I'm human

Active Directory Tutorial Setting up Active Directory and Domain Services for efficient network organization is crucial for administrators. This involves organizing resources, enforcing security policies, and using Group Policy Objects to manage the network. To begin, ensure Windows Professional or Enterprise is installed, then enable Remote Server Administration Tools by right-clicking on the Start button, selecting Settings > Apps > Manage optional features, and installing RSAT: Active Directory Domain Services and Lightweight Directory Tools. For older versions of Windows, such as Windows 8 and 10 Version 1803, follow a different process: download and install the correct version of Server Administrator Tools, then right-click on the Start button to access Control Panel > Programs > Programs and Features > Turn Windows features on or off. Select Remote Server Administration Tools, click Role Administration Tools, select AD DS and AD LDS Tools, and verify that AD DS Tools is enabled. Setting up a Domain Controller involves assigning a static IP address and installing Active Directory Domain Services or ADDS. Open Server Manager, click Roles Summary, add roles and features, select Remote Desktop Services installation if necessary, and then select Active Directory Domain Services. Leave the Features checked by default, press Next, and restart the destination server if required. Once installed, promote this server into a domain controller by pressing Promote this server to create a new forest, entering a Root domain name, and selecting the desired Domain functional level. To set up a domain controller on Windows Server 2016, first ensure your system can reboot after installation. Follow these steps: Open Server Manager, click Manage, and then Add Roles and Features. Select Role-based or feature-based installation and proceed with the next button until you reach AD DS screen. Here, select Next to install Active Directory Domain Services. Once installed, you'll see a notice prompting additional steps; click on Promote this server to a domain controller. This brings up the Deployment Configuration screen. Leave the Add a domain controller to an existing domain option active and enter the Administrator account's username and password in the format \Administrator. Decide whether to make the new DC a read-only one, then choose your original DC for replication purposes. Review options carefully before clicking Next. The system will perform prerequisites checks; if successful, click Install. Wait for the installation to complete, then reboot the computer. Log back in and verify your new domain controller is listed under Domain Controllers folder on Active Directory Users and Computers of the original DC machine. To set up new user accounts, follow these simple steps. The most efficient way to manage users is through the Active Directory Users and Computer or ADUC tool that comes with the Remote Server Administration Tools or RSAT pack. To install ADUC on Windows 10 Version 1809 or higher, click Settings > Apps, then Manage optional features > Add feature, select RSAT: Active Directory Domain Services and Lightweight Directory Tools, and follow the prompts. For older versions of Windows, right-click on Start > Control Panel > Programs > Programs and Features > Turn Windows features on or off, scroll down, and check Remote Server Administration Tools. Expand Role Administrator Tools > AD DS and AD LDS Tools, and select AD DS Tools. To create new users with ADUC, open the Server Manager, go to Tools menu, select Active Directory Users and Computers, expand the domain, click Users, right-click on the right pane, press New > User, fill in required information, and follow the prompts. It's also essential to monitor Active Directory for any security issues. Some important network events to watch out for include a replay attack detection (event ID 4649), system audit policy change (4719/12), SID History added to an account (4765), and potential DoS attacks (550). Understanding the forest and tree structure in Active Directory is also crucial, as it helps with managing domains, trust relationships, and hierarchy management. A forest is a group of connected domains, while a tree is a single domain or group of objects that are followed by child domains. Each tree within a forest connects through trust relationships, allowing different domains to share information seamlessly. One unified database with forests and trees structured in a hierarchy, where forests are at the top and trees are at the bottom. Managing multiple forests for network administration can be challenging. When choosing between single or multi-forest designs, administrators must consider simplicity versus security and manageability. To find account lockouts in Active Directory, using the Event Viewer is recommended. The PDC Emulator domain controller's address should be noted, and then the standard event log viewer can be used to filter current logs for event ID 4740 within a specific time frame or for a particular user or resource. Active Directory management tools like ManageEngine AD360 offer automation of tasks such as enforcing multi-factor authentication, auditing AD objects, detecting inactive accounts, and analyzing user behavior. However, this package might not be necessary if only one component tool is required. ManageEngine AD360 offers a 30-day free trial for its services. Trust relationships between Active Directory domains are crucial, with two types: transitive and non-transitive, affecting how domains can trust each other's users and resources. Trusted relationships between domains enable secure communication and access to shared resources. These trust relationships come in two forms: one-way and two-way. A one-way trust allows a domain to authenticate against another, while a two-way trust enables both domains to accept each other's authentication details. Within a trust, domains are categorized as trusting or trusted. Active Directory offers various types of trusts, including parent-child, tree-root, external, realm, forest, and shortcut trusts. Each type has its unique characteristics and use cases. To set up trusts in Active Directory, users can utilize the New Trusts Wizard. This wizard allows administrators to create new trust relationships, view existing trusts, and select the type of trust they want to establish. For optimized performance and regulatory compliance, generating reports on Active Directory is crucial. SolarWinds Access Rights Manager (ARM) is a powerful reporting tool that provides visibility into directory credentials management and usage. With ARM, users can detect insecure configurations, credential abuse, and potential cyber attacks. The platform also offers preconfigured reports for compliance demonstration. While SolarWinds Access Rights Manager is an in-depth platform requiring time to learn, it provides valuable features like visualizations, automatic mapping, and preconfigured reports, making AD management easier. 1. To protect your network from cyber threats, regularly monitor key directory events and use a directory monitor in Active Directory. 2. A domain is a collection of objects like users, computers, and devices that share the same access rights managed by the Active Directory database. 3. The domain controller manages authentication management for the domain's database objects using Active Directory functions. 4. To start security auditing in Active Directory, log in to Windows Server as an administrator, go to Group Policy Management Console, select the desired domain/OU, and edit the Group Policy Object. 5. In the Group Policy Management Editor, navigate to Audit Policies, select both Success and Failure options for Audit object access and Audit directory service access. 6. Active Directory is an open standard that outlines how access rights can be managed through the Lightweight Directory Access Protocol (LDAP). 7. Single sign-on (SSO) allows users access to multiple systems with just one authentication procedure, which Active Directory can implement. 8. When selecting an Active Directory tool, consider factors like ease of use for auditing, tracking capabilities, and value for money. 9. Active Directory was first released with Windows Server 2000, providing authentication and authorization to users on the network. 10. The core function of Active Directory is to authenticate and authorize users, granting or denying access to resources based on user credentials. Active Directory: Understanding the Core Functionality Active Directory is still widely used by most medium and large organizations, despite the push towards cloud-based solutions, particularly in a hybrid mode where local directories are synced with cloud services to provide seamless authentication for Office 365 resources. To grasp how Active Directory operates, let's examine some examples. When an account is created for a new user, such as Jim, the IT administrator provides a unique username and password that allows access to the company network. Upon logging in, the logon request is sent to the Active Directory server, which verifies the credentials by looking up the user's account details. If authentication is successful, the account is granted access to domain resources. In this scenario, when Jim attempts to access his email, contract file, and accounting database server, these resources check with Active Directory to verify if his account has permission for access. Once authenticated, Jim's account is authorized to access these resources, enabling him to perform tasks such as checking email, modifying files, and working on the database server. In contrast, when another user, Pam, logs in and attempts to access the same resources, but without proper authorization, Active Directory verifies her credentials (authentication) and checks which resources she has access to (authorization). If Pam's account lacks permission for a particular resource, such as accessing the accounting database server, Access is denied. At its core, Active Directory provides authentication and authorization services to users and network resources. While extensive configuration and planning are necessary to implement an Active Directory server, dedicated professionals often manage these systems within organizations. The Network Users Authorization Service grants or denies access to network resources. To avoid confusion, it's essential to understand three key terms: Active Directory (AD), AD Domain Services (AD DS), and Domain Controller (DC). AD refers to the abbreviation for Active Directory, while AD DS is a server running the Active Directory Domain Services Role, and DC is a server running the same role as AD DS. A Domain Controller is equivalent to a server running AD DS. When installing Active Directory, you'll install the AD DS Role on a Windows server. The main components of AD DS will be discussed, showcasing its complexity. The logical structure of Active Directory organizes resources in a hierarchical manner, helping to define relationships, control security boundaries, and organize objects. The forest is the top-level container, comprising multiple domains sharing directory schema, configuration, and global catalog. Domains within the same forest have a two-way transitive trust. The root domain is a logical structure containing containers and objects within Active Directory. A domain consists of a hierarchical structure for users, groups, computers, and other objects; security services providing authentication and authorization to resources; policies applied to users and computers; and a DNS name identifying the domain. When logging into a computer within a domain, you're accessing the corresponding DNS domain name (e.g., ad.activedirectorypro.com). During Active Directory installation, you must select a domain name, preferably a subdomain of a routable domain name. The initial installation creates a forest and root domain. Child domains share the same domain name space as the root domain and have their own collection of objects. Trees are sets of connected domains, with each addition creating a domain tree. A schema is a set of rules defining object classes and attributes in the directory. A global catalog contains information about every object in the directory, allowing users to find directory data regardless of the domain containing the data. By default, the first domain created will be the root domain. Having at least one GC server per site is crucial for improved performance in a domain. The replication service synchronizes the Active Directory database across multiple domain controllers to ensure redundancy. When an account is created on one DC, it's replicated to another, providing a backup in case one DC goes down. In the diagram, adding a user to DC1 is mirrored in DC2, and vice versa. Active Directory sites combine multiple DCs into logical containers based on physical location. Sites optimize Active Directory performance for branch offices and multiple domain controllers. Active Directory is a powerful tool for managing user authentication and authorization. It enables organizations to provide employees with secure access to network resources by storing their account information in a centralized database. User accounts can be assigned to individual employees or shared among multiple users, providing details such as name, address, manager, and more. Security groups simplify permission management by grouping users or computers together, making it easier to manage access to specific resources. For instance, creating a group for 20 people who need access to a file eliminates the need to manage individual accounts. When a computer joins an Active Directory domain, a trusted computer object is created, allowing users to log in and access network resources if authorized. Organizational units (OUs) organize Active Directory objects, making it easier to administer policies and apply settings. The primary benefit of Active Directory lies in its centralized management capabilities. This includes the centralized management of user accounts, permissions, and policy settings. By using Active Directory, administrators can create and manage all user accounts from a single location, eliminating the need for manual account creation on each device or system. Without an Active Directory server, managing employee access to network resources would be a tedious and time-consuming task. With 100 employees needing access to the network, an administrator would need to create individual accounts on each system, resulting in a massive administrative burden. Active Directory also enables centralized control and management of permissions to network resources through security groups. For example, multiple users can be added to a group requiring access to accounting resources, streamlining permission management and reducing administrative tasks. Adding users to an Active Directory security group is the simplest way to grant access to shared resources like files and folders. This approach makes it easy to manage permissions by adding or removing user accounts from the group. When a user leaves or needs permission removed, simply remove them from the group. In an Active Directory environment, Group Policy allows administrators to apply policy settings to users and computers in bulk. For instance, if all employees need to change their passwords every 60 days, you can configure a password policy using Group Policy, which will be automatically applied to all users. Without Active Directory or Group Policy, managing policy settings on individual computers would become unmanageable in large environments. Organizations that are entirely cloud-based use Microsoft Intune for policy management, which can also be used in hybrid setups. This lesson covers the various tools available for managing Active Directory. Most of these tools come bundled with Active Directory installation on a server and can be accessed under the "Windows Administrative Tools" folder. You can install RSAT (Remote Server Administration Tools) on another computer to access these management tools remotely. The main tool used to create, manage user accounts, computers, and groups is the ADUC (Active Directory Users and Computers) console. This is where you'd create a new user account, set their password, and add them to relevant groups. You can also use this console to organize your objects into Organizational Units (OUs). The ADAC (Active Directory Administrative Center) tool was introduced with Server 2008 R2 and higher but seems to be less widely used than ADUC. Other tools include the Dsreplicator console for raising domain or forest mode, managing trust relationships, and the Sites and Services console for managing your sites and subnets. Group Policy provides centralized management of policy settings for users and computers in an Active Directory environment. Understanding how to use Group Policy is crucial for System Administrators. For a deeper dive into Group Policy Management, see the linked guide. The DNS console is used for creating and managing DNS zones and resource records, which are essential for Active Directory functionality. It's included with AD installation but knowing basic DNS concepts is vital for working with Active Directory. Lastly, PowerShell is a command-line tool that allows administrators to automate routine tasks such as creating, updating, or removing user accounts, computers, groups, and more efficiently. As a seasoned System Administrator/Manager, I've managed numerous Active Directory environments throughout my career. However, I soon realized that the built-in tools provided by Microsoft were lacking in several key areas, including bulk management and reporting capabilities. PowerShell can be useful for automation, but it often requires significant time and effort to master. That's why I created the AD Pro Toolkit - a collection of Active Directory Management Tools designed to simplify and streamline administration tasks. In addition to the AD Pro Toolkit, there are several other Active Directory services that can be installed on your Windows server. These include: * Certificate Services: used for managing and deploying certificates, which enable secure digital signing and encryption of documents and network traffic * Federation Services: providing Single Sign-On (SSO) capabilities for user accounts accessing web-based applications like Office 365 * AD LDS (Active Directory Lightweight Directory Services): offering directory services for applications, as well as data storage and access services via standard APIs. This service also encrypts documents and limits access to sensitive content Meanwhile, Azure Active Directory has been rebranded as Entra ID - a cloud-based identity and access management service that authenticates users accessing cloud-based applications like Office 365, Azure, and other SaaS apps. Active Directory can be deployed in three modes: on-premises (ADDS), cloud-based (AAD), or hybrid. In the latter configuration, local AD is synced with Azure AD using Azure AD Connect software, allowing for single sign-on to both on-premises and cloud resources. However, note that this sync is one-way only - Azure AD does not sync with local AD. To learn more about Azure Active Directory, I recommend consulting Microsoft's official article: "What is Azure Active Directory?"