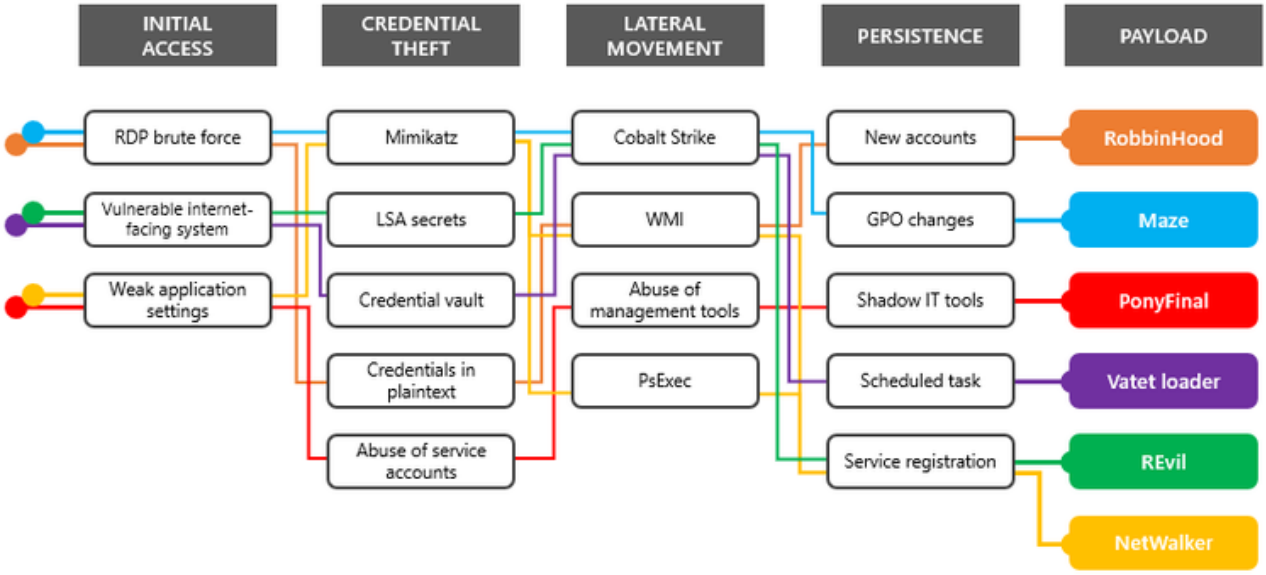
Active Directory Hardening Series - Part 7 – Implementing Least Privilege

techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-7----implementing-least-privilege/4366626



Blog Post

Hi all! Jerry here again to continue the AD hardening series. This time I want to address the concept of least privilege as it applies to Active Directory. Of the three principles of Zero Trust (verify explicitly, least privilege, assume breach), least privilege is the most achievable using native Active Directory features. It is also a concept that was well established before Windows domains were introduced. Some organizations did a great a great job minimizing administrative access from day one but sadly they were the exception. While we are far more disciplined when granting privileged access today, most domains have a couple decades of accumulated delegated access that needs to be reviewed and revoked where no longer justified. Today I want to walk you through areas typically reviewed during an assessment of Active Directory security as it relates to minimizing privilege.

Why hyper focus on privileged accounts?

When I deliver workshops on credential hygiene, I generally lead off with this diagram to illustrate that the initial access methods can be a moving target, but the pursuit of credentials is a constant. If we can prevent attackers from acquiring useful credentials we can disrupt the rest of their playbook. Accomplishing that involves minimizing the number of privileged accounts, restricting where privileged accounts are exposed (Tier model), deploying Privileged Admin workstations (PAWs), and implementing the protocol hardening settings covered in this series.

Service Accounts

Overprivileged service accounts are far too common. While governance for service accounts has greatly improved in recent years, many organizations still have opportunities to remediate service accounts provisioned before we became disciplined in this area. Placing service accounts in the Domain Admins group is a textbook example of not adhering to the principle of least privilege. This was sometimes done out of convenience and other times due to a lack of clarity regarding the application's true requirements. Once an application has been deployed, it can be very difficult to "right-size" the privileges of the service account, but it is a necessary step.

For the record, organizations who have held the line on minimal service account privileges have found ways to scan for vulnerabilities, deploy security updates, and perform Active Directory backups without placing accounts in Domain Admins or equivalent groups. Before you agree to purchase such products clarify the requirements for the solution. Vendors are far more likely to figure out how to adhere to least privilege before the sale than after.

As you remediate overprivileged service accounts, prioritize accounts with a Service Principal Name (SPN) since they are vulnerable to Kerberoasting attacks. Any such account that cannot have its privileges reduced should be enabled for AES and given a strong password.

Local admin on devices

In the early days of Active Directory, withholding local administrative rights on endpoints was often done to prevent configuration drift and the installation of unlicensed software. Today the position is primarily driven by security risks. Without local administrative privilege it is very difficult for malicious software to be accidentally installed. Additionally, interacting with LSASS memory where credentials are stored requires the Debug programs right which by default is limited to Administrators.

Withholding local administrative rights on endpoints is another area where we are seeing considerable improvement. However, there are often exceptions for select users like developers and system administrators. While it is great to see this progress, any exception should be thoroughly scrutinized to determine if it is necessary or just convenient. For context, consider these scenarios

User Profile	Configuration	Scenario	Blast Radius

Developer	A standard desktop is used for writing code along with productivity work. The developer is a member of administrators group in order to install tools	The developer visits a compromised website and unknowingly installs software (drive-by download) that gives the attacker command and control (C2) of the device. The attacker uses the access to manipulate the code project.	The project containing the malicious binaries is deployed to production servers given the attacker access to sensitive data and credentials
Help desk	The help desktop group has been added to the Administrators group of all endpoints	A user creates a support case after opening a link in a phishing email. The help desktop agent makes an RDP connect to the device which exposes the support credential to the adversary	The attacker uses the credential to move laterally across all endpoints in the domain

User Right Assignments

The User Rights Assignment (URA) settings in the Default Domain Controllers Policy are often bloated with delegations that have accumulated since the first domain controller was promoted. A quick review will often reveal privileges granted to defunct accounts, the IUSR account and other difficult to justify delegations.

To understand Microsoft's best practice for URAs on Domain Controller I suggest you download the Windows Server 2022 Security Baseline and review the group policy report named MSFT Windows Server 2022 - Domain Controller. Better yet you could use Policy Analyzer to compare your environment to the baseline as explained in this article.

The need to review and harden URAs is not limited to Domain Controllers. The same review should be performed for all domain-joined devices.

Group Policy Delegations

Once adversaries acquire privileged credentials, they often use native tools to accomplish their objectives. Manipulation of existing GPOs is a perfect example of such "Living off the Land" techniques. This threat can be compounded by delegating GPO management rights across various support groups. While decentralized GPO management can make operational tasks seem more efficient, it comes at a price.

The group named Group Policy Creator Owners has contributed to this issue. Members of the group can create new GPOs for which they will have full control. The net result is distributed GPO management permissions which can give an attacker many options to deliver a payload via a GPO. As a result, the use of Group Policy Creator Owners is no

longer recommended. Instead, operational processes to minimize policy delegations should be implemented. Historically the Advanced Group Policy Management tool was Microsoft's solution for centralized GPO management but extended support for AGPM will end in April of 2026. In light of that you may want to consider a 3rd party tool that offers similar features.

If you are on the fence about addressing this issue, I recommend you consider that by default any authenticated user can read the ACLs of GPOs. An attacker can use any victims account to quickly determine which accounts can modify a GPO. From there they just need to acquire one of those desktop, helpdesk or similar support accounts.

Organizational Unit Delegations

OU delegations are another area where privileges seem to accumulate over time. Sometimes these delegations have been well thought out and implemented. Other times they are the result of a less structured approach. Below are some examples of elevated permissions that can be useful to an adversary.

- Reset passwords
- Join devices to the domain
- Read confidential attributes
- Create and modify groups
- Create and modify user accounts
- Create and modify computer accounts
- Link GPOs
- Replicate Directory Changes - All (permission require to replicate password from a domain controller used by DCSync)

The Delegation of Control Wizard in Active Directory Users and Computers makes it very easy to grant new permissions on OUs. However, it has no functionality to easily identify what has been custom delegated or revoke the granted rights. A free tool to review what has been delegated is AD ACL Scanner which was written by Robin Granberg. AD ACL Scanner has many features that I think you will find useful as you review your domain and look for ways to remediate permissions applied to OUs.

Privileged Groups

Minimizing membership of privileged groups is a fundamental step in adhering to the principle of least privilege. While removing unnecessary accounts from these groups might be perceived as a lack of trust in individuals and taken personally, it's important to

consider the broader context of credential theft and lateral movement. The issue is more about trust in devices rather than individuals. Those who understand these risks are usually quick to relinquish any level of privilege that exceeds what is necessary for their roles. As you work on reducing your privileged group memberships, it's helpful to communicate that the primary concern is device trust.

When planning the membership of privileged groups, it is beneficial to distinguish between service administration and data administration. Service administration, as the name suggests, involves operational support for Active Directory Domain Services, including tasks such as promoting and supporting domain controllers, managing replication, and updating the schema. These tasks necessitate membership in the built-in privileged groups and cannot be delegated more granularly. On the other hand, data administration encompasses the management of users, groups, password resets, GPOs, and attributes, all of which can be delegated without relying on the built-in groups.

The table below lists the built-in groups that represent the most privilege which should be given priority when performing a Tier 0 access review.

Group Name	**Recommendation**
Account Operators	Account Operators group does not map well to how organizations operate. More appropriate delegations can be implemented to more granularly control the management of objects. As a result, the recommendation is to leave this group empty.
Administrators	Given Administrators grants full control to the Domain Controller's OS, membership should be limited to accounts responsible for operational support of directory services. Due to nesting, there is no need for members of Domain Admins to also be direct members of Administrators.
Backup Operators	To minimize privilege, leave Backup Operators empty and create a special purpose service account that has the URAs of Backup up files and directory and Restore files and directories.
Domain Admins	Membership should be limited to resources responsible for operational support of domain controllers.
Enterprise Admin	In multi domain forests this group is nested in the Administrators group of every domain. When a centralized team is responsible for all domains, this group is often used to minimize the number of accounts an Active Directory administrator would need to possess. However, it is important to consider the blast radius if such an account was compromised.

Group Policy Creator Owners	As previously mentioned, this group allows members to create new GPOs for which they will have full control. Given that will result in decentralized management of GPOs, it is recommended to leave this group empty and pursue other solutions to minimize accounts that can manage group policies.
Print Operators	Domain Controllers should never host print queues or have the print spooler service enabled. In addition to having no members, print operators should have the URAs Load and unload devices drivers and Allow log on locally removed from the Default Domain Controller policy.
Remote Desktop Users	Remote desktop privileges should be limited to accounts used to perform service administration of Active Directory. Additionally, network connectivity to the RDP service (3389) on domain controllers should be restricted using firewall rules or IPsec.
Schema Admins	Schema modification is a very rare event. This group should remain empty and only populated when actively extending the schema.
Server Operators	Members of this group can perform junior admin tasks on domain controllers including start and stop service, manage network shares and manage backups. This group does not align with how Active Directory service administration is performed today. As a result it should remain empty and the URAs Allow logon locally, Back up files and directories, Change the system time, Force shutdown from a remote system, Restore files and directories and Shut down the system should be removed from it in the Default Domain Controllers policy.

The following groups are considered to be equivalent to Tier 0 given they could be used in some manner to elevate privileges. Membership of these groups should also be minimized and monitored for modification.

Group Name	Recommendation
Incoming Forest Trust Builders Group	Members of the Incoming Forest Trust Builders group can create incoming, one-way trusts to this domain. By default, this group has no members.

Key Admins Group	This group is granted write access to msDS-KeyCredentialLink attribute of user and computer objects in a domain which is used to store public keys related to Passwordless authentication such as Windows Hello for Business. The group should be limited to accounts that administer WHFB keys and similar Passwordless key pair credentials
Enterprise Key Admins Group	This group is the same as Key Admins except the scope is the forest instead of just a domain.
Network Configuration Operators Group	This domain group grants the ability to manage TCP/IP and other network configuration settings on domain controllers. It could be used to enable a AiTM attack by manipulating name resolution and IP routing.
Read-only Domain Controllers Group	This group should only contain actual RODCs assuming you must have RODCs. Additionally, some third-party products are designed to be in the group in or order to emulate a RODC. The security risks introduced by such solutions should be fully evaluated.
Replicator Group	This is a legacy group that previously was used for Sysvol replication. By default, it has no members and should remain empty.
Storage Replica Administrators Group	This group can manage storage replicas on domain controllers. By default, this group has no members and should remain empty.
System Managed Accounts Group	This is a new group introduced with Server 2016. By default, the only member is the default account. This group should not have its membership manually modified.
Certificate Service DCOM Access Group	Members of this group can connect to certification authorities in the enterprise and by default is empty. Typically, only PKI administrators need to be added as members of this group.
Allowed RODC Password Replication Group	Members in this group can have their passwords replicated to all read-only domain controllers in the domain. Privileged accounts should not be members.
Cert Publishers Group	Members of this group are permitted to publish certificates to the directory. Membership should be limited to the accounts intended to be used for publishing certificates such as PKI administrators. Additionally, the computer accounts of the Enterprise CAs need to be in this group.

Cloneable Domain Controllers Group	Membership of this group should be limited to domain controllers you wish to clone.
Cryptographic Operators Group	Members are authorized to perform cryptographic operations. Membership should be limited to accounts that require this right for Certificate Services administration
Distributed COM Users Group	Members are allowed to launch, activate and use Distributed COM objects on domain controllers.
DnsUpdateProxy Group	This group is intended to be used by DHCP servers which are registering DNS records on behalf of DHCP clients. The group should only include those DHCP servers.
DnsAdmins Group	Group used to delegate management of DNS zones. This group was not introduced until Server 2003. Prior to then it was common to add an account to Domain Admins in order to manage DNS (e.g. Infrastructure team). Zones created before Windows 2003 need to have the ACLs updated to delegate access to this group.
Domain Controllers Group	This group has the extended right Replicating Directory Changes All. Members can replicate account passwords using that permission. Membership should be limited to domain controllers.
Enterprise Read-only Domain Controllers Group	This group has the extended right Replicating Directory Changes and should be limited to RODCs. Given RODCs are not without risks careful consideration should be given before deploying RODCs.

Kerberos Delegation

Kerberos Delegation enables an account or device to acquire Kerberos service tickets on behalf of another account. It is often referred to as Kerberos Double Hop authentication and is regularly explained using a diagram like this one.

An overly simplified explanation of the flow is:

1. The IIS server has been "trusted for delegation". The user connects to the IIS server using a Kerberos service ticket previously acquired and also provides a copy of its TGT.

1. An application running on the IIS server needs to connect to the SQL server as the user, so it presents the user's TGT to the domain controller and requests a service ticket for the SQL server.

1. The IIS server presents the service ticket to the SQL server and is authenticated in the context of the user's account.

In a perfect world this architecture works great. The user has a SSO experience and is only able to access the data it has been granted to it in the SQL database. However, in the real-world web servers sometimes get compromised, which could allow an adversary to acquire service tickets to other SPN enabled resources by leveraging the users shared TGT.

To mitigate that risk, we want to "constrain" or limit the delegation to select target SPNs. This screenshot shows an example of constrained delegation which limits CONTOSO-WEB1 delegation to the SQL SPN set on the CONTOSO-DB1 computer account. If CONTOSO-WEB1 was to be compromised, the attacker could still acquire service tickets to the CONTOSO-DB1 but not for any other targets.

When Active Directory was first introduced an account was either trusted (unconstrained) or not trusted for delegation. Constrained delegation was introduced with Windows 2003 and Server 2012 R2 took things a step further with Resource-based constrained delegation (RBCD) which allows the trust to be configured on the backside service rather than the frontend service. Additionally, RBCD was designed to work over trust relationships. The following PowerShell queries can be used to locate any computer or user object that has been trusted for unconstrained delegation. If you discover any such objects they should be reconfigured for constrained delegation.

Get-ADComputer -Filter {TrustedForDelegation -eq $true -and primarygroupid -eq 515} -Properties trustedfordelegation, serviceprincipalname, description

Get-ADUser -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation, ServicePrincipalName, Description

In most cases, privileged accounts used to administer Active Directory do not access applications that require Kerberos delegation. As result, least privilege can be imposed on those accounts by configuring the option Account is sensitive and cannot be delegated. Once enabled the account is incapable of sharing a copy of its TGT with a device that has been trusted for delegation (uncontained or constrained).

Exchange Permissions

When Exchange was first integrated with Active Directory (Exchange 2000), a shared permission model was the only option which gave Exchange servers and Exchange administrators the ability to create and manage objects along with elevated permissions

on the domain controllers. At the time, Domain and Exchange administration was often performed by the same team so there was little concern about violating the principle of least privilege. Eventually those responsibilities began to diverge to sperate teams and the concept of split permissions was introduced with Exchange 2010 SP1. Organizations that will continue to have on-prem Exchange servers are encouraged to implement Active Directory split permissions which will change how some operational processes are performed such as creating mailbox users or managing distribution groups. RBAC split permissions is another alternative but it does not provide the same level of privilege reduction for the Exchange objects (Exchange Trusted Subsystem, Exchange Servers group, Organization Management)

For a time, it was necessary to keep an Exchange server on-prem to perform recipient management even after all mailboxes were moved to Exchange Online. That is no longer a requirement due to a new set of Exchange Management Tools. Organizations who adopt the new tools can remove any remaining Exchange servers and then use the CleanupActiveDirectoryEMT.ps1 script to remove the Exchange related permissions from Active Directory.

If the Exchange shared permission cannot be removed, the Exchange Servers and Exchange administrators should be considered Tier 0 rather than Tier 1.

Credential Vaulting

In discussions about revamping privileged access, the concept of credential vaulting often comes up. Credential vaults can be a key component of a privileged account management solution, but how and where you use your account while it's checked out still matters. Consider this scenario:

> 3:00 AM - CONTOSO-FS1 (file server) is compromised. Malicious software is installed that will ship off newly acquired credentials to the adversary.
>
> 9:00 AM - Joe Admin checks out his Domain Admin account from the vault which required multi-factor authentication (MFA).
>
> 11:00 AM - Joe Admin logs on to CONTOSO-FS1 to manage some file share permissions.
>
> 11:01 AM - The adversary receives a message containing the NTLM hash of Joe's account.
>
> 11:30 AM - The adversary uses Joe's account to perform a DCSync attack, replicating the credentials of all domain user objects (including service accounts).
>
> 5:00 PM - Joe finishes his workday and his account goes back in the vault.
>
> 11:00 PM - Joe calls it a day and sleeps well knowing his Domain Admin account is in the vault.

8:00 AM - Joe returns to the office and is informed of a total compromise of Active Directory.

8:30 AM - Joe cancels any vacation plans he had for the next three months.

Hopefully my example illustrates that imposing security tiers for accounts and devices is still relevant, even with a credential vaulting solution. A few observations from it are:

- Proper hardening and monitoring via an Endpoint Detection and Response (EDR) product would have helped mitigate the initial compromise of CONTOSO-FS1.
- Joe exposed a Tier 0 account to perform a Tier 1 function. He should have used a separate account to manage Tier 1 devices.

  MFA secured the check-out of the account but provided no protection against passing the hash once the account was used.

  If Joe had been a member of the Protected Users group, authentication would have been limited to Kerberos, and the NTLM hash would not have been in the LSASS memory of CONTOSO-FS1.

  Adversaries pursue multiple forms of persistence to ensure they retain access. By the time Joe's account was checked back in the adversary already acquired alternative privileged credentials.

User Account Control

User Account Control is a security feature which can minimize the privilege used to launch processes. It is based on a split token model where privileged users begin their session with a full and low privilege token as depicted in the diagram below. Processes are launched default using the low privilege token but can switch to the high privilege token with consent. To be clear, this is a defense in the depth measure that is not intended displace other security controls or credential hygiene practices.

Microsoft baselines recommend the following UAC setting be implemented on domain controller.

Setting name	**Domain Controller Recommendation** **(Server 2022 baseline)**	**Default Setting**
Admin Approval Mode for the Built-in Administrator account	Enabled	Not defined

Allow UIAccess applications to prompt for elevation without using the secure desktop		Disabled
Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop	Prompt for consent for non-Windows binaries (default)
Behavior of the elevation prompt for standard users	Automatically deny elevation requests	Prompt for credentials
Detect application installations and prompt for elevation	Enabled	Enabled
Only elevate executables that are signed and validated		Disabled
Only elevate UIAccess applications that are installed in secure locations	Enabled	Enabled
Run all administrators in Admin Approval Mode	Enabled	Enabled
Switch to the secure desktop when prompting for elevation		Enabled
Virtualize File And Registry Write Failures To Per User Locations	Enabled	Enabled

Hopefully this information will help you review your Active Directory environment and identify opportunities to reduce excessive privileges. As you plan your remediations just keep these Do's and Don'ts in mind.

> **Do** utilize tools to help you perform a deep scan of your environment. Microsoft Unified customers have access to the On-Demand Active Directory Security Assessment as part of their contract. If that is not an option, there are some nice 3rd party assessment tools that are either free or low cost.
>
> **Don't** be afraid to take action once you discover issues. Test the changes in an isolated environment to raise your comfort level. Once you have documented your rollback plan move forward with securing your environment.
>
> **Do** document the changes you make. That will help with troubleshooting if something does not go as planned.

Do proactively monitor for changes in privileged access.

Do mark privileged accounts and groups as "sensitive" if you are using Defender for Identity (MDI). MDI is already aware of which built in privilege groups are sensitive but you will need to let it know about any user, group or device that you have delegated privilege.

Don't forget to review the Security privileged access guidance published by Microsoft.

Updated Jan 16, 2025

Version 1.0