Abstract

The invention of the first mechanical computer by Charles Babbage in 1882 has innovated not just lives but also corporations and governing bodies. Almost a century later Bill Gates and Paul G. Allen pushed the envelope and developed the first MS-DOS (Microsoft Disk Operating System) by improving on the *BASIC* mainframe language. Microsoft had complete control over the personal computer consumer market due to how successful their product was, but success is always followed by competition. Bill Gates and co strived to maintain their monopoly of the market, but other companies like RISC and Unix followed suit to challenge Microsoft for the top spot. The only way to defeat both RISC and Unix were to create a product that was appealing to corporate customers. Which also implied that Microsoft would need to improve on security, hardware power, reliability, and redundancy. This series of events ultimately led to the introduction of the Windows NT operating system which is deemed as the first version of Windows Server. The paper examines Active Directory and its core processes in relation to Windows Server.

Introduction

Windows Server has become the industry standard specifically the 2016 version which includes Active Directory, DNS Server, DHCP Server, and Hyper-V Network virtualization. It supports enterprise-level management consisting of data storage, communications, and applications. It was first released on September 26, 2016, at the Ignite conference which is hosted by Microsoft, and Microsoft Server 2016 developed simultaneously with the Windows 10 operating system. The core feature that is widely used the most is Active Directory. A directory service or also known as a name service is responsible for mapping names of network assets to network addresses. Active Directory consists of multiple directory services constructed by Microsoft to maintain and manage Windows domain networks.

Domain and Services

Active Directory Domain Services is the core function and the most popular directory services and considered the foundation of Windows domain networks. It is a system that is used to store data containing users, devices, credential, and access rights. The logical structure of Active directory consists of objects, which is a single entity that could be a user, computer, security group, or printer and has its own

unique attributes. There is a possibility that an object itself can contain another object, and the framework that contains these entities have different levels. The logical divisions of Active Directory are known as the forest, tree, and domain. A forest is a grouping of trees that share a logical structure, global catalog, schema, and directory configuration. Global catalog allows a domain controller to share information and resources to objects that are located in the forest, even if that object is not located in the domain. Next, a domain is a group of network objects like computers and users that have the same Active Directory database. Finally, a tree contains one or more domain that are linked through a trust hierarchy.

Trusts and Schema

Active Directory trusts are bridges that establish a connection between different domain in an Active Directory network. Data cannot be shared between several domains without a trust established. There are two different classifications for Active Directory trusts known as transitive and non-transitive. Transitive trusts simply means that if two domains connect to one another, then those domains can also connect to other domains that each other has established a trust with. For example, if domain A has a trust with domain B and domain B has another trust with domain C then domain A can connect to domain C without having to establish a connection with domain C first. On the other hand, non-transitive trusts are the complete opposite which means that domains cannot extend beyond their original connection. The blueprint that explains the methods and regulations of what types of objects and its attributes can be stores in Active Directory is known as the schema. The core structure of a schema object is divided into objects, classes, and attributes. Just like previously described an object is an entity of data storage in Active Directory and a class is a grouping of object definitions that is the rubric for object creation. An attribute is the data that is stored inside a class and can belong to several different classes.

Group Policy and Organization Units

Groups of objects that exist in a domain are contained in an organization unit (OU). Organizational Units help provide a hierarchy in a domain to make it an easier to manage and maintain. If all of users, computers, and printer objects were all placed in the same folder per se, it would be extremely difficult to administer. This is

why organizational units exist is an important feature in Active Directory. Organizational units can also contain organizational units just like how folders can have folders within itself. Microsoft recommends that users and computers configurations should be applied at the organizational unit level, so it's applied to every object inside the organizational unit. These configurations for computers and users can be created in the Group Policy console and its main goal is to simplify administrative tasks and ultimately reduce cost, because without Group Policy system administrators would have to access every single computer and user in a domain manually order to configure it. This would take an absurd amount of time in order to keep a singular task completed, because an enterprise level system would have a numerous number of users and computers in its domain. The physical structure of Active Directory is prominent through the use of Active Directory sites which is simply a connected network through Internet Protocol subnets. An Active Directory site will be mapped to a domain, while an Active Directory domain can contain several sites mapped to it. Site link objects are necessary in order to form a link between Active Directory sites, in order for replication to occur. Active Directory replication is simply a process where data is transferred between domain controllers, and without replication two domains cannot share information. A site link bridge is used to connect group of site links that are already linked together. Also, site links are transitive so if site A and site B are linked together then site C is also linked to site A and so on. There are two types of replications that can occur in an Active Directory environment: intra-site replication and inter-site replication. Intra-site replication plainly means that replication is transpiring between domain controllers that are placed in the same site, whereas inter-site replication is replication between domain controllers that are in different sites. Through Active Directory Sites and Services console system administrators can view, modify, delete, and add sites and networks.

Active Directory Consoles

There are several management tools in Active Directory to automate tasks and make it easier for system administrators to do their jobs. One of the most important one is Active Directory Administrative Center (ADAC) which is a tool developed by Microsoft to help administer objects in Active Directory. ADAC is a graphical user interface built on Windows PowerShell, so whenever an event occurs

cmdlets are responsible for execution and runs in the background. Active Directory Users and Computers (ADUC) is a Microsoft Management Console snap in that exists in Active Directory. It can be used to manage user and computer objects, organization units, and their attributes. ADUC can also be used to administer FSMO server roles. Active Directory Domains and Trusts is a Microsoft Management console that is used to manage domain trusts, domain and forest functional level, and User Principal Names. A forest functional level implement features that affects every domain within a forest, while a domain level functional level enables features that affect only everything within the domain. A user principal name is used to validate users on a Windows operating system.

FSMO Roles

First, the Flexible Single Master Operations role also known an FSMO role is a group of roles that can be assigned to a domain controller to make up an Active Directory system. Microsoft previously had a Single Master Model for Active Directory, which means that one domain controller had the rights to make changes in a domain. This process was not fault tolerant so if that specific domain controller went down, then no changes could be made in the domain until it was fully back up. This fundamental flaw was replaced with the introduction of FSMO roles and separated responsibilities across several domain controllers inside a domain. Next, a Schema Master FSMO role administer the read-write copy of an Active Directory schema. It defines every single attribute like phone number, email address, login name, etc. These pre-defined attributes can be used to apply to an object in Active Directory, also there should be one Schema Master per forest. After that, the Domain Naming Master FSMO role makes sure there cannot be a secondary domain that contains the same name as another domain and it's responsible for everything to do with domain names. There should be one per forest and can exist on domain controller that has another role since domain names aren't changed very frequently. Then, the Relative ID Master FSMO role is responsible for assigning security identifiers to different domain controllers in order to be used on newly created objects. Every object in Active Directory is assigned a security identify and the Relative ID Master role helps prevent objects from having the same security identify. There should be one Relative ID Master per domain. Also, the Primary Domain Controller Emulator FSMO role is the authoritative domain controller in a domain,

and its responsibly for password changes, Group Policy objects, and authentication requests. It also tells all the other domain controllers in the domain what time it is, and there should be one Primary Domain Controller Emulator role per domain. Finally, the Infrastructure Master FSMO role makes sure that objects across domain controllers can be referenced properly and also processes updates for objects in a domain. For example, a user from a domain controller will be able to be added to a different security group in another domain controller through this role. FSMO roles help a domain function properly even if a domain controller goes down.

Conclusion

Windows Server 2016 is detrimental to the functions of an enterprise and provides delegated control of applications, data storage and networks. System administrators are required to have an expertise in Windows Server 2016 and also Windows PowerShell. Although, there are several Linux systems that are used by corporations, However Microsoft is still the leading supplier of enterprise systems across the world. This research paper helped illustrate the technicalities of Active Directory and how it is built precisely to support several aspects of an enterprise system.

Works Cited

"Active Directory Domain Services Overview." Microsoft Docs, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

"Understanding the Active Directory Logical Model." Microsoft Docs, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-
active-directory-logical-model.

Deland-Han. (n.d.). *Active directory flexible single master operation (FSMO) roles in windows - windows server*. Active Directory Flexible Single Master Operation (FSMO) roles in Windows - Windows Server | Microsoft Learn. Retrieved November 10, 2022, from https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles

"Windows Admin Center Overview." Overview | Microsoft Docs, https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/overview.

Archiveddocs. (n.d.). *Group policy overview*. Microsoft Learn. Retrieved November 7, 2022, from https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)

Wil Jia. (n.d.). What are intra site and Inter site? Retrieved September 27, 2022, from https://social.technet.microsoft.com/Forums/windows/en-US/6f108dd5-759b-4fb8-8292-832be4eb20f6/what-are-intra-site-and-inter-site?forum=winserverDS

Encyclopædia Britannica, inc. (n.d.). *Microsoft windows*. Encyclopædia Britannica. Retrieved September 17, 2022, from https://www.britannica.com/technology/Microsoft-Windows