needs. For example, you might create OUs based on departments (HR, IT, Sales), function (Servers, Workstations), or location (HQ, Branch Office A). Create an OU: In ADUC, right-click the domain or another OU where you want to create the new OU. Select 'New' > 'Organizational Unit', then give it a meaningful name. Populate the OU: Move or create objects (users, groups, computers) in the OU. This can be done by dragging and dropping objects into the OU or using the 'New' option to create new objects directly within the OU. Real-Life Scenario: Consider a growing company that just opened a new branch office. You might create an OU named "Branch Office B", then create or move user accounts and computer accounts specific to this new location into the OU. This structure helps in managing and applying policies specific to that office, such as security settings or software deployment, in an organized manner. Best Practices for OU Organization: Keep it Simple: Start with a simple structure that can grow with your organization. Avoid creating too many nested OUs, as this can become difficult to manage. Consistency is Key: Use consistent naming conventions and structures across your OUs for clarity and ease of management. Plan for Delegation: Consider which teams or individuals will need to manage resources within each OU. Proper OU structuring can make delegating administrative tasks more straightforward. Effectively using OUs in Active Directory not only brings order and clarity to your network's resources but also facilitates smoother, more efficient administration and policy application. As your organization evolves, so too can your AD structure, adapting to changing needs and complexities. Implementing best practices in Active Directory (AD) management is essential for ensuring a secure, efficient, and reliable network environment. Here are key strategies to help maintain and optimize your AD settings: Regular AD Backups: System State Backup: Utilize tools like Windows Server Backup to perform regular system state backups. This backup includes critical AD data. Automated Backup Schedules: Configure automated backup schedules, ensuring consistent backups are taken without the need for manual intervention. This can be done through the Task Scheduler or backup software. Monitoring and Reviewing AD Event Logs: Regular Checks with Event Viewer: Use the Event Viewer on domain controllers to regularly monitor AD-related logs, focusing on the Directory Service and DNS Server logs. Alert Configurations: Set up alerts for critical errors or specific event IDs related to AD. This proactive approach helps in quickly identifying and addressing potential issues. Keeping AD Servers Updated: Regular Windows Updates: Consistently apply Windows Updates on your domain controllers. This practice is crucial for patching security vulnerabilities and updating AD features. Scheduled Maintenance Windows: Establish regular maintenance windows for applying updates, ideally during off-peak hours to minimize user impact. Enforcing Strong Password Policies: Use Group Policy: Implement password policies using Group Policy. Define rules for password complexity, change frequency, and history to enhance network security. User Education: Regularly educate users on the importance of strong passwords and secure practices. This human element is often the first line of defense against security breaches. Regular AD Cleanup and Maintenance: Removing Obsolete Accounts: Periodically review and clean up old user and computer accounts. This practice prevents potential security risks associated with inactive accounts. Consistency Checks: Regularly perform consistency checks on your AD database to identify and rectify discrepancies or anomalies. Delegation of Administrative Roles: Role-Based Access Control: Implement role-based access control to delegate specific AD tasks. This approach minimizes the risk of errors and security breaches by limiting the scope of access based on user roles. This is all you need to get started working with Active Directory. If you're interested in learning more and getting your hands on Active Directory with our interactive IT labs, consider creating a free account which will get you access to our Active Directory Fundamentals course! Changing the IP address of a domain controller is a non-standard operation that could disrupt domain services and affect client connectivity. However, if properly planned and executed,...0 Facebook Twitter Google + Pinterest Time synchronization in an Active Directory is critical to properly functioning of the domain services and security mechanisms. If a proper and reliable time sync scheme is not configured in...1 Facebook Twitter Google + Pinterest Only the most basic password length, frequency, and complexity requirements can be enabled for domain users in the default Active Directory password policy. Enabling the mandatory password complexity option, which...0 Facebook Twitter Google + Pinterest There are several ways to prevent certain Group Policy Object (GPO) settings from being applied to specific users and/or computers in Active Directory: Use GPO security filtering to control which...6 Facebook Twitter Google + Pinterest When attempting to join a computer to an Active Directory domain, an error may occur: Error 0xaac (2732): NERR AccountReuseBlockedByPolicy: An account with the same name exists in Active Directory. Re-using...1 Facebook Twitter Google + Pinterest In the previous post, we covered how to deploy a centralized log collection and management service based on the Graylog stack (Graylog + OpenSearch + MongoDB). Now let's cover how...4 Facebook Twitter Google + Pinterest The password policy, which is enabled by default in Active Directory, sets a maximum age for a user's password. If the password age exceeds this value, it is considered expired,...11 Facebook Twitter Google + Pinterest In this article, we'll look at how to use the official Microsoft HardwareReadiness.ps1 PowerShell script to perform a bulk Windows 11 hardware compatibility check on domain computers. 3 Facebook Twitter Google + Pinterest Two special Windows Server DNS features can be used to automatically clean up old DNS records in Active Directory: DNS Aging - allows to determine the age of the dynamically...5 Facebook Twitter Google + Pinterest A user account lockout in a domain is one of the most popular reasons why users contact the technical support team. In most cases, the lockout is caused either by...3 Facebook Twitter Google + Pinterest Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, or build upon the material you have to pick a domain name to use. It is recommended to use a subdomain of a routable domain name. For example, ad.activatedirectorypro.com is a subdomain of activatedirectorypro.com and est.ad.activatedirectorypro.com are part of the same domain tree. The schema is a set of rules that defines the classes of objects and attributes contained in the directory. A global catalog contains information about every object in the directory. This allows users and administrators to find directory information regardless of which domain in the directory actually contains the data. By default the first domain controller in a domain is designated as the GC server; it is recommended to have at least one GC server for each site to improve performance. The replication service synchronized the Active Directory database with other domain controllers. Active Directory is typically deployed with two or more domain controllers for redundancy reasons. When you create an account on one Domain controller it is replicated to the other one. If one domain controller goes down the other one will have a copy of the database. In the above diagram, if a user is added to DC1, it will be copied to DC2 and vice versa. Active Directory sites are used to control how Active Directory works. Jim was recently hired as an accountant for Active Directory Pro. The IT administrator creates an account for Jim in Active Directory, the account is unique to Jim and contains details such as first name, last name, office, phone number, etc. Jim is provided with a username and password so he can log into the company's network. Jim logs into his laptop with the provided username and password. The login request goes to the Active Directory server to verify Jim's username and password. Active Directory looks up Jim's account and verifies the username and password. The account has been verified, Jim is now logged into his laptop and is authenticated to the domain. In this example, the Active Directory server will authorize access to network resources. Jim logs into his computer using his username and password and wants to access his email, a contract file, and the accounting database server. These network resources check with Active Directory to see if Jim's account is authorized for access. Active Directory verifies Jim's account is authorized for access. Jim's account is granted access. Jim can now check email, modify the contract file and work on the database server. In this last example, we will look at another user that has mixed access (allow and deny permissions. Pam logs into the network with her username and password. She tries to access the same resources as Jim (email, a contract file, and a database server. ) These network resources check with Active Directory to see if Pam's account is authorized for access. Active Directory verifies Pam's account (Authentication). AD also checks what resources Pam's account has access to (Authorization). Pam can now access email and the contract file but does not have permission to access the accounting database server. In all of the above examples, Active Directory works by providing authentication and authorization to users and network resources. No matter what technical jargon you hear, that is the core function of Active Directory. It is important to note that these network resources must be configured to use Active Directory. The resources are typically joined to the Active Directory server (but not all systems require this). There is a lot of configuration and planning that goes into configuring an Active Directory server. Organizations typically have dedicated professionals to implement and manage these systems. In the next section, we will explore how Active Directory works. Active Directory is a directory service created by Microsoft for Windows domain networks developed by Microsoft which comes as a set of processes and services with most Windows Server operating systems. At first, Active Directory was exclusively responsible for domain management. Active Directory, on the other hand, has come to represent a wide range of directory-based identity-related services.A domain controller is a server that runs the Active Directory Domain Service (AD DS) role. In a Windows domain network, it authenticates and authorizes all users and computers. Creating and enforcing security policies across all computers, as well as installing and updating software. For example, when a user enters into a Windows domain machine, Active Directory analyses the submitted password and decides the user is a system administrator or a regular user. It also enables for information management and storage, as well as authentication and authorization processes and other related services, such as Certificate Services, Active Directory Federation Services, Lightweight Directory Services, and Rights Management Services are all built on top of this framework. Active Directory Services Multiple directory services are included in Active Directory Services. Active Directory Domain Services, sometimes known as AD DS or just AD, is the most well-known. Every Windows domain network is built on the foundation of Active Directory Domain Services (AD DS). It keeps track of domain members, such as devices and users, verifies their credentials, and establishes their access privileges.This service is run by a domain controller, which is a server. When a user signs into a device, connects to another device over the network or runs a line-of-business Metro-style app on the device. Domain Services is used or relied on by other Active Directory services and most Microsoft server technologies.Encrypting File System, BitLocker, Domain Name Services, Remote Desktop Services, Exchange Server, and SharePoint Server are just a few examples. Self-managed AD DS should not be confused with Azure AD DS, which is a cloud-based service. Lightweight Directory Services Active Directory is a directory service that allows you to Active Directory Application Mode (ADAM), formerly known as Lightweight Directory Services (AD LDS), is an LDAP protocol implementation for AD DS. On Windows Server, AD LDS runs as a service. It includes a Data Store for directory data storage as well as a Directory Service with an LDAP Directory Service Interface. Multiple AD LDS instances, unlike AD DS, can run on the same server. On-premises public key infrastructure is created using Active Directory Certificate Services (AD CS). It may generate, validate, and revoke public key certificates for an organization's internal use. Files (when used with Encrypting File System), emails (per the S/MIME standard), and network traffic (when used by virtual private networks, Transport Layer Security protocol or IPsec protocol) can all be encrypted with these certificates.Although AD CS predates Windows Server 2008, it was previously known as Certificate Services. Active Directory Federation Services (AD FS) is a single sign-on service for Active Directory users. Users can utilize several web-based services (e.g., internet forum, blog, online shopping, webmail) and network resources with only one set of credentials kept centrally, rather than having to be issued a separate set of credentials for each service, with AD FS infrastructure in place.The role of AD FS is to extend the functionality of AD DS, which allows users to authenticate with and use devices on the same network using a single set of credentials. They can utilize the same set of credentials in a different network with the former. AD FS is built on the concept of federated identification, as the name suggests. Rights Management Services Before Windows Server 2008, Active Directory Rights Management Services (AD RMS) was known as Rights Management Services or RMS. It is a server software for managing information rights that comes with Windows Server. It restricts access to documents such as corporate e-mails, Microsoft Word documents, and websites and the actions that authorized users are allowed to carry out on them using encryption and a sort of selective capability denial. Trusting Terminology Trusts are used by Active Directory to control resource access privileges between domains. Trusts come in several different types: One-way Trust When a first domain grants access privileges to users on a second domain, this is known as a one-way trust. The second domain, on the other hand, does not allow users from the first domain to access it. Two-way Trust When there are two domains, each of which enables access to users from the other domain, this is known as a two-way trust. Trusted Domain A trusted domain is a single domain that grants users access to a second domain. Transitive Trust A transitive trust can span more than two domains and grant access to other trusted domains in the forest. Intransitive Trust A one-way trust that is limited to two domains is known as an intransitive trust. Explicit Trust A network admin creates an explicit trust, which is a one-way, nontransitive trust. Cross-link Trust A sort of explicit trust is a cross-link trust. Cross-link trusts exist between domains that are either in the same tree, with no child-parent relationship, or in distinct trees. Forest Trust A forest trust is a one-way, two-way, or transitive, and it can apply to domains within the entire forest. Shortcut A shortcut connects two domains from different trees. One-way, two-way, and transitive shortcuts are all possible. Realm A realm is a one-way or two-way trust that might be transitive, intransitive, or both. External Trust An external trust is a trust that connects domains from other forests or non-AD domains. External trusts can be one-way or two-way, nontransitive or transitive. Private Access Management (PAM) Trust A one-way trust is a private access management trust. Between a production forest and a bastion forest, Microsoft Identity Manager creates it. Features of Active Directory Domain Service To coordinate networked pieces, Active Directory Domain Services uses a tiered structure consisting of domains, trees, and forests. Domain A domain is a collection of things that share the same Active Directory database, such as users or devices. The domain name system (DNS) is a system that organizes domains. Tree One or more domains are grouped together to form a tree. A continuous namespace is used to organize the collection of domains into a logical hierarchy in the tree structure. Trees can be considered as trust relationships in which two domains share a secure connection, or trust. Multiple domains can be trusted, with one trusting the other and the second trusting the third. The first domain can implicitly trust the third domain due to the hierarchical nature of this system. Forest A forest is a collection of trees. A forest is made up of catalogs, directory schemas, application data, and domain configurations that are all shared. In a forest, the schema defines an object's class and attributes. Furthermore, global catalog servers keep track of all the objects in a forest. The forest is Active Directory's security border, according to Microsoft. Organizational Units Users, groups, and devices are organized under Organizational Units (OUs). Each domain is allowed to have its own OU. However, because each user or item in a domain must be unique, OUs cannot have separate namespaces. Containers Containers are comparable to organizational units (OUs), except GPOs cannot be applied to or linked to container objects. Benefits of Active Directory Active Directory offers a number of functional and business advantages, including the following: Security - Access to network resources is controlled by Active Directory, which helps enterprises ensure security. Extensibility - Active Directory data may be easily organized to correspond with an organization's structure and business demands. Simplicity - Administrators can manage user identities and access privileges across the enterprise from a single location, making management easier and lowering operational costs. Resiliency - To ensure high availability and business continuity, Active Directory enables redundant components and data replication. ConclusionActive Directory is a widely used directory service. It aids in the organization of your company's users, computers, and other assets. Your company's full hierarchy is organized using AD, from which PCs belong on which network to what your profile picture looks like and which users have access to the storage area. Monitor Your Entire Application with Atatus Atatus provides a set of performance measurement tools to monitor and improve the performance of your frontend, backends, logs and infrastructure applications in real-time. Our platform can capture millions of performance data points from your applications, allowing you to quickly resolve issues and ensure digital customer experiences. Atatus can be beneficial to your business, which provides a comprehensive view of your application, including how it works, where performance bottlenecks exist, which users are most impacted, and which errors break your code for your frontend, backend, and infrastructure. Try your 14-day free trial of Atatus.