Tier 0 Built-In Groups

Active Directory Built-In Groups to Audit

This security post continues the mini series Active Directory Builtin groups that are often overlooked. The permissions for the groups are granted by default upon the creation of a domain. The focus on the these groups plans to be a reference point for budding security analysts and engineers.

For a full list of permissions on the default built in groups, please reference the Microsoft article

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b–privileged-accounts-and-groups-in-active-directory

The list of groups covered in this post, in alphabetical order:

Each group will be defined with my everyday and very general overview. I'll list security fears related to the rights granted to the group. I'll then finish up by describing some basic recommendations to perform on the group listed and accounts added to the group.

Administrators

Defined:

Often overlooked by auditors, this group is God-Mode. Full access to all objects on the domain.

Danger:

- Groups or users are often added directly to this group
- Default audits only require reporting on "Domain Admins" and often overlook this group

Recommendation:

- Audit the group membership, starting today
- Remove any groups nested inside this group besides: Domain Administrators and Enterprise Administrators
- Remove any users added directly to this group

Domain Admins

Defined: This group is nested in the administrators group (nested god mode). By default it is also listed as administrator on all workstations and servers in the domain.

Danger:

- Everything from the administrator list
- Member of every computer's admin group

Recommendation:

- Limit this group to 5 users max
- Admins: Get in a room to talk about who needs to be in this group. Look around the room. Identify everyone in the room at that moment. Kick everyone out of the group that is not currently in the room
- Monitor and alert for all domain admin account activity

Enterprise Admins

Defined: Forest administrators. The EA group is granted rights to affect forest wide changes: adding/removing domains, creating trusts, upgrading/raising forest levels

Danger:

- This group isn't often needed after the initial setup of a simple domain
- Can create rogue trust to compromised domain. This would provide a direct persistent path to compromise a domain

Recommendation:

- Remove all users and groups from this group
- Monitor and alert on this group's additions and removals

The above groups should be the groups auditors are checking. If you are planning on creating a self directed risk assessment begin your documentation with a confirmation that these groups are on your audit list.

Account operators

Defined: Often used as the default group for managing users groups and computers in the domain, this group has many permissions often overlooked. The permissions granted to this group are granted at the root of the domain. This group controls most every user and group and computer in the entire organization

Danger:

- Can read the LAPS attribute on all computers in the domain
- Default permissions to log on locally to domain controllers
- Can self escalate into exchange groups, which have write access on the root of the domain

The recommendation:

- Empty this group
- Apply permissions directly to OUs instead of through this domain wide group - I'll be posting about unraveling the account operators later

Backup operators

Defined: This group is used to create system backups of the most privileged servers in the domain.

Danger:

- Can override security restrictions
- Allow log on locally
- Allow log on as batch job
- Shut down systems
- Can backup files (ntds.dit)

The recommendation:

- Empty the group if you can.
- Monitor logins from accounts in this group
- Use this group for least privileged rights to back up Active Directory.
- Time bound the service account in the group

Exchange groups

Defined: Microsoft exchange creates these groups when an administrator installs exchange into an Active Directory environment. Follow this link for the full list of groups created are in the Microsoft Exchange Security Groups OU.

Danger:

- Exchange groups can edit the security on the root of the domain.
- As effective as Domain admin with root ACLpermissions

The recommendation:

- Remove all users from the organization management group
- Perform a full mitigation [per Sean's instructions](https://adsecurity.org/?p=4119}

Group policy creator owners

Defined: Members of this group have full control over all group policy objects (GPOs) in the domain. This includes changing the security of these GPOs, adding additional users to any GPO, and editing GPOs.

Danger:

- GPOs applied to root can affect all users and computers on the domain
- Can control highly privileged policies that control privileged users and computers

Recommendation:

Remove all users from this group

Print Operators

Defined: Members can log on locally to domain controllers. Load and unload drivers on domain controllers. Shut down the DOMAIN CONTROLLERS.

Danger:

No one but DAs should be performing those functions listed above

Recommendation:

Empty the group

Remote desktop services users

Defined: can log onto computers via RDP

Danger

- Can access all machines on the domain
- Machines often have user privilege exploits that allow users to gain admin access

Recommendation:

- Empty the group
- Don’t put “Domain Users” in this group
- Domain Users in RDP Users

Server operators

Defined: members of this group can administer servers in the domain

Danger:

- Unintended access granted to all servers in the domain through this group
- Users in this group are often easy pivot point for attacks for lateral movement

Recommendation:

Empty the group

> The common goal here for all these built in groups is to empty the group when possible. Remove all users. Remove all groups nested inside these groups. Once completed your AD environment will be in a much more secure state.