User and Machine Accounts

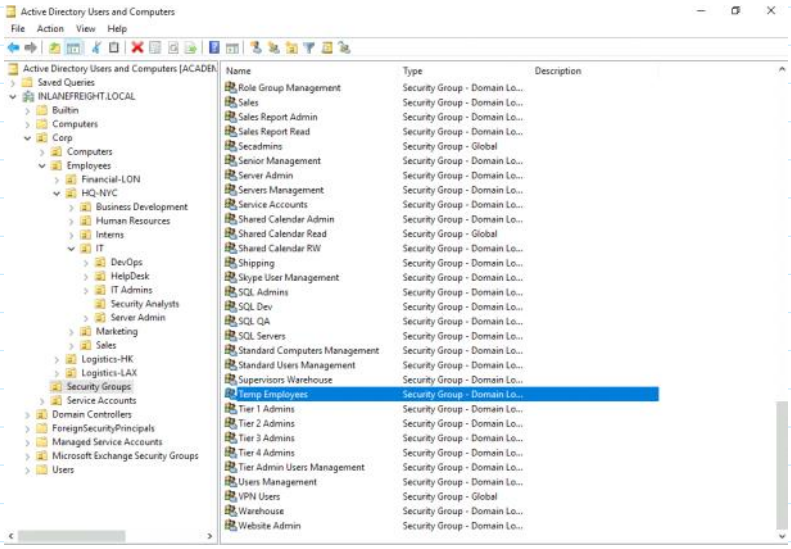
mercredi 27 novembre 2024 12:18 PM

USERS

The management of **user accounts** in **Active Directory (AD)** is a critical aspect of ensuring secure access control in an organization.

Key Concepts:

1. **User Accounts:**
   - **Local User Accounts**: These accounts are created on individual systems (not joined to a domain) and are typically used for accessing local resources or services on the machine.
   - **Domain User Accounts**: Created in Active Directory, these accounts **enable users to log on to any computer that is part of the domain** and **access resources shared within the domain**. They are identified by a unique **User Principal Name (UPN)** and have associated rights and permissions across the network.
2. **Access Token:**
   - When a user logs in, an **access token** is created. This token includes the user's security identity (SID), group memberships, and any other rights or privileges they have. The access token is presented when the user interacts with a process or thread.
3. **Groups and Group Membership:**
   - **Groups** simplify administration by allowing users to inherit permissions based on their group membership.
   - Groups can be used for various purposes, such as controlling access to resources (network shares, applications, etc.).
4. **Service Accounts:**
   - These are special user accounts used by applications or services to run under a specific security context. Service accounts often have elevated privileges and should be managed carefully to minimize security risks. Examples include accounts running web servers, database services, etc.
5. **Deactivated and Disabled Accounts:**
   - **Disabled Accounts**: In an AD environment, an account may be disabled but not deleted. This is often the case **for terminated employees**, **temporary/seasonal** workers, or **contractors**. Disabling accounts ensures that they cannot be used for authentication, while **retaining their information for audit or historical purposes.**
   - **Former Employees**: It's common to have an Organizational Unit (OU) called something like **"Former Employees"** where deactivated user accounts are stored. These accounts may still exist in AD for auditing or compliance purposes but will not be active for login.



Common Account Types and Their Uses:

1. **Standard User Account:**
   - Typical for everyday employees. They have limited permissions based on their role within the organization.
2. **Administrator Account:**
   - These accounts have elevated privileges to manage and configure system settings, user accounts, and more. They are generally assigned to IT staff or other users with a need for high-level system control.
3. **Service Accounts:**
   - Accounts used by services or applications to perform background tasks, such as running a web service, managing a database, or accessing network resources. These accounts should have the minimum necessary privileges to reduce the potential impact if compromised.
4. **Guest Account:**
   - A special account with minimal access, typically used for temporary users or external visitors. The guest account should be restricted and

disabled when not in use.

5. **Deactivated Accounts:**
   - Accounts for former employees, contractors, or temporary workers that are no longer active but are kept for record-keeping purposes. These accounts are often stored in an OU like **"Former Employees"** and are disabled to prevent unauthorized access.

Local Accounts in Windows:

Local accounts are specific to individual systems and provide access to resources on that particular host. These accounts are not part of Active Directory and do not have domain-wide access. Common **local accounts** include:

1. Administrator Account:

- **SID**: **S-1-5-**<domain>**-500**
- This account is **created during the installation of Windows** and holds full control over almost every resource on the system.
- **It cannot be deleted**, but it can be disabled or renamed.
- **By default**, ***this account is disabled on Windows 10 and Server 2016 hosts during installation.***

2. SYSTEM Account: (NT AUTHORITY\SYSTEM)

- A predefined account **used by the operating system for internal functions**. This is the highest privilege level account on Windows.
- The SYSTEM account has **Full Control** over all files and can perform critical OS-level operations.
- It **doesn't appear in the User Manager** and **cannot be assigned to groups.**

3. Guest Account:

- Disabled by default for security reasons.
- Typically allows temporary access with very limited permissions and often has a blank password. It is generally considered a security risk if enabled.

4. Network Service:

- A predefined local account that the Service Control Manager (SCM) uses to run system services.
- When running under this account, **it presents credentials to remote services.**

5. Local Service:

- Another predefined account used by the SCM (Service Control Manager) **for running services with minimal privileges.**
- It presents **anonymous credentials** to the network.

Domain Users:

- **Domain Users** have access to resources in the domain such as file servers, printers, or intranet hosts based on the permissions granted to their accounts or group memberships. Unlike **local users**, they can log in to any host in the domain.

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

1. Administrator

- **Description**: The Administrator account is the most privileged user account in the domain. It has full control over all domain resources, and this account can perform any task across the domain.
- **SID**: **S-1-5-32-544**
- **Purpose**: It is the default administrative account created for managing all domain resources. This account is typically used for domain administration and is often **used to create and manage other domain(current) user accounts.**

2. Guest

- **Description**: The Guest account allows users to log in without a personal account. By default, this account is disabled and should be left disabled for security reasons.
- **SID**: **S-1-5-32-546**
- **Purpose**: This account is typically used **for users who need temporary access with limited privileges** to certain domain resources.

3. KRBTGT

- **Description**: The **KRBTGT** account is a special service account used by the **Key Distribution Center (KDC)** in Active Directory ***for Kerberos authentication.***

- **SID**: **S-1-5-21**-<Domain>**-502**
- **Purpose**: This account is essential for Kerberos ticket generation. It is often targeted in advanced attacks (e.g., **Golden Ticket** attacks) because compromising this account allows attackers to create fraudulent Kerberos tickets.

Administrators

SID : **S-1-5-32-544**

Members of the Administrators group **have complete and unrestricted access to the computer. If the computer is promoted to a domain controller, members of the Administrators group have unrestricted access to the domain.**
This group can't be renamed, deleted, or removed. This built-in group controls access to all the domain controllers in its domain, and it can change the membership of all administrative groups. Members of the following groups can modify the Administrators group membership: the default service Administrators, Domain Admins in the domain, and Enterprise Admins. This group has the special privilege to take ownership of any object in the directory or any resource on a domain controller. This account is considered a service administrator group because its members have full access to the domain controllers in the domain.

A standalone Managed Service Account (sMSA)

gMSAs provide a single identity solution for services running on a server farm or on systems behind Network Load Balancer. By providing a gMSA solution, you can configure services for the new gMSA principal while Windows handles the password management.
When services or service administrators use a gMSA, they don't need to manage password synchronization between service instances. The gMSA supports hosts kept offline for an extended time period and manages member hosts for all instances of a service. You can deploy a server farm that supports a single identity that existing client computers can authenticate without having to know which service instance they're connecting to.
Although failover clusters don't provide support for gMSAs, services that operate on the Cluster service can utilize a gMSA or sMSA if they're a Windows service, an app pool, a scheduled task, or natively support gMSA or sMSA.

À partir de l'adresse <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-managed-service-accounts/group-managed-service-accounts/group-managed-service-accounts-overview>

4. Domain Admins (group)

- **Description**: The Domain Admins group **is a predefined group in AD** that has **full control of all domain controllers** and **other domain objects**. Members of this group are typically responsible for domain administration.
- **SID**: **S-1-5-21-<domain>-512**
- **Purpose**: Users in this group can perform any task in the domain, including managing user accounts, group policies, and domain controllers.
  Default members : Administrator
  Default member of : Administrators , Denied RODC Password Replication

5. Enterprise Admins (group)

- **Description**: The Enterprise Admins group is a **broader group than Domain Admins.** Members of this group have administrative **control across all domains *in a forest.***
- **SID**: **S-1-5-32-519**
- **Purpose**: This group is used for administrative tasks that span multiple domains within an Active Directory forest, including **forest-wide configurations** like **DNS** and **schema changes**.

6. Schema Admins (group)

- **Description**: The Schema Admins group has the ability to **modify the Active Directory schema.**
- **SID**: **S-1-5-32-518**
- **Purpose**: Members of this group are responsible for making changes to the schema, which affects how objects in AD are defined and stored.

7. Account Operators (group)

- **Description**: The Account Operators group **can create**, **modify**, and **delete** user accounts and groups **within the domain**.
- **SID**: S-1-5-32-548
- **Purpose**: This group allows delegation of user and group account management **but without full administrative privileges.**

8. Server Operators (group)

- **Description**: The Server Operators group has rights to **manage servers** and perform tasks like **shutting down the server, backing up files**, or **managing local groups.**
- **SID**: S-1-5-32-549
- **Purpose**: Members of this group can manage server configurations and ***perform certain system-level administrative tasks***.

9. Print Operators (group)

- **Description**: The Print Operators group has permissions to **manage printers** and print queues on the domain.

- **SID**: S-1-5-32-550
- **Purpose**: This group is used for tasks related to printer management, including adding or removing printers and managing print jobs.

10. Backup Operators (group)

- **Description**: The Backup Operators group has permission to **back up** and **restore** **files on domain controllers** and **other systems**.
- **SID**: S-1-5-32-551
- **Purpose**: Members can perform backup and restore operations, including files that are otherwise protected.

11. Remote Desktop Users (group)

- **Description**: The Remote Desktop Users group grants members the **ability to log in to the system using Remote Desktop Services (RDS)**.
- **SID**: **S-1-5-32-555**
- **Purpose**: Members can log into servers or workstations remotely through Remote Desktop Protocol (**RDP**).

12. Domain Users (group)

- **Description**: The Domain Users group is **the default group assigned to all users within the domain.**
- **SID**: S-1-5-32-545
- **Purpose**: This group **grants** **basic rights** **for** **logging into domain-joined computers**, ***accessing domain resources*** ***like file shares***, and ***using network printers.***

13. DnsAdmins (group)

- **Description**: The DnsAdmins group has **administrative control over DNS server settings within the domain.**
- **SID**: S-1-5-32-580
- **Purpose**: Members can manage DNS settings, which can affect domain resolution and service availability across the network.

14. Enterprise Read-Only Domain Controllers (RODCs) (group)

- **Description**: The Enterprise Read-Only Domain Controllers group is used to **define read-only** **domain controllers** **within the forest.**
- **SID**: S-1-5-32-573
- **Purpose**: These domain controllers are typically placed in locations where security is a concern, such as branch offices, and **allow limited administrative control.**

15. Local Administrators (group)

- **Description**: The Local Administrators group consists of users who have administrative control over individual machines ***but do not have domain-wide privileges.***
- **SID**: S-1-5-32-544
- **Purpose**: Members of this group **can administer local settings** **on specific machines**, including installing software and modifying system configurations.

Important Considerations for Domain Users:

- Domain users can be members of multiple **groups**, and their permissions are typically managed via group membership, making administration easier and more scalable.
- The **KRBTGT Account** is a **special built-in account in AD** **responsible for the Key Distribution Service (KDS),** which is involved in authenticating and providing access to domain resources. **Attackers often target this account**, as compromising it can lead to significant domain control through attacks like **Golden Ticket** attacks.

Key User Naming Attributes in AD:

Understanding these naming attributes is essential for identifying user objects and improving security within AD:

UserPrincipalName (UPN):	▪ The primary logon name for a user, often resembling an email address (e.g., username@domain.com). ▪ Used as the default logon credential for accessing domain resources.
ObjectGUID:	▪ A unique identifier for the user object within AD. ▪ It remains unchanged even if the user is deleted and recreated, providing a stable reference for the object.
SAMAccountName:	▪ This attribute represents the legacy logon name, which is compatible with older versions of Windows (pre-2000). ▪ It's typically a short-form username (e.g., domain\username).
objectSID (Security Identifier):	▪ A globally unique identifier for a user or object in AD. ▪ It identifies the user and their group memberships during security interactions with the domain controllers.
sIDHistory:	▪ Contains previous SIDs when a user object is migrated between domains.

	▪ It allows access to resources in the old domain after migration, ensuring users maintain access during domain migrations.

```
PS C:\htb > Get-ADUser   -Identity    htb-student

DistinguishedName : CN=htb student,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
Enabled           : True
GivenName         : htb
Name              : htb student
ObjectClass       : user
ObjectGUID        : aa799587-c641-4c23-a2f7-75850b4dd7e3
SamAccountName    : htb-student
SID               : S-1-5-21-3842939050-3880317879-2865463114-1111
Surname           : student
UserPrincipalName : htb-student@INLANEFREIGHT.LOCAL
```

Domain-joined vs. Non-Domain-joined Machines

1. Domain-Joined Machines

- **Management**: Domain-joined machines are **part of a centralized management system** through **Active Directory (AD)**. The **Domain Controller (DC)** handles policies, configurations, and updates, ensuring consistency across all machines within the domain.
- **Resource Sharing**: Domain-joined computers have **easy access to resources across the entire domain**, such as file servers, printers, and databases. **Users can log into any domain-joined machine** and **have their profile and settings automatically applied.**
- **Group Policy**: Machines in the domain are governed by **Group Policy Objects (GPOs)**, which define security settings, software installations, and other administrative tasks across the network. These **policies are applied consistently to all domain-joined systems**.
- **User Authentication**: Users authenticate using their **domain credentials**, which are managed centrally. **The same login credentials allow access to multiple machines** and **domain resources**.
- **Security**: Domain-joined machines **typically have higher security because they are controlled through the domain**, and administrators can enforce strict security measures like **password policies**, **account lockout policies**, and **two-factor authentication**.
- **Ease of Administration**: Centralized management via **Active Directory** and **Group Policies** simplifies the administration of software updates, security patches, and user permissions across all machines in the domain.

Example: An employee in a company can log into any workstation in the company with their credentials, and they will have access to shared files, printers, and other networked resources.

2. Non-Domain-Joined Machines (Workgroup Machines)

- **Management**: Non-domain-joined machines do not have centralized management. They are independent and do not rely on a domain controller. **Each machine is essentially its own isolated unit.**
- **Resource Sharing**: **Sharing resources between workgroup machines is more complicated and requires manual configuration**. Each machine must be configured individually to allow file and printer sharing.
- **User Authentication**: **Local user accounts** are **created on each machine**. These accounts are not centralized, meaning **the same user will need to have separate credentials for each machine they want to access**.

- **Group Policy**: Workgroup machines do not receive **Group Policy** updates from a domain controller. Any system configurations and updates must be applied individually on each machine.
- **Security**: Security policies and settings on workgroup machines are not centralized. This means it is more difficult to enforce consiste nt security settings across multiple machines. **The lack of centralized management also makes it harder to implement standard security measures**.
- **Ease of Administration**: Managing software, updates, and user permissions is done locally on each machine. In larger environments, this can become cumbersome, as there is no centralized way to control or automate these tasks.

Example: In a small office, each computer might have its own set of local user accounts, and each machine needs to be manually configured to share resources with others in the same workgroup.

Groups :

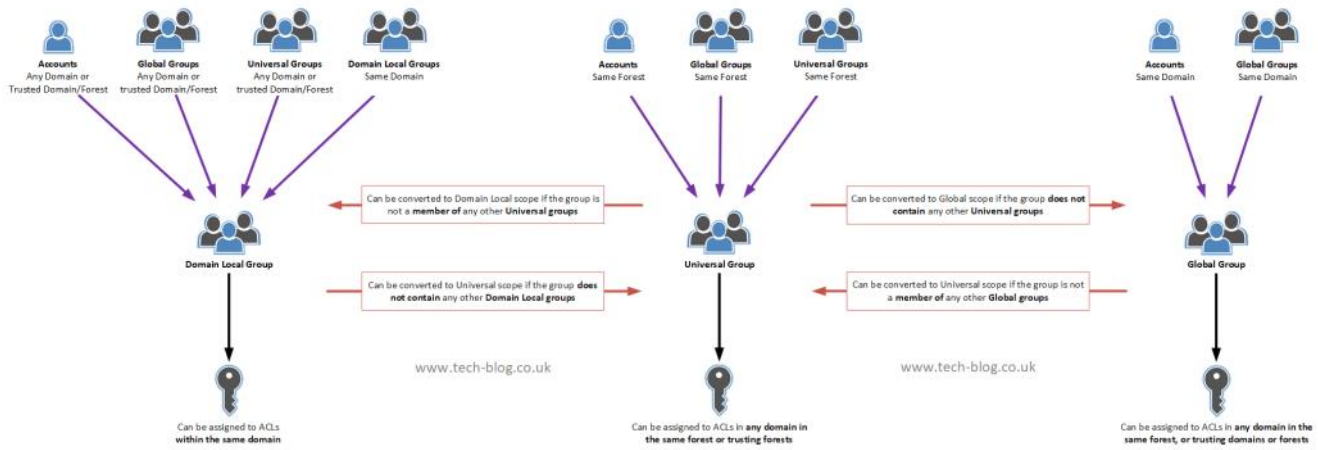
Group Types

Group Type	Purpose	Used for Assigning Permissions?
Security	Access control for resources All users added to a security group will inherit any permissions assigned to the group, making it easier to move users in and out of groups while leaving the group's permissions unchanged.	**Yes**
Distribution	Email distribution lists ("To" group) This type of group cannot be used to assign permissions to resources in a domain environment.	**No**

Group Scopes

Group Scope	Membership	Usage	Example
Domain Local	Can include users, computers, and groups from the **same domain**, **other domains**, or even **trusted forests**.	Assign permissions to resources **specific to the domain** (e.g., printers, shared folders). **NB** : Local groups **cannot be used in other domains** but CAN contain users from OTHER domains	A domain local group can include members from other domains but can only be used to control resources within the domain where it resides.
Global	Can only include objects **from the same domain.**	Grant access **in another domain.** Typically used as members of domain local groups for assigning permissions or added to universal groups for wider access.	A global group called "**HR_Employees**" can include **all HR department users** from a domain.
Universal	**Any domain** in the forest	Provide access to resources across multiple domains within a forest. Best suited for large enterprises with multi-domain environments.	A universal group called "**All_Managers**" could include **managers from multiple domains** and provide them **access to resources across the entire forest.**

Active Directory Group Scopes



Domain Local Group:

- **Scope**: Resources in the same domain.
- **Membership**:
  - Can include:
    - User accounts and computer accounts from any domain in the forest.
    - Global groups, universal groups, and other domain local groups from the same domain.
  - Does **not replicate** membership to other domains or the Global Catalog.
- **Usage**:
  - Ideal for granting access to resources like shared folders or printers within a domain.
  - Example: A "Finance Printers" domain local group might control access to all printers used by the finance team within a specific domain.

Global Group

- **Purpose**: Primarily used to manage permissions for resources within a single domain.
- **Scope**:
  - Can be added to other groups or assigned permissions on resources in **any domain** within the forest.
- **Membership:**
  - Members can **only** come **from the domain in which the group is created.**
  - Global Groups **replicate only** their **memberships**, not the permissions they grant.
  - Membership information is stored in the Global Catalog, allowing domain controllers in other domains to use this data for **authentication** and **authorization** purposes.

- **Usage**:
  - Ideal for grouping users who share similar job roles within the same domain.
  - For example, a "Sales Team" group in Domain A would only include user accounts from Domain A.
- **Advantages**:
  - Keeps membership focused on a single domain, simplifying management.
  - Highly efficient in terms of replication because it does not replicate membership information outside the domain.

Universal Group

- **Purpose**: Used to assign permissions across multiple domains within a forest.
- **Scope**:
  - Members can come from **any domain** in the forest.
  - Can be assigned permissions on resources in **any domain** in the forest.
- **Usage**:
  - Useful for grouping users, groups, and computers from different domains for resource access across the forest.
  - For example, a "Forest Admins" group might include members from multiple domains to manage resources universally.
- **Replication**:
  - Membership is stored in the **Global Catalog** and is replicated forest-wide.
  - This replication overhead can cause increased network traffic, especially if membership changes frequently.

A **Domain Local** Group **can only be converted to a Universal Group if the Domain Local Group does NOT contain any other Domain Local Groups as members:**

Practical Implications

- Before converting a Domain Local Group to a Universal Group, administrators must remove any nested Domain Local Groups and replace them with individual members or other compatible groups (e.g., Global Groups).
- This requirement ensures that **Universal Groups remain effective and manageable** for access control across multiple domains.

A Universal Group can only be converted to a **Global Group/Domain Local if it does NOT contain any other Universal Groups as members.**

- If a Universal Group containing another Universal Group were converted to a **Global Group**, the nested memberships could introduce **conflicts or errors** in security and access permissions because the nested Universal Group might include members from domains outside the Global Group's scope.

- **Domain Local Groups**, while they can include members from other domains, are primarily intended for **managing resources locally within their domain**.
- If a Domain Local Group contained another Universal Group as a member, resolving memberships and permissions for objects outside the local domain could become **complex** or **error-prone**, especially during replication. (in case the universal group is nested)

```
PS C:\htb> Get-ADGroup  -Filter * |select samaccountname,groupscope
```

```
samaccountname                groupscope
--------------                ----------
Administrators                DomainLocal
Users                         DomainLocal
Guests                        DomainLocal
Print Operators               DomainLocal
Backup Operators              DomainLocal
Replicator                    DomainLocal
Remote Desktop Users          DomainLocal
Network Configuration Operators DomainLocal
Distributed COM Users         DomainLocal
IIS_IUSRS                     DomainLocal
Cryptographic Operators       DomainLocal
Event Log Readers             DomainLocal
Certificate Service DCOM Access DomainLocal
RDS Remote Access Servers     DomainLocal
RDS Endpoint Servers          DomainLocal
RDS Management Servers        DomainLocal
Hyper-V Administrators        DomainLocal
Access Control Assistance Operators DomainLocal
Remote Management Users       DomainLocal
Storage Replica Administrators DomainLocal
Domain Computers              Global
Domain Controllers            Global
Schema Admins                 Universal
Enterprise Admins             Universal
Cert Publishers               DomainLocal
Domain Admins                 Global
Domain Users                  Global
Domain Guests                 Global

<SNIP>
```

Built-in vs. Custom Groups

1. Built-in Groups:

- Automatically created when a domain is initialized.
- Typically **Domain Local Groups** with specific administrative purposes.
- Examples:

1. Domain Admins:

- **SID**: S-1-5-32-544 (Note: The SID S-1-5-32-544)
- **Scope**: The *Domain Admins* group is a **Domain Local** group, but it has a broader role across the domain:
  - It is used to grant full administrative rights to **members** within the domain where the group resides.
  - The *Domain Admins* group can contain members from **any domain** in the forest (including trusted domains).
- **Privileges**:
  - Members of *Domain Admins* have full control over **domain controllers** and all domain resources.
  - They also automatically have **local administrative privileges** on all computers joined to the domain, including domain controllers.
  - They can create and manage **Active Directory objects** (such as users, computers, and groups), and configure domain-wide settings and policies (such as Group Policy).
- **Replication**:
  - The **membership** of *Domain Admins* is not replicated to the **Global Catalog** (because it is a **Domain Local** group), but the group itself is replicated across all domain controllers in the domain.
  - This group is primarily used to manage resources within the specific domain.

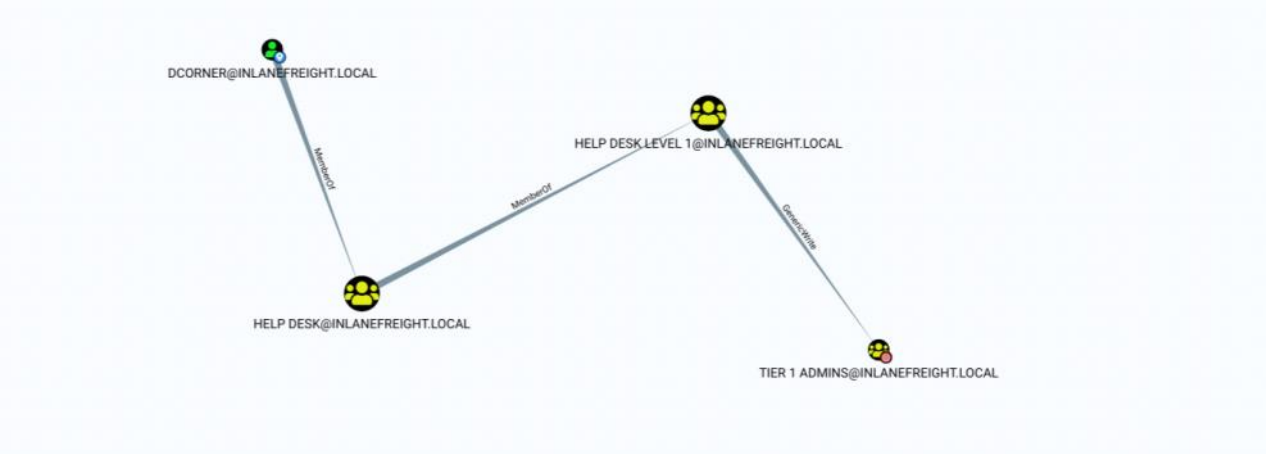
- **Note**: **Built-in groups often do not allow group nesting.**

2. Custom Groups:

- Created by organizations to meet specific needs.
- Used to manage user access, apply permissions, or for email distribution.
- Can be Security or Distribution groups and any scope (Domain Local, Global, Universal).
- Additional custom groups may be added automatically by software (e.g., Microsoft Exchange), which may introduce highly privileged groups requiring strict management.

Nested Group Membership

Below is an example of privileges inherited through nested group membership. Though DCorner is not a direct member of Helpdesk Level 1, their membership in Help Desk grants them the same privileges that any member of Helpdesk Level 1 has. In this case, the privilege would allow them to add a member to the Tier 1 Admins group (GenericWrite). If this group confers any elevated privileges in the domain, it would likely be a key target for a penetration tester. Here, we could add our user to the group and obtain privileges that members of the Tier 1 Admins group are granted, such as local administrator access to one or more hosts that could be used to further access.



Important Group Attributes

Like users, groups have many attributes. Some of the most important group attributes include:

- **cn**: The cn or Common-Name is the name of the group in Active Directory Domain Services.
- **member**: Which user, group, and contact objects are members of the group.
- **groupType**: An integer that specifies the group type and scope.
- **memberOf**: A listing of any groups that contain the group as a member (nested group membership).
- **objectSid**: This is the security identifier or SID of the group, which is the unique value used to identify the group as a security principal.

AD Rights and Privileges

- **Rights** : are typically assigned to users or groups and deal with **permissions to access an object** such as a file

  while

- **privileges** : **grant a user permission to perform an action** such as run a program, shut down a system, reset passwords, etc.

Privileges can **be assigned individually** to users **or** conferred upon them **via** built-in or custom **group membership**. Windows computers have a concept called User Rights Assignment, which, while referred to as rights, **are actually types of privileges granted to a user**. We will discuss these later in this section. We must have a firm grasp of the differences between rights and privileges in a broader sense and precisely how they apply to an AD environment.

Built-in AD Groups

AD contains many default or built-in security groups, some of which grant their members powerful rights and privileges which can be abused to escalate privileges within a domain and ultimately gain Domain Admin or SYSTEM privileges on a Domain Controller (DC). Membership in many of these groups should be tightly managed as excessive group membership/privileges is a common flaw in many AD networks that attackers look to abuse. Some of the most common built-in groups are listed below.

Group Name	Description
Account Operators **S-1-5-32-548**	Members can **create** and **modify** most types of accounts, including those of users, local groups, and global groups, and members **can log in locally to domain controllers**. **They cannot manage the**; Administrator account, administrative user accounts, **or** members of the Administrators, Server Operators, Account Operators, Backup Operators, or Print Operators groups.
Administrators **S-1-5-32-544**	Members have **full** and **unrestricted access to a computer** or **an entire domain** if members are in this group on a Domain Controller.
Backup Operators **S-1-5-32-549**	Members can **back up** and **restore all files on a computer**, **regardless of the permissions set on the files**. Backup Operators can also **log on to** and **shut down** the computer. Members **can log onto DCs locally** and **should be considered Domain Admins**. They **can make shadow copies** of the **SAM/NTDS database,** which, if taken, can be used to extract credentials and other juicy info.
DnsAdmins **S-1-5-32-580**	Members have access to network DNS information. *The group will only be created if the DNS server role is or was at one time installed on a domain controller in the domain.*
Domain Admins **S-1-5-32-512**	Members have **full access to administer the domain** and **are members of the local administrator's group on all domain-joined machines.**
Domain Computers **S-1-5-32-515**	**Any computers created in the domain** (aside from domain controllers) **are added to this group.**
Domain Controllers **S-1-5-32-516**	Contains **all DCs within a domain**. New DCs are added to this group automatically.
Domain Guests **S-1-5-32-518**	This group includes the **domain's built-in Guest account**. Members of this group **have a domain profile created when signing onto a domain-joined computer as a local guest.**
Domain Users **S-1-5-32-517**	This group contains **all user accounts in a domain**. A new user account created in the domain is automatically added to this group.
Enterprise Admins **S-1-5-9**	Membership in this group provides **complete configuration access within the domain.** The group **only exists in the root domain of an AD forest.** Members in this group are granted the ***ability to make forest-wide changes*** such as **adding a child domain** or **creating a trust**. The Administrator account for the forest root domain is the only member of this group by default.
Event Log Readers **S-1-5-32-573**	Members can **read event logs on local computers**. The group is only created when a host is promoted to a domain controller.
Group Policy Creator Owners **S-1-5-32-549**	Members **create**, **edit**, or **delete** **Group Policy Objects** in the domain.
Hyper-V Administrators **S-1-5-32-579**	Members have **complete** and **unrestricted access to all the features in Hyper-V**. If there are virtual DCs in the domain, any virtualization admins, such as members of Hyper-V Administrators, should be considered Domain Admins.
IIS_IUSRS **S-1-5-32-557**	This is a **built-in group** used by Internet Information Services (IIS), beginning with IIS 7.0.
Pre–Windows 2000 Compatible Access **S-1-5-32-554**	This group exists for backward compatibility for computers running Windows NT 4.0 and earlier. Membership in this group is often a leftover legacy configuration. **It can lead to flaws where anyone on the network can read information from AD without requiring a valid AD username and password.**
Print Operators **S-1-5-32-550**	Members can **manage, create, share, and delete** **printers that are connected to domain controllers in the domain** along with any printer objects in AD. **Members are allowed to log on to DCs locally** and **may be used to load a malicious printer driver and escalate privileges within the domain.**
Protected Users **S-1-5-32-569**	Members of this group are provided additional protections against credential theft and tactics such as Kerberos abuse.
Read-only Domain Controllers **S-1-5-32-568**	Contains **all Read-only domain controllers in the domain.**
Remote Desktop Users **S-1-5-32-555**	This group is used to grant users and groups permission to connect to a host via Remote Desktop (**RDP**). **This group cannot be renamed, deleted, or moved.**
Remote Management Users **S-1-5-32-560**	This group can be used to grant users remote access to computers via Windows Remote Management (WinRM)
Schema Admins **S-1-5-32-549**	Members **can modify the Active Directory schema**, which is the way all objects with AD are defined. This group **only exists in the root domain of an AD forest**. The Administrator account for the forest root domain is the only member of this group by default. (like Entreprise Admins group)
Server Operators	This group **only exists on domain controllers**. Members can **modify services, access SMB shares, and backup files** on domain

S-1-5-32-561	controllers. **By default, this group has no members.**

Important Notes:

- **Enterprise Admins**: The **Enterprise Admins** group is a special group that applies across the entire forest and has **SID S-1-5-9**. Members of this group have full administrative rights across all domains within the forest.
- **Pre-Windows 2000 Compatible Access**: This group allows backwards compatibility for legacy applications and access control mechanisms.
- **Protected Users**: This group is used to enhance security for highly privileged accounts by placing them in a special group **that restricts certain authentication protocols (like NTLM).**

Server Operators Group Details

```
PS C:\htb>  Get-ADGroup -Identity "Server Operators" -Properties *
```

```
adminCount                : 1
CanonicalName             : INLANEFREIGHT.LOCAL/Builtin/Server Operators
CN                        : Server Operators
Created                   : 10/27/2021 8:14:34 AM
createTimeStamp           : 10/27/2021 8:14:34 AM
Deleted                   :
Description               : Members can administer domain servers
DisplayName               :
DistinguishedName         : CN=Server Operators,CN=Builtin,DC=INLANEFREIGHT,DC=LOCAL
dSCorePropagationData     : {10/28/2021 1:47:52 PM, 10/28/2021 1:44:12 PM, 10/28/2021 1:44:11 PM, 10/27/2021
                            8:50:25 AM...}
GroupCategory             : Security
GroupScope                : DomainLocal
groupType                 : -2147483643
HomePage                  :
instanceType              : 4
isCriticalSystemObject    : True
isDeleted                 :
LastKnownParent           :
ManagedBy                 :
MemberOf                  : {}
Members                   : {}
Modified                  : 10/28/2021 1:47:52 PM
modifyTimeStamp           : 10/28/2021 1:47:52 PM
Name                      : Server Operators
nTSecurityDescriptor      : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory            : CN=Group,CN=Schema,CN=Configuration,DC=INLANEFREIGHT,DC=LOCAL
ObjectClass               : group
ObjectGUID                : 0887487b-7b07-4d85-82aa-40d25526ec17
objectSid                 : S-1-5-32-549
ProtectedFromAccidentalDeletion : False
SamAccountName            : Server Operators
sAMAccountType            : 536870912
sDRightsEffective         : 0
SID                       : S-1-5-32-549
SIDHistory                : {}
systemFlags               : -1946157056
uSNChanged                : 228556
uSNCreated                : 12360
whenChanged               : 10/28/2021 1:47:52 PM
whenCreated               : 10/27/2021 8:14:34 AM
```

```
PS C:\htb>  Get-ADGroup -Identity "Domain Admins" -Properties * | select
DistinguishedName,GroupCategory,GroupScope,Name,Members
```

```
DistinguishedName : CN=Domain Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Admins
Members           : {CN=htb-student_adm,CN=Users,DC=INLANEFREIGHT,DC=LOCAL, CN=sharepoint
                    admin,CN=Users,DC=INLANEFREIGHT,DC=LOCAL, CN=FREIGHTLOGISTICSUSER,OU=Service
                    Accounts,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL, CN=PROXYAGENT,OU=Service
                    Accounts,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL...}
```

User Rights Assignment

Depending on their current group membership, and other factors such as privileges that administrators can assign via Group Policy (GPO), users can have various rights assigned to their account. This Microsoft article on User Rights Assignment provides a detailed explanation of each of the user rights that can be set in Windows. Not every right listed here is important to us from a security standpoint as penetration testers or defenders, but some rights granted to an account can lead to unintended consequences such as privilege escalation or access to sensitive files. For example, **let's say we can gain write access over a Group Policy Object (GPO) applied to an OU containing one or more users that we control**. In this example, we could potentially leverage a tool such as SharpGPOAbuse to assign targeted rights to a user. We may perform many actions in the domain to further our access with these new rights. A few examples include:

Privilege	Description
SeRemoteInteractiveLogonRight	This privilege could give our target user **the right to log onto a host via Remote Desktop (RDP)**, which could potentially be used to obtain sensitive data or escalate privileges.
SeBackupPrivilege	This grants a user the **ability to create system backups** and could be used to **obtain copies of sensitive system files** that can be used to retrieve passwords **such as the SAM** and **SYSTEM Registry hives** and the **NTDS.dit** Active Directory **database** file.
SeDebugPrivilege	This allows a user to **debug and adjust the memory of a process**. With this privilege, attackers **could utilize a tool** such as **Mimikatz to read the memory space of the Local System Authority (LSASS) process** and **obtain any credentials stored in memory.**
SeImpersonatePrivilege	This privilege **allows us to impersonate a token of a privileged account** such as NT AUTHORITY\SYSTEM. This could be leveraged with a tool such as **JuicyPotato**, **RogueWinRM**, **PrintSpoofer**, etc., **to escalate privileges on a target system.**
SeLoadDriverPrivilege	A user with this privilege **can load and unload device drivers** that could potentially be used to escalate privileges or compromise a system.
SeTakeOwnershipPrivilege	This **allows a process to take ownership of an object**. At its most basic level, we could **use this privilege to gain access to a file share** or a file on a share that was otherwise not accessible to us.

There are many techniques available to abuse user rights detailed here and here. Though outside the scope of this module, it is essential to understand the impact that assigning the wrong privilege to an account can have within Active Directory. A small admin mistake can lead to a complete system or enterprise compromise.

Viewing a User's Privileges

Standard Domain User's Rights

```
PS C:\htb> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

We can see that the rights are very limited, and none of the "dangerous" rights outlined above are present.

Domain Admin Rights Non-Elevated

```
PS C:\htb> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

We can see the following in a **non-elevated console** which does not appear to be anything more than available to the standard domain user. This is because, by default, **Windows systems do not enable all rights to us unless we run the CMD or PowerShell console in an elevated context**. **This is to prevent every application from running with the highest possible privileges**. This is controlled by something called User Account Control (UAC) which is covered in-depth in the Windows Privilege Escalation module.

Domain Admin Rights Elevated

If we enter the same command **from an elevated PowerShell console**, we can see the complete listing of rights available to us:

```
PS C:\htb> whoami /priv

PRIVILEGES INFORMATION
----------------------
Privilege Name                Description                          State
============================= ==================================== ========
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process   Disabled
SeMachineAccountPrivilege     Add workstations to domain           Disabled
SeSecurityPrivilege           Manage auditing and security log     Disabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects Disabled
SeLoadDriverPrivilege         Load and unload device drivers       Disabled
SeSystemProfilePrivilege      Profile system performance           Disabled
SeSystemtimePrivilege         Change the system time               Disabled
SeProfileSingleProcessPrivilege Profile single process             Disabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority       Disabled
SeCreatePagefilePrivilege     Create a pagefile                    Disabled
SeBackupPrivilege             Back up files and directories        Disabled
SeRestorePrivilege            Restore files and directories        Disabled
SeShutdownPrivilege           Shut down the system                 Disabled
SeDebugPrivilege              Debug programs                       Enabled
SeSystemEnvironmentPrivilege  Modify firmware environment values   Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system  Disabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeEnableDelegationPrivilege   Enable computer and user accounts to be trusted for delegation Disabled
SeManageVolumePrivilege       Perform volume maintenance tasks     Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
SeCreateSymbolicLinkPrivilege Create symbolic links                Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
```

Backup Operator Rights

User rights increase based on the groups they are placed in or their assigned privileges. Below is an example of the rights granted to a Backup Operators group member. **Users in this group have other rights currently restricted by UAC** (additional rights such as the powerful **SeBackupPrivilege are not enabled by default in a standard console session**). Still, we can see from this command that they have the **SeShutdownPrivilege**, which **means they can shut down a domain controller**. This privilege on its own could not be used to gain access to sensitive data but **could cause a massive service interruption should they log onto a domain controller locally** (not remotely via RDP or WinRM).

```
PS C:\htb> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeShutdownPrivilege           Shut down the system           Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

dzdz