WorkshopPLUS Remote - Securing Windows Active Directory

References

# Recommended Security Hardening

1. Ensure all machines are configured to not store LM hashes
   1. [Network security: Do not store LAN Manager hash value on next password change](https://docs.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-do-not-store-lan-manager-hash-value-on-next-password-change)
2. Disable the DES e-type for Kerberos
   1. [Network security: Configure encryption types allowed for Kerberos](https://docs.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos)
3. Configure LDAP signing and channel binding token requirements on domain controllers
   1. Enable auditing for client that do not use LDAP signing and monitor for events with ID 2889, and client that attempt to bind without valid CBT and monitor for events with ID 3039, and finally configure recommended values for Signing and CBT.
   2. [Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing](https://msrc.microsoft.com/update-guide/vulnerability/ADV190023)
   3. [2020 LDAP channel binding and LDAP signing requirements for Windows](https://support.microsoft.com/topic/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows-ef185fb8-00f7-167d-744c-f299a66fc00a)
4. Disable print spooler service on servers that do not require it.
   1. [Security assessment: Domain controllers with Print spooler service available](https://docs.microsoft.com/defender-for-identity/cas-isp-print-spooler)
5. Configure the **Network security: LAN Manager Authentication Level** setting to Send NTLMv2 responses only.
6. Configure NTLM SSP on clients and servers to require the negotiation of 128-bit encryption and NTLMv2 session security to help protect against man-in-the-middle attacks.
   1. [Network security: Minimum session security for NTLM SSP based (including secure RPC) servers](https://docs.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-servers)
   2. [Network security: Minimum session security for NTLM SSP based (including secure RPC) clients](https://docs.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-clients)
7. Configure Extended Protection for Authentication to better safeguard the use of authentication credentials being transferred between a client and server when using Integrated Windows Authentication (IWA)
   1. [Extended Protection for Authentication](https://msrc-blog.microsoft.com/2009/12/08/extended-protection-for-authentication/)
   2. [Credential Relaying Attacks on Integrated Windows Authentication](https://docs.microsoft.com/security-updates/securityadvisories/2009/974926)
   3. [Authentication failure from non-Windows NTLM or Kerberos servers](https://docs.microsoft.com/troubleshoot/windows-server/windows-security/authentication-fails-non-windows-ntlm-kerberos-server)
8. Patch your domain controllers for insecure Netlogon secure channel connections
   1. [How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472](https://support.microsoft.com/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e#bkmk_enforcementmode)

1. Configure the security accounts manager (SAM) to restrict the users and groups that can perform remote RPC connections to SAM on domain controllers to Authenticated Users and on member servers and workstations to the built-in Administrators group.
   1. Configure audit-only mode first to identify compatibility issues. Use the [Events 16962 - 16969 Reader](https://github.com/LijuV-MSFT/W-_Securing_AD/blob/main/Event-16962to9-Reader.zip) script to parse the event logs.
   2. [Network access: Restrict clients allowed to make remote calls to SAM](https://docs.microsoft.com/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls)
2. Configure Additional LSA Protection for Windows 8.1 and Windows Server 2012 R2 and for machines that do not support credential guard.
   1. [Configuring Additional LSA Protection](https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn408187(v=ws.11))
3. Enable support for Kerberos Armoring in your environment
   1. Set **KDC support for claims, compound authentication, and Kerberos armoring** to **Supported** or higher.
   2. Set **Kerberos client support for claims, compound authentication and Kerberos armoring** to Enabled
   3. [Support for claims, compound authentication, and Kerberos armoring](https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831747(v=ws.11)#support-for-claims-compound-authentication-and-kerberos-armoring)
4. Disable WDigest authentication using the UseLogonCredential registry value. For this setting to work on Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012, KB2871997 must first be installed.
   1. [Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014](https://support.microsoft.com/topic/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13-2014-93434251-04ac-b7f3-52aa-9f951c14b649)
5. Block TGT delegation after you install the March 2019 updates across an incoming trust by setting the netdom flag EnableTGTDelegation to No
   1. [Updates to TGT delegation across incoming trusts in Windows Server](https://support.microsoft.com/topic/updates-to-tgt-delegation-across-incoming-trusts-in-windows-server-1a6632ac-1599-0a7c-550a-a754796c291e)
6. Harden Net Session Enumeration to prevent enumeration of remote net sessions
   1. [NetCease.zip](https://github.com/LijuV-MSFT/W-_Securing_AD/blob/main/NetCease.zip)
7. Verify that the dsHeuristics attribute is not set to enable anonymous logon or that members of the following groups are not excluded from protections by adminSDHolder.
   1. [Delegated permissions are not available and inheritance is automatically disabled](https://support.microsoft.com/topic/delegated-permissions-are-not-available-and-inheritance-is-automatically-disabled-56a70fa8-6d17-35ac-0f2c-87ec14b61980)
8. Verify that the dsHeuristics attribute is not set to 0000002. This setting allows anonymous clients to perform any operation that is permitted by the access control list (ACL).
   1. [Anonymous LDAP operations to Active Directory are disabled on domain controllers](https://docs.microsoft.com/troubleshoot/windows-server/identity/anonymous-ldap-operations-active-directory-disabled)
9. Remove Everyone from membership of the Pre-Windows 2000 Compatible Access group
   1. In Windows Server 2003 and later operating systems, in the Pre-Windows 2000 Compatible Permissions mode, Everyone (S-1-1-0) and Anonymous (S-1-5-7) are members, and in the Windows 2000-Only Permissions mode, only Authenticated Users (S-1-5-11) are members.
   2. Do this after you have sufficiently monitored for Anonymous Access
   3. [Enabling Monitoring for Anonymous Access](https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/bb727065(v=technet.10)?redirectedfrom=MSDN#enabling-monitoring-for-anonymous-access)
   4. To determine the source of the connections, you may also need to enable diagnostic event logging for LDAP Interface (16 LDAP Interface Events) temporarily on the domain controllers and monitor for 1138/1139 events where the SID is S-1-5-7.
10. On your DNS servers, set the maximum TCP packet size, in bytes, that the DNS server can accept to 0xFF00
    1. [KB4569509: Guidance for DNS Server Vulnerability CVE-2020-1350](https://support.microsoft.com/topic/kb4569509-guidance-for-dns-server-vulnerability-cve-2020-1350-6bdf3ae7-1961-2d25-7244-cce61b056569)
11. Secure RDP connections from the transmission of reusable credentials
    1. [Remote Desktop Services: Enable Restricted Admin mode](https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx)
    2. [Remote Credential Guard](https://docs.microsoft.com/windows/security/identity-protection/remote-credential-guard#remote-credential-guard-requirements)
12. OS and role hardening with the help of baselines.
    1. [Microsoft Security Compliance Toolkit](https://www.microsoft.com/download/details.aspx?id=55319)
13. Implement Privileged Access Workstations to provide a secure workstation for sensitive users
    1. [Securing devices as part of the privileged access story](https://docs.microsoft.com/security/compass/privileged-access-devices)
    2. Resource kit to help with deploying a Privilege Access Workstation setup according to the documentation on Microsoft docs.
    3. <https://github.com/microsoft/PAWTools>

# Auditing and Event Management

Enable auditing for PowerShell using the group policy settings "Turn on PowerShell Script Block Logging" and "Turn on Module Logging" and monitor for Event ID 4103 (Module) and 4104 (Script block) in the Microsoft-Windows-PowerShell/Operational event log

**Recommended (additional) audit policy**

<https://docs.microsoft.com/azure-advanced-threat-protection/configure-windows-event-collection#configure-audit-policies>

**Recommended Events to Monitor**

<https://docs.microsoft.com/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

**How to set up Windows Event Forwarding**

<https://docs.microsoft.com/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem>

**Trigger a PowerShell Script from a Windows Event**

<https://docs.microsoft.com/archive/blogs/wincat/trigger-a-powershell-script-from-a-windows-event>

# Cool Features

**Privileged Access Management - demystified**

<https://docs.microsoft.com/archive/blogs/fieldcoding/privileged-access-management-demystified>

**Temporary Group Memberships**

<https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/previewing-server-2016-tp4-temporary-group-memberships/ba-p/400372>

**Azure Sentinel Insecure Protocols Workbook Implementation Guide**

<https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-insecure-protocols-workbook-implementation-guide/ba-p/1197564>

# Housekeeping

* Privileged accounts must be members of "Protected Groups" security group
* Privileged accounts must be configured with "Account is sensitive and cannot be delegated"
* Accounts should not be configured with "Do not require Kerberos preauthentication"
* Accounts should not be configured for unconstrained delegation
* Accounts should not be configured for "Password Never Expires"
* Accounts should not be configured for "Store Password Using Reversible Encryption "
* Accounts should not be configured for "Use Only Kerberos DES Encryption Types for This Account"

**Periodically reset the KrbTgt Password For RWDCs And RODCs In A Controlled Manner**

<https://github.com/microsoft/New-KrbtgtKeys.ps1/blob/master/New-KrbtgtKeys.ps1>

# Tools and Scripts

**AD ACL Scanner**

<https://github.com/canix1/ADACLScanner>

**Active Directory OU Permissions Report**

<https://github.com/LijuV-MSFT/W-_Securing_AD/blob/main/OU_permissions.zip>

**Administrative Groups Collection and Report**

<https://github.com/LijuV-MSFT/W-_Securing_AD/blob/main/FGS.zip>

**Group Policy Search!**

<https://gpsearch.azurewebsites.net/>