jamk

Hardening TTC6050-3004

Lab 1: Server configuration

Michael Herman

Toni Peltola

Karri Päivärinta

Project report

Instructor: Jarmo Viinikanoja

Return date: 6.9.2023

Group: TIC21S1

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Contents

Figures

1 Introduction

This report outlines the steps involved in hardening, Active Directory (AD) Windows Server and Group Policy. Hardening was performed in accordance with Microsoft best practice (Microsoft, 2021). The report begins with a theoretical discussion of the security challenges associated with these platforms and their roles in the IT infrastructure management ecosystem. A detailed account of configuration changes and the reasoning behind them is provided. Changes were made specifically with the intention of mitigating the security challenges highlighted in the literature. A conclusion summarizing the steps taken follows. The conclusion also outlines the many challenges encountered when performing this task.

2 Theoretical background

2.1 Active Directory

Active Directory (AD) is a directory service designed for Windows domain networks. A critical component of the service is the domain controller (DC). The DC runs the Active Directory Domain Service (AD DS) responsible for authenticating and authorizing users and computers within a Windows domain network (Krause, 2019).

AD also manages security policies and facilitates software installation and updates. It serves as a central hub for storing and managing network information (King, 2003). It is used for user authentication and authorization. It supports Certificate Services, Active Directory Federation Services, Lightweight Directory Services and Rights Management Services. It relies on protocols such as Lightweight Directory Access protocol (LDAP), Kerberos and DNS for its functionality (Microsoft, 2021a).

2.1.1 Services

Domain services interact with a range of Microsoft server technologies. The most relevant of these are Group Policy, Encrypting File System (EFS) and Remote Desktop Services (RDS) (Carpenter, 2011). Group Policy controls the working environment of user accounts and computer accounts. EFS provides filesystem-level encryption. RDS allows users to initiate and control interactive sessions on remote computers or virtual machine over a network connection (Microsoft, 2021b). AD lies at the

heart of Windows domain networks (Cerling & Buller, 2011). It is responsible for the services outlined below.

Figure 1: Core AD services

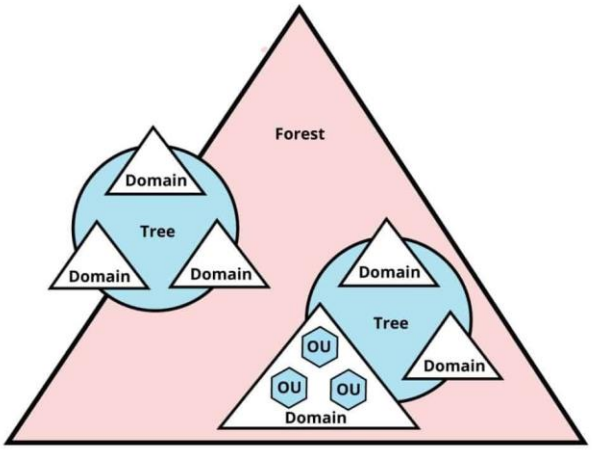
Service	Acronym	Description
Domain Services	AD DS	Stores information about domain members such as devices and users, verifies credentials and defines access rights
Lightwight Directory Services	AD LDS	Stores directory data and provides an LDAP Directory Service Interface
Certificate Services	AD CS	Establishes public-key infrastructure that creates, validates and revokes public key certificates
Federation Services	AD FS	Single sign-on service which allows users to access muliple web or network resouces using one set of credentials
Risk Management Services	AD RMS	Uses encryption and the principle of selective denial for information rights management

2.1.2 Logical structure

At the top of Active Directory's logical structure is the f*orest.* The forest represents a collection of domains with shared configurations and trust relationships. Each domain functions as a security boundary containing user accounts, groups and resources. Object structures and attributes are defined by a schema consistently across the forest. The forest is comprised of *trees.* A tree is a collection of domains sharing an adjoining namespace. Domains with a parent-child relationship are organized into a tree structure.

Domain controllers handle authentication and directory queries for each domain. *Organizational Units (OUs)* allow logical object organization within domains and are used for delegation and Group Policy application (Iyer, Kabbur & Wali, 2018). Sets of configuration settings and their corresponding values are defined by *Group Policy Objects (GPOs)* (Jillepalli et al., 2018). This logical framework empowers administrators to flexibly manage resources and ensure secure network access.

Figure 2: AD logical structure



2.1.3 Security

Approximately 90% of enterprises use AD as their primary user management system (Krishnamoorthi & Carelton, 2022). AD serves as the central directory and access control mechanism for enterprise services. It is a prime target for malicious actors owing to its centrality in managing user identities and authentication. Attackers can gain access to critical network systems and assets or acquire administrator privileges to take control of the domain if AD is breached (Grillenmeier, 2022). Such attacks can be difficult to detect because the compromised user account typically appears to be operating within its authorized access rights.

The utility of AD lies in the scope of the user management services it provides. Security is for the most part a secondary concern (Crandall & Cole, 2022). This is problematic for a range of interconnected reasons. The functionality offered by AD is deeply intertwined with the most critical aspects of business operations. It is used to establish and oversee the connections of individual endpoints within corporate networks. It is integrated into the Windows server operating system. It acts as a repository for a wide range of sensitive information. It encompasses user data, passwords, device details, applications, services, and IT infrastructure operations (Microsoft, 2021b). It assumes a pivotal role in regulating access to all Windows networks, software applications and data resources.

2.2 Windows Server

Windows Server is an enterprise-level family of operating systems. It features robust management, data storage, application hosting and communication capabilities. Historical iterations of Windows Server have primarily been centered on enhancing stability, bolstering security measures and optimizing networking capabilities (Microsoft, 2023a). Windows Server distinguishes itself from UNIX equivalents with a user-friendly interface which streamlines administrative tasks. It supports technologies such as MySQL, PERL and PHP (Krause, 2019).

Windows Server is tightly integrated into AD. it is the platform for AD. It provides the services and tools required by AD directory services, authentication, and policy enforcement capabilities. This includes Active Directory Users and Computers and Group Policy (Microsoft, 2021a). It manages AD's DNS services and ensures resources are properly allocated within the domain. File share and printer management requires seamless integration between AD and Windows Server. Windows Server's backup and recovery tools are also utilized to secure AD data. This integration allows organizations to build and maintain secure, efficient and scalable network environments (Rossberg & Redler, 2006). The next section discusses why these disparate systems should be hardened and the practical ways in which this can be achieved.

3 Hardening

AD is notoriously complex. It requires considerable expertise to operate. A major challenge for novices is simply navigating the menu system. In this context it is easy for vulnerabilities and gaps in security to be overlooked (Krishnamoorthi & Carelton, 2022). *Hardening* refers to the process of securing networks by implementing various security measures and best practices (Jillepalli et al., 2018).

There are good reasons to harden IT infrastructure. Chief among these is to reduce vulnerability to cyberattacks and unauthorized access. Mitigating vulnerabilities and maintaining system updates can also reduce system crashes and downtime (Lyle, Chan & Head, 1999). Safeguarding the confidentiality of sensitive information can minimize the risk of data breaches (Tankard, 2016). Hardening also plays a critical role in preventing unauthorized access to sensitive data and systems.

Compliance with regulatory requirements such as the General Data Protection Regulation (GDPR) necessitates hardening.

3.1 Best practice

Microsoft (2023a) proposes best practices for network hardening. One area is of direct relevance to the subject of this report. This concerns the reduction of the AD attack surface through technical controls. It involves the following:

- Properly configuring and managing privileged accounts and groups to prevent unauthorized access
- Implementing a *least-privilege* administration model
- Removing excessive privileges on member servers, workstations, applications and data repositories
- Implementing secure administration hosts configured solely for administrative tasks
- Securing domain controllers against attack
    - Domain controller operating systems should be updated and patched regularly
    - Implementing security configuration baselines for domain controllers using native tools and Group Policy Objects (GPOs) to enforce security policies consistentl

4 Environment

Hardening was performed in the VLE environment with the abovementioned recommendations in mind. It was performed on the Servers-net subnet. The network is comprised of DC01 and SRV01.

4.1 Active Directory

This section outlines the configuration changes made to Active Directory on the SRV01 machine. The aim was to address the most critical security issues raised by Windows Best Practices Analyzer (BPA). BPA was used to enumerate the configuration changes necessary to comply with Microsoft's best practice guidelines for servers under typical circumstances. Microsoft (2023b) notes that best practice violations do not necessarily herald the arrival of the four horsemen of the apocalypse. But suboptimal configurations can result in poor performance across a range of areas. Servers should for this reason be configured to minimize unexpected conflicts and security risks.

BPA measures compliance according to best practice rules in eight different categories. These relate to effectiveness, trustworthiness and reliability. Results are assessed according to three severity levels.

Figure 3: BPA severity levels

Severity level	Description
Error	Error results are returned when a role does not satisfy the conditions of a best practice rule, and functionality problems can be expected.
Information	Information results are returned when a role satisfies the conditions of a best practice rule.
Warning	Warning results are returned if the results of noncompliance can cause problems if changes are not made. The application might be compliant as operating currently, but may not satisfy the conditions of a rule if changes are not made to its configuration or policy settings. For example, a scan of Remote Desktop Services might show a warning result if a license server is unavailable to the role, because even if no remote connections are active at the time of the scan, not having the license server prevents new remote connections from obtaining valid client access licenses.

Roles are measured against the following categories:

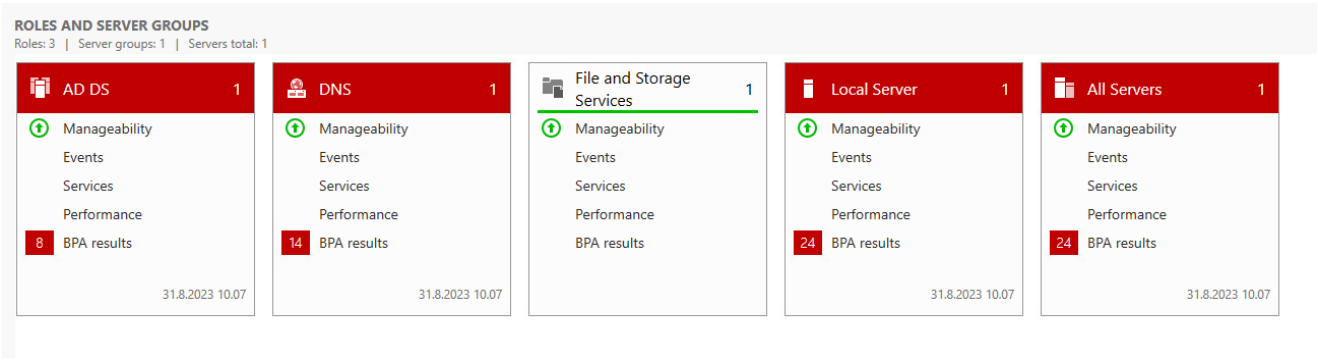
Figure 4: Rule categories

Category Name	Description
Security	Security rules are applied to measure a role's relative risk for exposure to threats such as unauthorized or malicious users, or loss or theft of confidential or proprietary data.
Performance	Performance rules are applied to measure a role's ability to process requests and perform its prescribed duties in the enterprise within expected periods of time given the role's workload.
Configuration	Configuration rules are applied to identify role settings that might require modification for the role to perform optimally. Configuration rules can help prevent conflicts in settings that can result in error messages or prevent the role from performing its prescribed duties in an enterprise.
Policy	Policy rules are applied to identify Group Policy or Windows registry settings that might require modification for a role to operate optimally and securely.
Operation	Operation rules are applied to identify possible failures of a role to perform prescribed tasks in the enterprise.
Predeployment	Predeployment rules are applied before an installed role is deployed in the enterprise. They let administrators evaluate, before the role is used in production, whether best practices were satisfied.
Postdeployment	Postdeployment rules are applied after all required services have started for a role, and after the role is running in the enterprise.
Prerequisites	Prerequisite rules explain configuration settings, policy settings, and features that are required for a role before BPA can apply specific rules from other categories. A prerequisite in scan results indicates that an incorrect setting, a missing program, an incorrectly enabled or disabled policy, a registry key setting, or other configuration has prevented BPA from applying one or more rules during a scan. A prerequisite result does not imply compliance or noncompliance. It means that a rule could not be applied, and is not therefore part of the scan results.

The main advantage of BPA is the way it conceptualizes potential configuration problems. It allows administrators to target issues most likely to produce functionality issues. Hardening the SRV01

machine was fairly straightforward using this methodology. The initial status of roles and server groups is presented below.

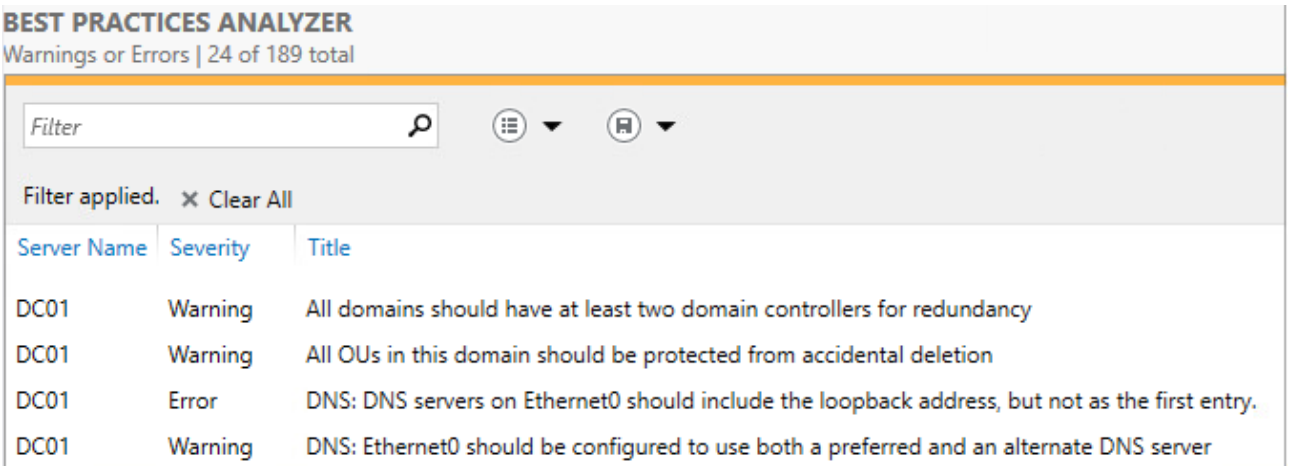
Figure 5: Initial server status



4.1.1 Errors

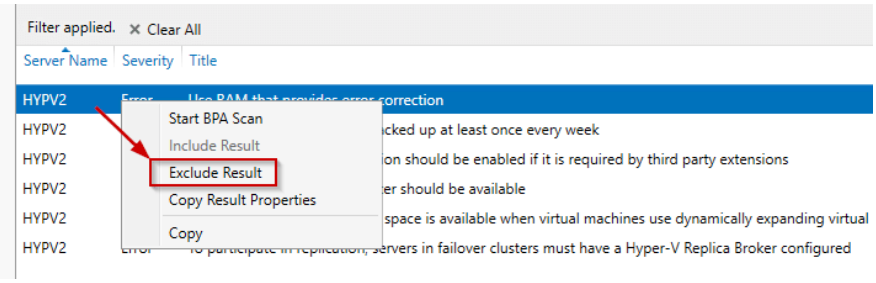
BPA results in the snapshot are slightly misleading. The twenty-four issues seen above are not all mission-critical. Only two of these were errors. The most immediate task was to fix problems which measurably impacted server functionality. Addressing these errors was therefore the first port of call. The DNS error below was in fact a false positive. This was because there is only one DNS server in the network. Loopback addresses will appear as the first entry on networks with only one DNS server by default. This cannot be changed without adding another DNS server.

Figure 6: Ethernet0 loopback address error



The error could be safely excluded.

Figure 7: Exclude error



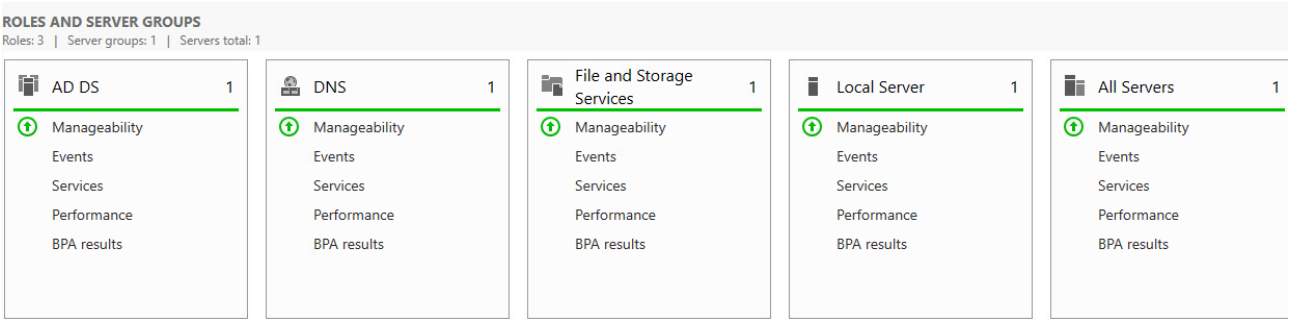
BPA raised another error concerning a synchronization error. It was quite difficult to locate the appropriate solution in the UI. The opaqueness of the interface was a source of considerable frustration; many dead-ends were encountered along the way. It was ultimately decided to fix the error in the terminal. This was without question the most efficient solution even if it did not strictly align with the learning goals of the task.

Figure 8: Terminal time-sync workaround

```
PS C:\Users\Administrator> w32tm /config /update /manualpeerlist:"0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org" /syncfro
mflags:manual /reliable:YES
The command completed successfully.
PS C:\Users\Administrator> w32tm /resync /rediscover /nowait
Sending resync command to local computer
The command completed successfully.
PS C:\Users\Administrator>
```

BPA indicated the roles and server groups were in proper working condition once these errors were fixed.

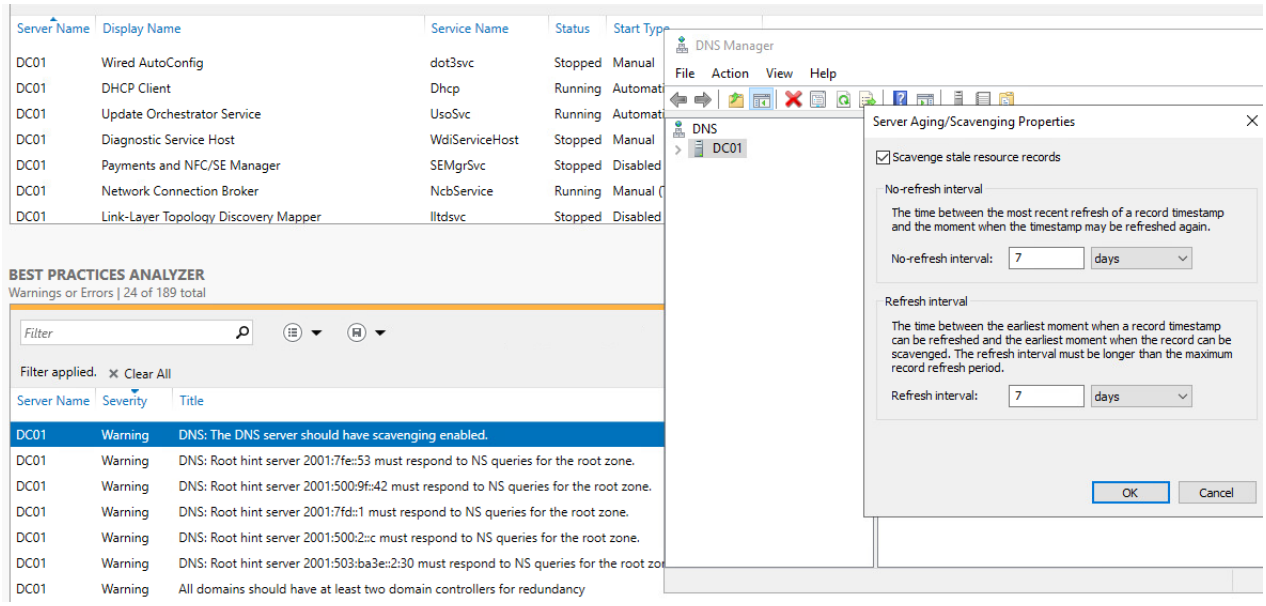
Figure 9: Errors corrected



4.1.2 Warnings

BPA raises *warnings* when it identifies configuration divergences from established best practice which don't strictly result in a loss of functionality (Microsoft, 2023b). Warnings were fixed for illustrative purposes. The first warning concerned enabling scavenging. Scavenging maintains the efficiency of DNS infrastructure by automatically removing stale or outdated records from the DNS database. This results in more efficient resource management and reduces resolution failures or delays (Lushta, 2017). Automating the process streamlines administrative workflow.

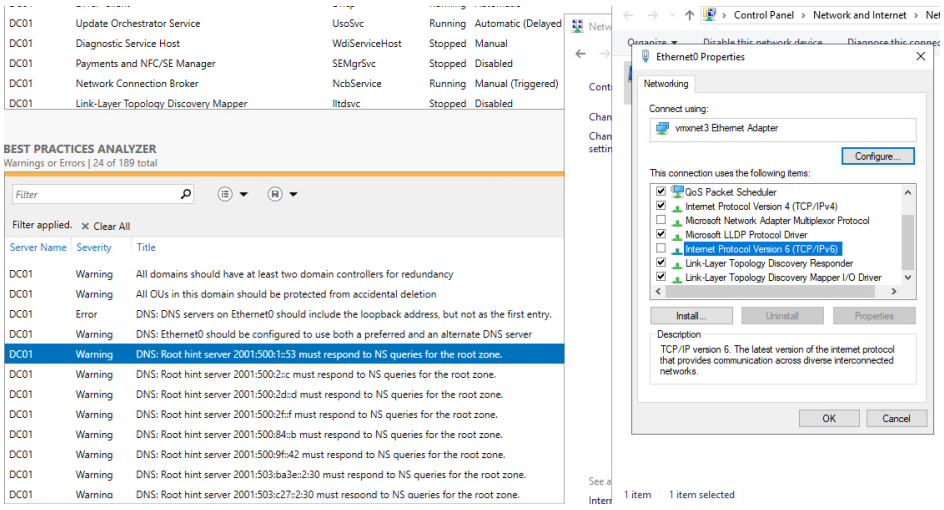
Figure 10: Enable scavenging



The second warning concerned IPv6. There has been some debate as to whether inactive IPv6 endpoints should be disabled (Sarrar et al., 2012, Babik et al., 2017, Anbar et al., 2016). Microsoft (2023b) has observed that disabling IPv6 can potentially result in configuration headaches in Windows domains in the long term even in networks not using the protocol.

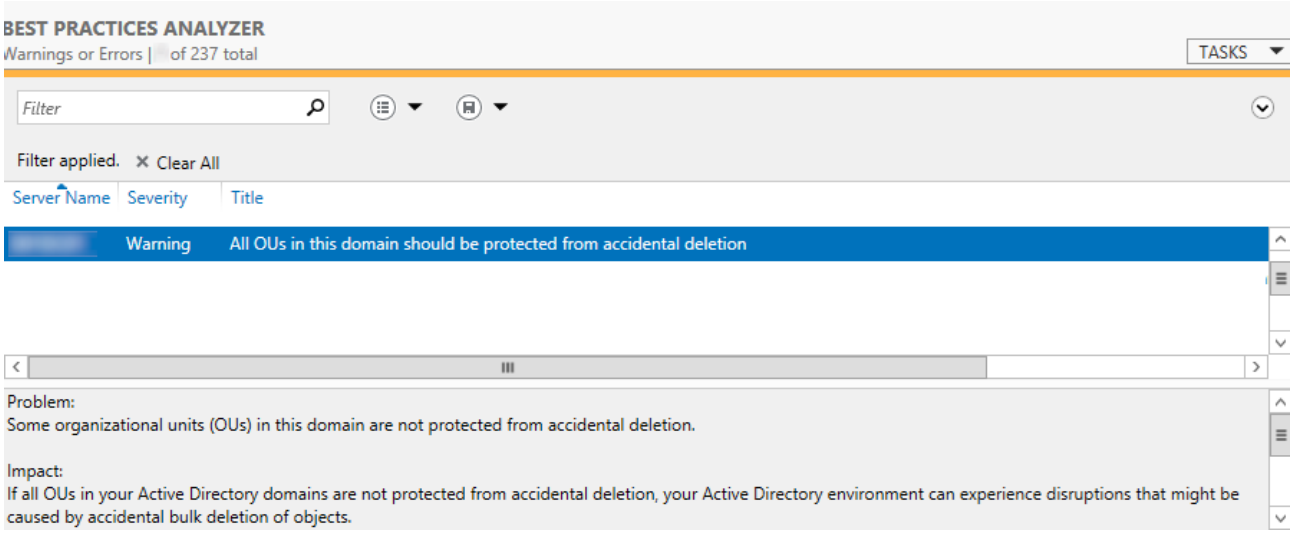
But this should be weighed against the consideration that best practice from a security standpoint dictates unused ports and services be disabled (Hassan et al., 2017). The risk associated with the former was deemed negligible in this case given the size of the network. IPv6 was therefore disabled. No noticeably adverse effects were observed.

Figure 11: Disabling IPv6



The above image also indicated all OUs were not protected from accidental deletion. This was the final warning to be fixed. *Protect object from accidental deletion* is a useful security measure to safeguard network objects such as user accounts, OUs and groups. It requires administrators to explicitly disable protection before deleting an object. This reduces the risk of data loss, security breaches, and operational disruptions caused by human error (Simpkins, 2016). It ensures data integrity, simplifies recovery processes and demonstrates compliance with regulatory requirements (Tankard, 2016).

Figure 12: Protect against accidental deletion warning



This warning is not relevant in this case because the AD domain only contains policy repositories. There are no OUs to speak of in this domain. This means the warning can safely be ignored.

BPA is in sum a useful hardening tool. The severity hierarchy removes much of the guesswork associated with hardening AD. The severity hierarchy renders absolute security requirements immediately apparent. It empowers administrators to efficiently zero in on mission critical vulnerabilities. Thankfully these were not particularly burdensome in this case. Section 4.2 discusses the process of hardening Windows Server. This entailed a good deal more detective work.

4.2 Windows Server

4.2.1 Initial server status

An initial examination of the server revealed a host of unnecessary configurations. The first task was to remove all redundant roles and features. The intention was to configure the server as a standard fileserver with no additional functionality. Basic hardening would then be performed.

4.2.2 Removing redundant roles and features

Initial server roles and features are displayed in the images below.

Figure 13: Initial server roles

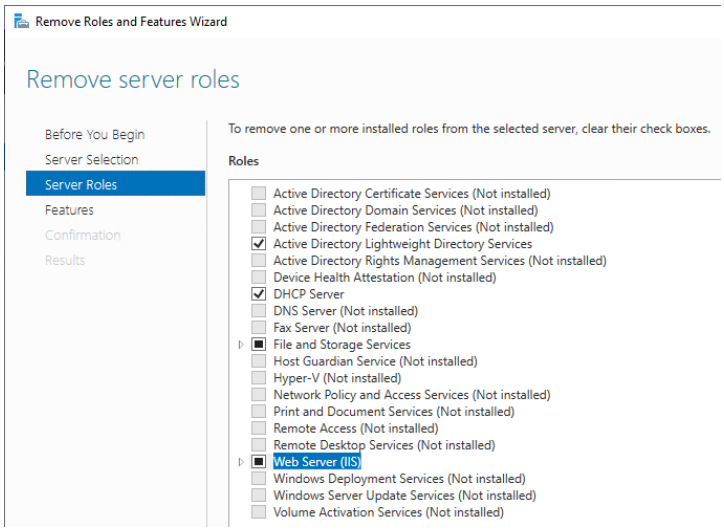
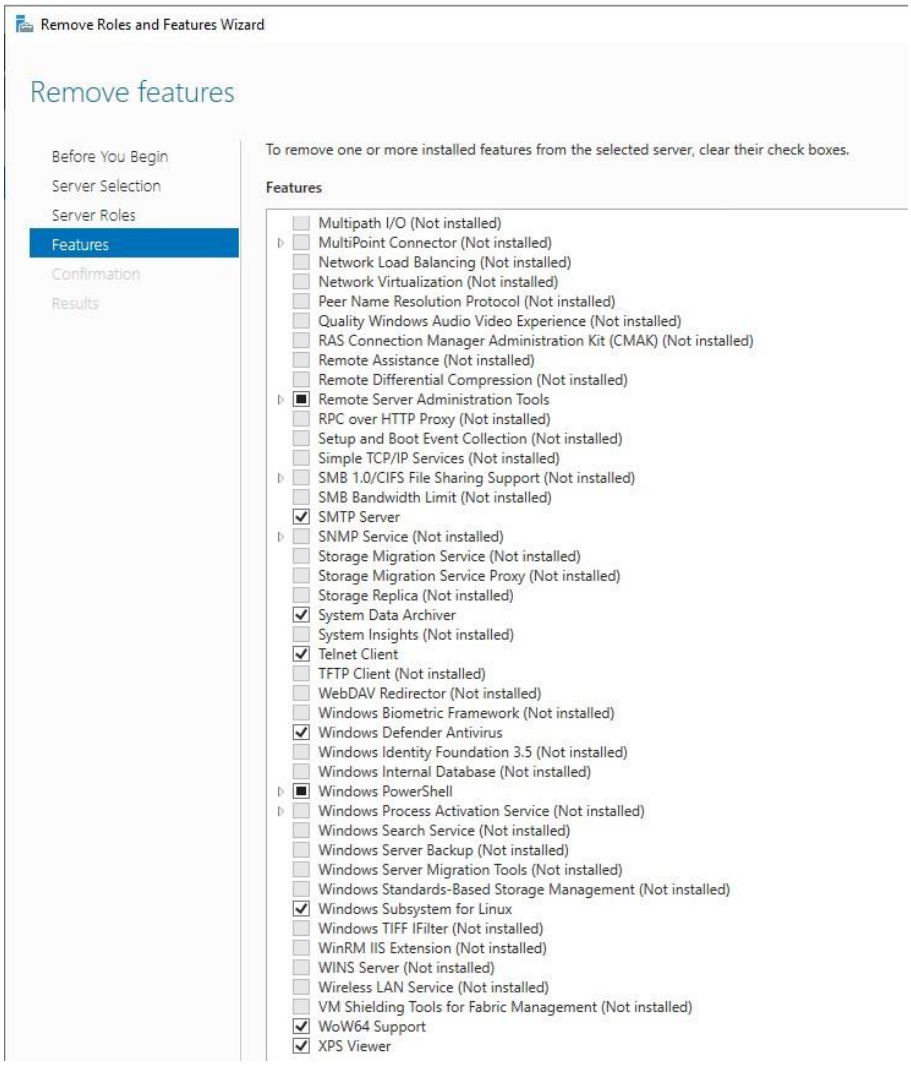


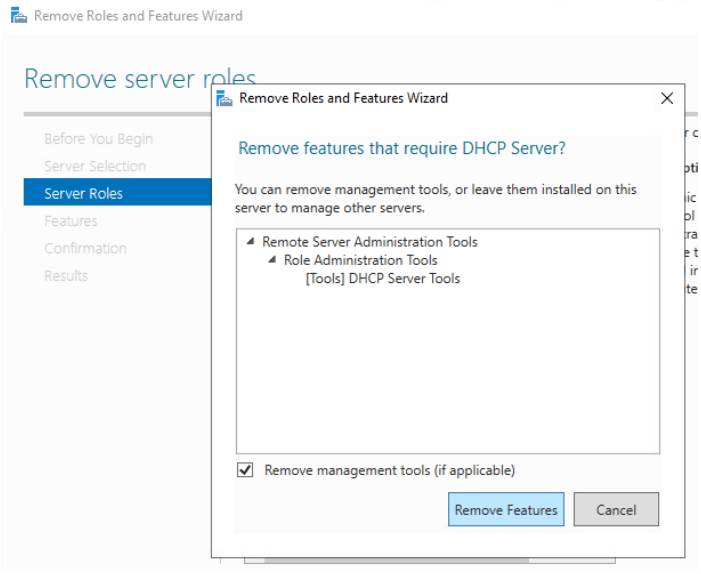
Figure 14: Initial server features



All unnecessary roles and features were removed. .NET framework functionality was retained. Disabling it can potentially affect the functionality of core features and tools such as PowerShell (Microsoft, 2022).

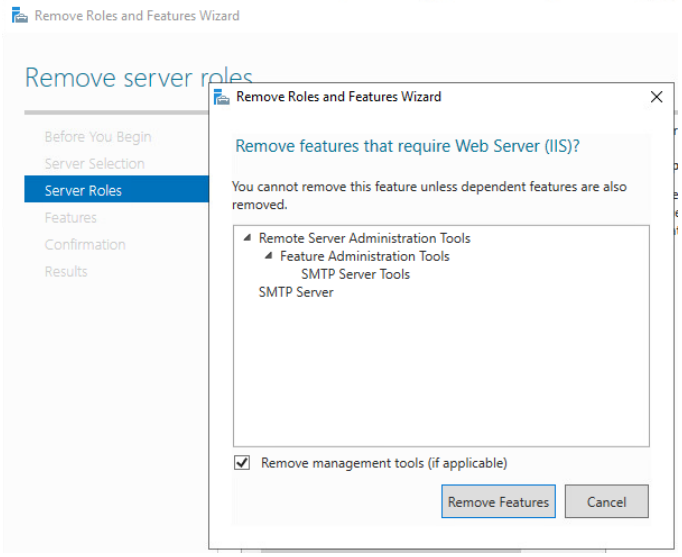
The first role under inspection was the DHCP Server. This role was not required for a fileserver because a DHCP Server is running elsewhere in the environment. It was possible to remove all related DHCP features and management tools when removing this role.

Figure 15: Remove features requiring DHCP



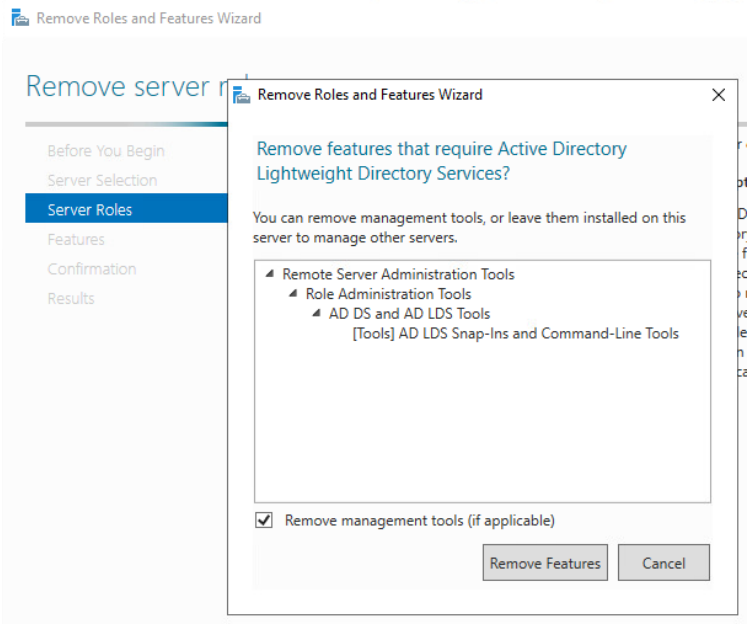
The Web Server role includes required tools to run web applications on the server. Plain fileservers do not require this feature. Features and tools related to this role could be removed as well. SMTP server and related tools are linked to this role. The fileserver does not require email related features, software or tools be cause these functions are implemented elsewhere.

Figure 16: Remove Web Server and SMTP



Active Directory Lightweight Directory Services AD LDS provides dedicated directory services for applications. The role was unnecessary because fileserver would not be running any applications. The related features and tools to be removed with AD LDS are shown below.

Figure 17: Remove features requiring AD LDS



The following additional features were also removed:

- **Telnet Client** - Telnet is an old and insecure data transmission protocol. It lacks encryption, has weak authentication mechanism and does not check data integrity.
- **Windows Defender Antivirus** - Not required on the fileserver. File checking and filtering is done elsewhere in the environment before the files are stored on the fileserver. In larger networks local antivirus capabilities may be preferable as an additional layer of protection (Microsoft 2023c).
- **Windows Subsystem for Linux** - Allows developers to run GNU/Linux environment directly on Windows. This includes command-line tools, utilities and applications. Not needed to run the fileserver.
- **XPS Viewer** - A tool used to view XPS files. Redundant to a fileserver.

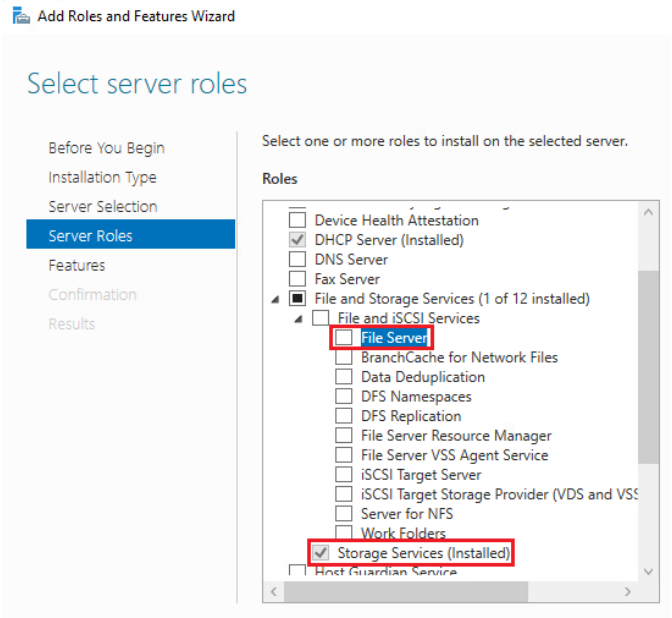
The following were left in place:

- **System Data Archiver** - This feature collects server system CPU, network and volume capacity data. It predicts any future changes they may require. This seemed potentially useful and was therefore left on the server.
- **WoW64 Support** - Subsystem of Windows allowing 32-bit applications run on 64-bit Windows. Removing this was thought to potentially cause more trouble in the future instead of leaving it.
- **Windows PowerShell** - The fileserver does not require PowerShell to function. It was left in place for the time being.

4.2.3 Required roles and features

The minimum roles required for full fileserver functionality are *File Server* and *Storage Services*. These can be applied by using the *Add Roles and Features* wizard. The File Server wizard was selected under *File and iSCSI Services*. Storage Services was already installed on the server. These minimum components are illustrated below.

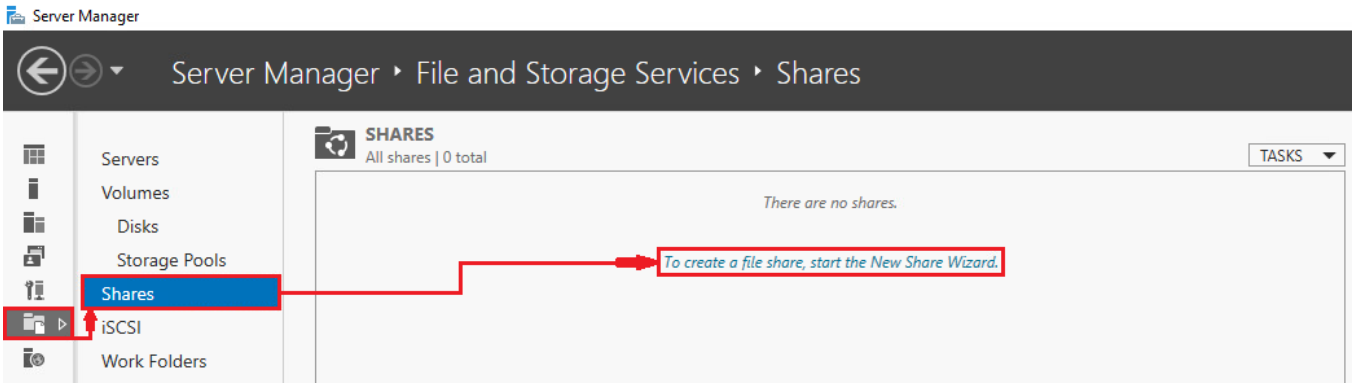
Figure 18: Required fileserver roles



4.2.4 Adding server shares

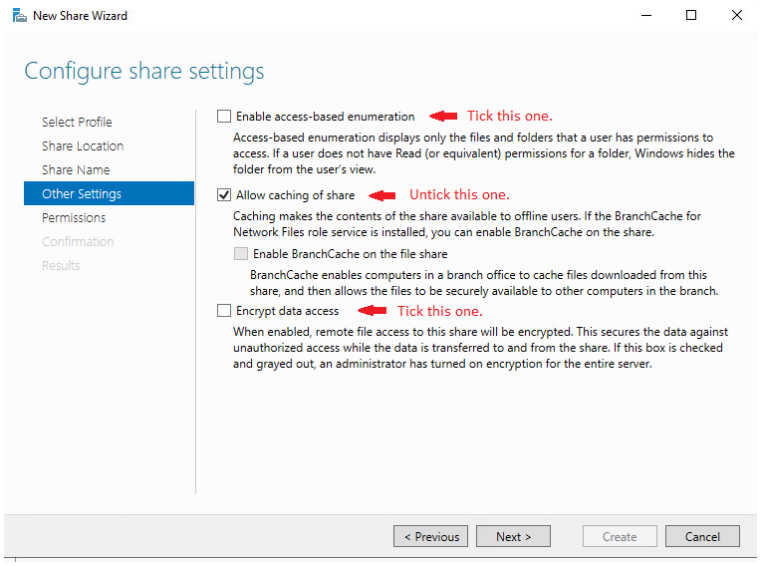
The final step was to create a share on the server. This was done in Server Manager by navigating to *File and Storage Services* and on to *Shares* on the Server Manager dashboard. Here a wizard can be initiated to create a new share.

Figure 19: Adding shares



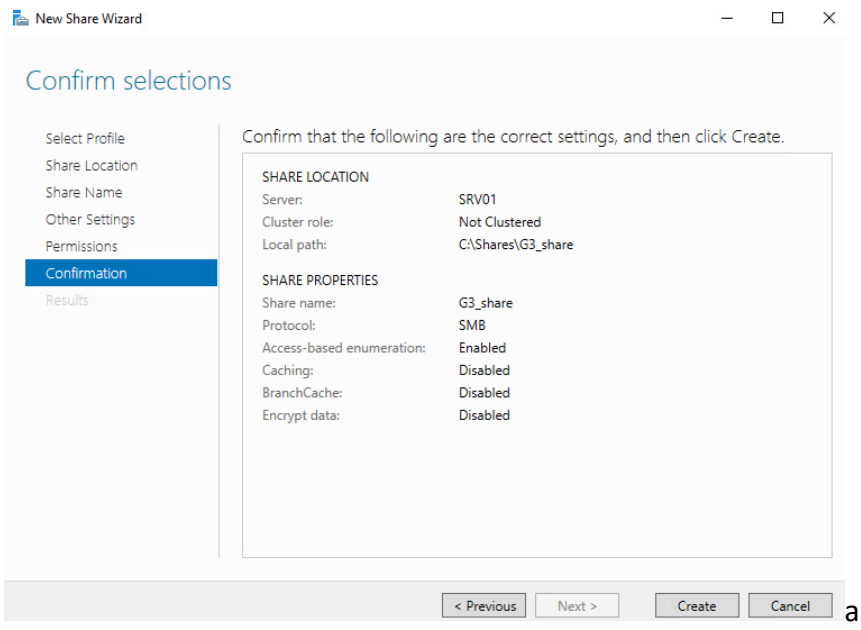
The creation process proceeds via the wizard with clear steps. The *Other settings* section was worth noting. Here *Enable access-based enumeration* is checked. This ensured users can only view files they have permission to access. *Allow caching of share* was unchecked because the share was not active in offline mode. *Encrypt data access* was ticked to protect the share against unauthorized access.

Figure 20: Other settings



The image below provides an overview of the share to be created. *Encrypt data* was initially in a disabled state for an unknown reason. Share properties indicated the state is enabled after the share was created.

Figure 21: Share creation overview



a

4.3 Group Policy

4.3.1 Purpose

Group Policy is a set of rules and settings which determine the rights and privileges users have in their network environments (Microsoft, 2016). These can include requiring employee email correspondence be tied to a specific platform such as Outlook. The use of other email clients could be prohibited. Another policy could be requiring two-factor authentication when logging onto company networks. These are intended to ensure the network environment is safe and free from outside influence. Microsoft (2023d) has prepared extensive guidelines in their Security Compliance Toolkit on setting up group policy enforcements. The policies implemented in this below are based on these guidelines.

At the heart of the group policy is the administrator in charge of managing the environment. The administrator allocates user privileges according to specific needs. In an efficient environment those user privileges should be bestowed on an as-needed basis. Access should be granted on the basis of the principle of least-privilege (Ma et al., 2011). This ensures the safety of the company network. This ensures attackers will not gain full network access in the event of a local security breach.

Group policy objects (GPOs) are a separate entity within the same subject. A group policy is a rule. This could, for example, be to force a password change in eight-week cycles. The GPO is enforced globally within the environment. GPOs form the basis of user experience, available tools and the regulations. The changes that made within the environment are in most cases GPOs by which administrators enforce rules intended to manage user activity.

4.3.2 Environment group policies and GPOs

Group policies apply to the entirety of the VLE environment in most cases. Some are theoretical in nature. Password changes should in ordinary circumstance be enforced at regular intervals in production networks. In the VLE environment it was deemed more appropriate to keep the simple passwords currently present. The system does not have any other users apart from the administrator. In this context it is not feasible to implement the privileges of the standard user. It is nevertheless worth considering what those restrictions could be. These could restrict certain actions

to be performed by administrators only. This could include installing new software, accessing the command line and restricting the use of physical media such as USB sticks.

4.3.3 Implementing and documenting GPOs

Many of these policies are universal and would work for hardening purposes for the entire environment. They are also necessary for server interfaces. They are not implemented as physical rules in the environment. These settings were enabled and changed for hardening purposes.

4.4 Hardening principles

Hardening is a centralized process. In the VLE environments this was performed on the DC01 machine. From there all changes are implemented in the entire servers-net framework. Hardening itself is a relatively simple concept. Implementation is not as straightforward. The Servers-net subnet runs Windows Server 2019 operating systems. Microsoft Best Practices offers an extensive guide for best hardening procedures for this platform (2023d). Most of the hundreds of hardening examples presented by Microsoft cannot be feasibly implemented in the VLE environment. Only changes deemed of critical importance were implemented.

Hardening was performed in order to limit the privileges of the users. This ensures a more secure working environment (Plachkinova and Knapp, 2022). The VLE environment was quite secure at the outset. The user-base is very limited. Most actions require administrator rights. The modifications to DC01 and SRV01 in the previous section already involved a degree of hardening. It was deemed most appropriate to initially perform user-related hardening. Within the Microsoft environment there are two useful tools to manage users, groups and group policies. These are Active Directory Users and Computers and Group Policy Management. Most hardening was performed using these tools.

Hardening was in large part implemented according to Microsoft's best practices. These were outlined in the Microsoft Security Baseline for Microsoft Server 2019 found in the Security Compliance Toolkit (2023). They were applied to the Default Domain Policy GPO in order to efficiently apply the changes globally. Numeric values were set according to values specified in the

Excel files where applicable. Some changes were implemented on the basis of group discussions concerning what would be most appropriate.

4.5 Initial configuration

Hardening was performed in a wide range of areas. These relate broadly to user and password management, access control and system configuration. The changes implemented are detailed in the sections below. Two initial steps were taken prior to hardening. These were necessary to establish a clear baseline for the process. The first involved disabling guest and example. New test users configured with standard privileges were then created. This was necessary to understand how the proposed changes would affect ordinary users.

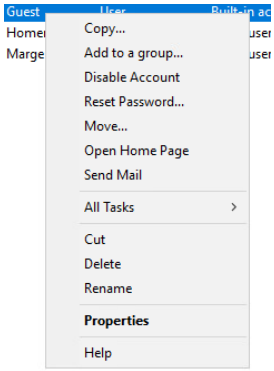
4.5.1 Disabling old users

Active Directory Users and Computers contains all essential information about users in the system. In this case the system has two extra users. These are *Guest* and *Example User*. Both should be considered security risks because their usage is not monitored. A guest account could potentially access the system without using a password. The safest way forward is to disable both accounts.

Figure 22: Users

Disabling the accounts can be done by right-clicking the username and selecting it to be disabled in Active Directory Users and Computers. Disabling extra accounts neutralizes a potentially significant threat to the safety of the environment. There are other settings for users as well. These will be investigated later in the document.

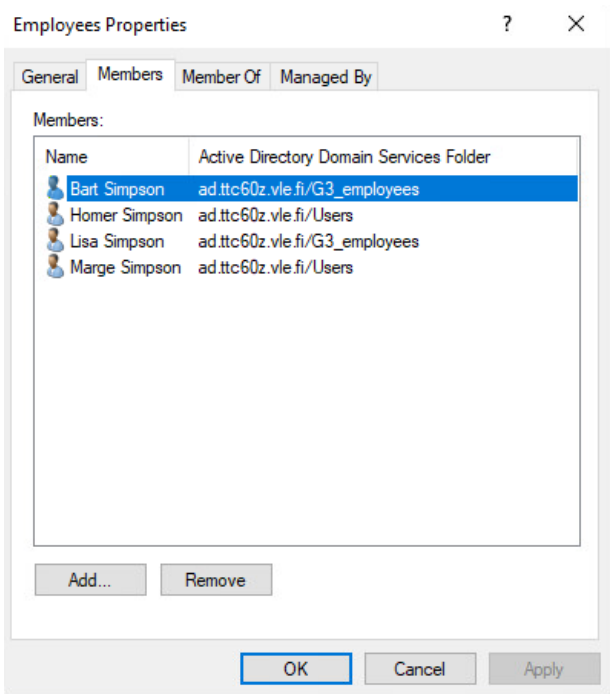
Figure 23: Disabling accounts



4.5.2 Creating test user accounts

The system was left with only one user after deleting unnecessary accounts. This was the administrator. It was not feasible to limit the use of the account because the administrator requires maximum privileges within the environment. Four test users were created in the system for the purpose of this task. The users were called Homer, Marge, Bart and Lisa Simpson. Creating accounts in the system was straightforward. Users can be added to groups for further management once their accounts have been created. A new group called *Employees* was created for all users.

Figure 24: Newly added users and group



4.6 Hardening

4.6.1 Periodic password change

For this task it was decided that no passwords would be changed. Enforcing periodic password changes was not implemented for this reason. This ensures future accessibility to the system for team members. It is nevertheless important to acknowledge the importance of periodic password changes in production environments.

4.6.2 Password lockout

Microsoft (2023d) recommends users be locked out of their account after 10 incorrect password attempts. This meant the account would enter a 15-minute lockdown after 10 wrong password entries. The following configuration changes were made in the Group Policy Management Editor

Figure 25: Password lockout

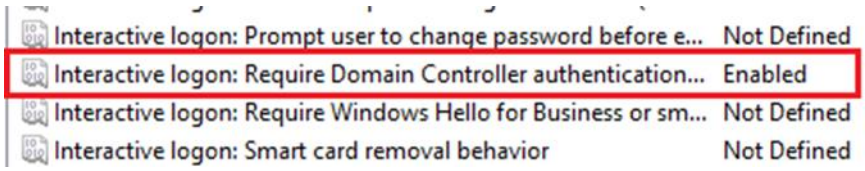


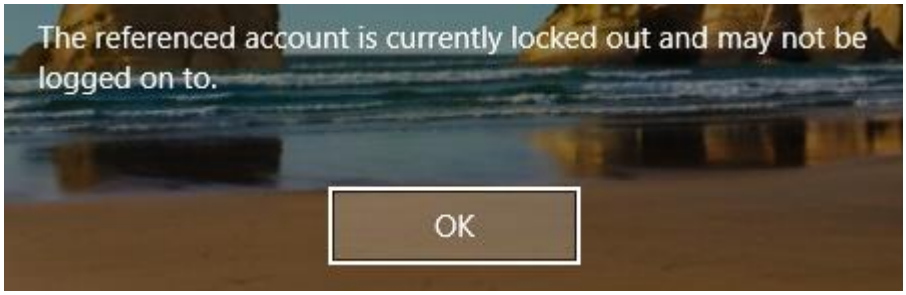
Figure 26: Lockout policy

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

The end-user will see the following message if the password-entry limit is exceeded:

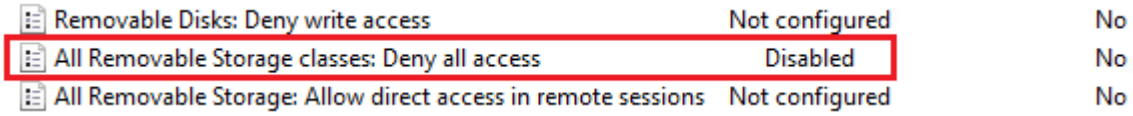
Figure 27: Lockout view



4.6.3 Denying access to physical media

The use of physical media was deemed unnecessary for users with basic privileges. The policy denies/blocks usage of any kind of external storage devices. This includes CD/DVD drives, USB sticks and legacy technologies such as floppy-disk drives. The following change was made in the Group Policy Management Editor:

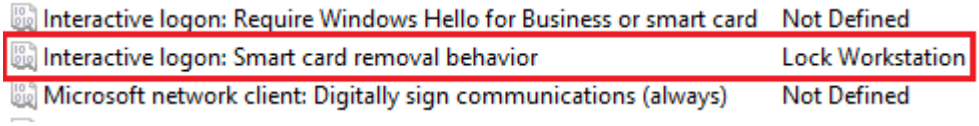
Figure 28: External storage devices disabled



4.6.4 Smartcard removal behaviour

Default behavior was implemented for smartcard logins. Workstations should lock automatically when smartcards are removed. A forced logoff upon smartcard removal would be another good option. It was nevertheless decided to follow Microsoft's best practice guidelines (2023d) in this case.

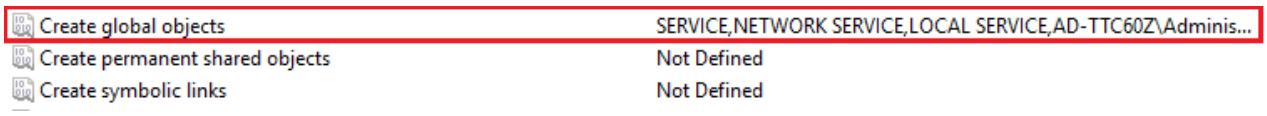
Figure 29: Smartcard removal behaviour



4.6.5 Creating global objects

The option for creating global objects should be allowed for Administrators, LOCAL SERVICE, NETWORK SERVICE and SERVICE exclusively (Microsoft, 2023d). This is set in place in user rights assignments in the Group Policy Management Editor.

Figure 30: Create global objects



4.6.6 Force remote shutdown

Best practice dictates the ability to force a shutdown from a remote system should be reserved for administrators.

Figure 31: Admin only remote shutdown

4.6.7 Manage auditing and security logs

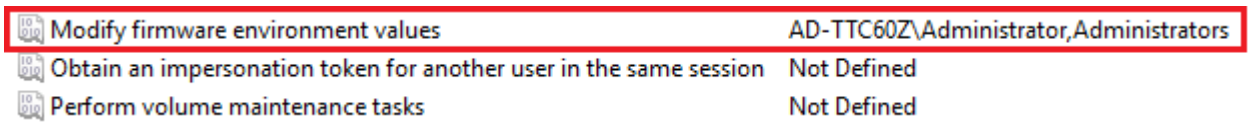
There is no reason for a regular user to have access to auditing and/or security logs. It is considered best practice for logs to be accessible only to administrators.

Figure 32: Log access

4.6.8 Modify firmware environmental values

Tampering with firmware environmental values is frequently ill-advised. This should be safeguarded from intentional or accidental actions. The right to modify firmware environmental values should be reserved for administrators.

Figure 33: Firmware environment values



4.6.9 Taking ownership of files or other objects

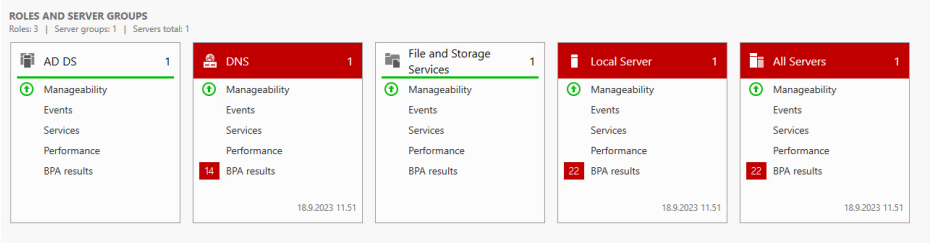
Regular users should not have the right to take ownership of various objects. This could potentially allow attackers to introduce malicious files or code into the system. Administrators should be the only users with this capability. This applies to files, folders, AD objects, processes etc.

Figure 34: Taking ownership of files and objects

5 Final BPA Scan

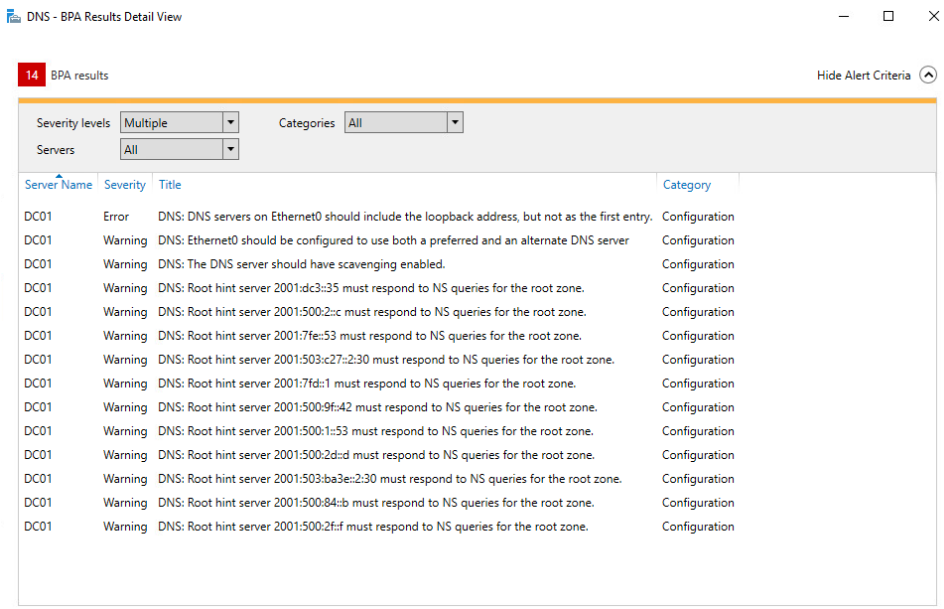
A final Best Practice Analyzer scan was performed after the hardening measures above were implemented. The scan indicated new errors had emerged as a result of the hardening process. It can safely be concluded that hardening one section of an environment can manifest in unintended consequences elsewhere in the network.

Figure 35: Final BPA scan results



New DNS and server issues were raised by the scan. But it was determined that fixing DNS warnings and errors on the Ethernet0 interface fell beyond the scope of this report. Such issues would have to be taken seriously in a production environment, however.

Figure 36: Ethernet0 errors and warnings



6 Conclusion

In lab 1 we were given a sense of what hardening is and how it should be implemented. It was obvious that hardening extends beyond the borders of the Servers.net environment. We gained an understanding of the importance of hardening by making decisions on how to approach hardening Windows Server edition 2019. We also learned about user privilege management and how Windows AD implementations differ from a basic file server approach. Understanding the scope of the administrator role will be critical when performing more complicated tasks spanning the entire environment.

The most challenging aspect of the task was understanding how the server manager works within the Windows environment. It was not always easy to understand the server side of Windows operating systems. It was frequently difficult to learn what everything was and how it worked. Ultimately we were able to understand the most important aspects of server hardening. Discretion was used when ranking the relevance of our changes. We concede this mostly reflected our subjective understanding of their significance.

We view our choices as imperfect but sufficient; the environment still works as intended. DC01 and SRV01 are without question more secure. Restrictions are now in place which ensure resources are used only as needed. Our approach was to allow what only was necessary. In this we believe we succeeded. Future hardening tasks will without doubt be easier with this foundational knowledge in place.

7 Sources

Anbar, M., Abdullah, R., Saad, R. M., Alomari, E., & Alsaleem, S. (2016). Review of security vulnerabilities in the IPv6 neighbor discovery protocol. In *Information Science and Applications* (ICISA) 2016 (pp. 603-612). Springer Singapore.

Babik, M., Chudoba, J., Dewhurst, A., Finnern, T., Froy, T., Grigoras, C., & Wartel, R. (2017, October). IPv6 Security. In *Journal of Physics: Conference Series* (Vol. 898, No. 10, p. 102008). IOP Publishing.

Carpenter, T. (2011). *Microsoft Windows Server Administration Essentials*. John Wiley & Sons.

Cerling, T., & Buller, J. L. (2011). *Mastering Microsoft Virtualization*. John Wiley & Sons.

Fitzgerald, A. (2023). *Top Best 30 Active Directory Security Best Practices Checklist (in 2023)*. Cloud Infrastructure Services. Retrieved September 5, 2023, from https://cloudinfrastructureservices.co.uk/active-directory-security-best-practices/

Grillenmeier, G. (2022). Improving your Active Directory security posture: AdminSDHolder to the rescue. In *Cyber Security: A Peer-Reviewed Journal*, Volume 6, Issue 3. Retrieved September 8, 2023, from https://www.semperis.com/wp-content/uploads/resources-pdfs/resources-improving-ad-security-posture-adminsdholder.pdf

Gebusia, J. (2007, December). Data Encryption on File Servers. In *ISSE/Secure 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference* (pp. 38-48). Retrieved September 8, 2023, from https://link.springer.com/chapter/10.1007/978-3-8348-9418-2_4

Hassan, N. A., Hijazi, R., Hassan, N. A., & Hijazi, R. (2017). *Windows security. Digital Privacy and Security Using Windows: A Practical Guide*, 103-122.

Iyer, N. C., Kabbur, A. M., & Wali, H. G. (2020). Implementation of Active Directory for efficient management of networks. *Procedia Computer Science*, 172, 112-114. https://doi.org/10.1016/j.procs.2020.05.016

Jillepalli, A. A., de Leon, D. C., Sheldon, F. T., & Haney, M. A. (2018). Enterprise-level hardening of web browsers for Microsoft windows. *International Journal of Computing and Digital Systems (IJCDS)*. https://dx.doi.org/10.12785/ijcds/070501

Krause, J. (2019). Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities. Packt Publishing Ltd.

Krishnamoorthi, S., & Carleton, J. (2022). *Active Directory Holds the Keys to Your Kingdom, But Is It Secure?* Frost & Sullivan. Retrieved September 5, 2023, from https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-ca/brand/tenable/sept-2022/tenable-sept-2022-frost-and-sullivan-whitepaper-active-directory-holds.pdf

Lushta, B. (2017). *Active Directory Infrastructure Design and Network Topology Design for StarCom Software Developer Company*. Theses and Dissertations. Retrieved September 15, 2023, from https://knowledgecenter.ubt-uni.net/etd/1137

Lyle, D., Chan, Y. & Head, E. Improving information-network performance: reliability versus invulnerability. *IIE Transactions* 31, 909–919 (1999). https://doi.org/10.1023/A:1007630901474

Ma, X., Li, R., Lu, Z., Lu, J., & Dong, M. (2011). Specifying and enforcing the principle of least privilege in role-based access control. Concurrency and Computation: Practice and Experience, 23(12), 1313-1331. https://doi.org/10.1002/cpe.1731

Microsoft. (2016, August 31). *Group Policy Overview*. Microsoft Learn. Retrieved September 18, 2023, from https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)

Microsoft. (2021a, July 29). *Best Practices for Securing Active Directory*. Microsoft Learn. Retrieved September 5, 2023, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Microsoft. (2021b, July 29). *Executive Summary*. Microsoft Learn. Retrieved September 14, 2023, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/executive-summary

Microsoft. (2022, August 30). *Troubleshoot blocked .NET Framework installations and uninstallations - .NET Framework*. Microsoft Learn. Retrieved September 18, 2023, from https://learn.microsoft.com/en-us/dotnet/framework/install/troubleshoot-blocked-installations-and-uninstallations

Microsoft. (2023a, July 11). *Security baselines guide - Windows Security*. Microsoft Learn. Retrieved September 5, 2023, from https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

Microsoft. (2023b, January 25). *Run best practices analyzer scans and manage scan results*. Microsoft Learn. Retrieved September 15, 2023, from https://learn.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results

Microsoft. (2023c, April 6). Microsoft Defender Antivirus on Windows Server. Microsoft Learn. Retrieved September 18, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-on-windows-server?view=o365-worldwide

Microsoft (2023d). MS Security Baseline Windows 10 v1809 and Server 2019. In *Security Compliance Toolkit and Baselines*. Downloaded September 18, 2023, from https://www.microsoft.com/en-us/download/details.aspx?id=55319

Plachkinova, M., & Knapp, K. (2022). Least Privilege across People, Process, and Technology: Endpoint Security Framework. Journal of Computer Information Systems, 1-13. https://doi.org/10.1080/08874417.2022.2128937

Rossberg, J., & Redler, R. (2006). Windows Server System. *Pro Scalable. NET 2.0 Application Designs,* 31-62.

Sarrar, N., Maier, G., Ager, B., Sommer, R., Uhlig, S. (2012). Investigating IPv6 Traffic. In: Taft, N., Ricciato, F. (eds) *Passive and Active Measuremen*t. *PAM 2012*. Lecture Notes in Computer Science, vol 7192. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-28537-0_2

Simpkins, S. (2016). *Active Directory. In: Building a SharePoint 2016 Home Lab*. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-2170-9_4

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8. https://doi.org/10.1016/S1353-4858(16)30056-3