An Evaluation of the Impact of Utilizing Active Directory in Place of Workgroups

7/15/2022

Daniel Moreno

Recently, Always Fresh Foods Inc. experienced an unfortunate information security breach that resulted in the loss of proprietary data. This prompted a full investigation into the company's network and policies. As part of this investigation, I received the task of researching Active Directory as a potential solution to some of the network's current vulnerabilities and flaws. In addition, I identified possible changes to certain procedures that must occur if the company elects to proceed with the transition. The following will be the summary of a detailed evaluation of the flaws in the current system, improvements offered by Active Directory, and the alterations for four procedures.

Currently, the company's network consists of 8 servers and 25 workstation computers located at the central headquarters located in Colorado, along with additional remote workstations from warehouses situated in Nevada and Virginia. The computers utilized by employees at the regional warehouses connect to the central network through the use of a Virtual Private Network (VPN). The central network's devices have been networked together with a workgroup. This workgroup has established a peer-to-peer (P2P) mesh network without centralized controllers or users. The absence of a "trusted managing authority" creates instability and allows attackers to connect without authenticating themselves (Wararkar et al.). An attacker can listen to, jam, or inject messages into the network (Wararkar et al.). Malware, like a worm, may spread itself throughout the network due to the lack of oversight or filtering mechanisms, like firewalls. A P2P network possesses additional problems from an administrative and productivity perspective. The network will quickly drain the bandwidth supplied by the cables, as every device needs a direct connection to all other hosts (Gaille). Each

employee requires a distinct account on every host in the network. This necessitates separate administration on all hosts and forces the employees to remember and change different passwords on each one, since the account passwords will not synchronize. This wastes man-hours as the employees alter the password on each host when they expire (“What is a Workgroup and How Is It Set Up?”). In addition, employees exhaust time attempting to find shared files and resources which could be located on any of the hosts.

As instructed, I then proceeded to investigate the potential of Active Directory (AD) to solve the identified issues with the current network design. Microsoft offers a proprietary directory service that provides a hierarchical structure to store data and serve it to network users (Foulds et al.). Similar to the current system, files and resources would be stored on the servers. However, the logical star topology of an AD network allows employees to access these objects through the domain controller (DC), a dedicated server that manages an AD network (Lammle 13-14; Solomon 30). In addition to saving time and streamlining cooperation, this system would simplify the creation of secondary copies and the encryption of mission-critical files (“What is Active Directory?”; Shelladmin). Especially when dealing with remote connections like the company’s regional warehouses, AD networks increase in scale easier and cheaper than P2P networks where the number of wires required to form the connections increases along an exponential curve (Lammle 15; Shelladmin). AD would permit the company to centralize the authentication of users and the authorization of resources, allowing administrators to make a change in one location and automatically propagate it throughout the network (“What is Active Directory?”). In addition, this creates the

potential to implement Single Sign-On (SSO) for the company's network. With SSO technology, a user provides their credentials to be authenticated once and receives a token that allows them to access everything they require without needing to be authenticated again. Besides saving computing resources, SSO permits users to access files faster and makes security measures, like multi-factor authentication or password complexity requirements, more tolerable for users ("Benefits of Active Directory Domain Services (AD DS)"; Lammle 459, 465-466).

While AD offers numerous benefits, the company will need to alter certain procedures to accommodate the differences between AD and workgroup networks. First, system administrators will create users differently. In our current network design, the administrators must individually add a new user account to every device on the network. AD will permit the administrators to create accounts on the DC automatically through a PowerShell script or manually by entering Server Manager and navigating through the Tools menu to reach the Active Directory Administrative Center (ADAC) application. From the ADAC program, an administrator can select a domain and container which will hold a new user account, created with a wizard offered by the ADAC ("Create and Manage Active Directory Users and Computers"). Second, AD necessitates a different procedure to alter preexisting user accounts, like resetting a forgotten password. While logged into the DC, the administrator must navigate through the Control Panel to reach the Administrative Tools window before arriving at the Active Directory Users and Computers. Once in that window, the administrator will need to locate the proper user account, right-click it, and select the proper option to alter the user's account as opposed to doing this on individual computers (Agustafson).

Next, I researched the transition of the current, workgroup-based user accounts to AD accounts. While it may require large amounts of overhead, this transition will decrease the workload in the future through the simpler procedures explained above. If a host is elevated to DC, all workgroup accounts on it will be deleted (Cerling). Even on other computers, administrators will need to use the netdom command or manually create the new accounts because the old local users will not transfer over into the new AD user database (Chaitanya; Sivarajan). In addition, all Discretionary Access Control Lists (DACLs), permissions, and privileges will need to be recreated for each group and user (Cerling).

Finally, I investigated how Active Directory handles users with different permissions and privileges on separate computers. A file's owner can alter permissions like normal through Properties and using the Advanced button on the Security tab to add AD users and groups ("Assigning Permissions to Active Directory Service Accounts"). Alternatively, permissions can be set from the DC through the creation of a Group Policy Object (GPO) which will store the permissions and be applied to an entire group. The administrator will need to add a folder, set permissions, and assign ownership under Computer Configuration/Policies/Windows Settings/Security Settings/File System. To save time, I recommend that administrators make permissions inheritable for all subfolders and files. After exiting the editor, the administrator must link the newly-created GPO to a domain or group, assigning those permissions to users within that domain (Keary). These groups are categorized by their scope and are machine local, domain local, global, and universal. A machine local group permission will only affect a single host. When a user logs on, Windows will generate an access

token for that user which consists of that user's rights, personal Security Identifier (SID), and group SIDs. The access token will be compared to a folder's DACL to determine the user's privileges in regards to that folder and its contents ("Active Directory Users, Computers, and Groups").

The P2P network possesses too many security vulnerabilities and flaws that increase administrative work. AD offers a simpler, more secure, and more scalable network. This comes at the cost of a substantial amount of overhead to conduct the transition due to recreating all user accounts and associated access privileges. After a thorough evaluation of our current system and AD, I recommend that the company enacts the changeover to AD in place of the workgroup.

Works Cited

“Active Directory Users, Computers, and Groups.” *Microsoft Docs*, 9 Dec. 2009, docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727067(v=technet.10). Accessed 15 July 2022.

Agustafson. “How to Reset a User Password in Active Directory?” *Computers N Stuff of Waco*, 15 July 2020, computersnstuffwaco.com/how-to-reset-a-user-password-in-active-directory. Accessed 15 July 2022.

“Assigning Permissions to Active Directory Service Accounts.” *Teradici Corporation*, www.teradici.com/web-help/cas_manager_as_a_service/reference/assigning_permissions_to_active_directory. Accessed 15 July 2022.

“Benefits of Active Directory Domain Services (AD DS).” *Intelecis*, 12 Nov. 2021, www.intelecis.com/benefits-of-active-directory-domain-services/. Accessed 15 July 2022.

Cerling, Tim. Comment on “Switching from Workgroup to Domain Environment.” *Microsoft TechNet*, 1 Nov. 2016, social.technet.microsoft.com/Forums/en-US/feb58c6d-aa81-4c49-94f1-8d00eca04186/switching-from-workgroup-to-domain-environment?forum=winserver8gen. Accessed 15 July 2022.

Chaitanya. “How to Add a Computer to a Domain (GUI and PowerShell).” *ATA Learning*, 8 Apr. 2021, adamtheautomator.com/add-computer-to-domain/. Accessed 15 July 2022.

“Create and Manage Active Directory Users and Computers.” *sourceDaddy*, sourcedaddy.com/windows-7/create-and-manage-active-directory-users-and-computers.html. Accessed 15 July 2022.

Foulds, Iain, et al. “Active Directory Domain Services Overview.” *Microsoft Docs*, 11 Jan. 2022, docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. Accessed 15 July 2022.

Gaille, Jouise. “20 Advantages and Disadvantages of a Peer-To-Peer Network.” *Vittana.org*, 1 Mar. 2020, vittana.org/20-advantages-and-disadvantages-of-a-peer-to-peer-network. Accessed 15 July 2022.

Keary, Tim. “Setting Folder Security Permissions in Active Directory.” *CompariTech*, 15 Jul. 2022, www.comparitech.com/net-admin/security-permissions-active-directory/. Accessed 15 July 2022.

Lammle, Todd. *CompTIA Network+ Study Guide Exam N10-007*. 4th ed., E-book, John Wiley & Sons, Inc., 2018.

Shelladmin. “Active Directory Advantages and Disadvantages.” *ShellGeek*, shellgeek.com/active-directory-advantages-and-disadvantages/. Accessed 15 July 2022.

Sivarajan, Santhosh. Comment on “Switching from Workgroup to Active Directory.” *Microsoft TechNet*, 30 Mar. 2011, social.technet.microsoft.com/Forums/windowsserver/en-US/9bad6262-52ae-4ef5-9ccf-835d43e750f2/switching-from-workgroup-to-active-directory?forum=winserverManagement. Accessed 15 July 2022.

Solomon, Michael G. *Security Strategies in Windows Platforms and Applications*. 3rd ed., E-book, Jones & Bartlett Learning, 2021.

Wararkar, Parvin, et al. “Resolving Problems Based on Peer to Peer Network Security Issue's.” *Procedia Computer Science*, vol. 78, 2016, pp. 652-659, doi.org/10.1016/j.procs.2016.02.113. Accessed 15 July 2022.

“What is Active Directory?” *Quest*, www.quest.com/solutions/active-directory/what-is-active-directory.aspx. Accessed 15 July 2022.

“What is a Workgroup and How Is It Set Up?” *Windows Active Directory*, www.windows-active-directory.com/what-is-a-workgroup-and-how-is-it-set-up.html. Accessed 15 July 2022.