Beyond Domain Admins – Domain Controller & AD Administration

adsecurity.org

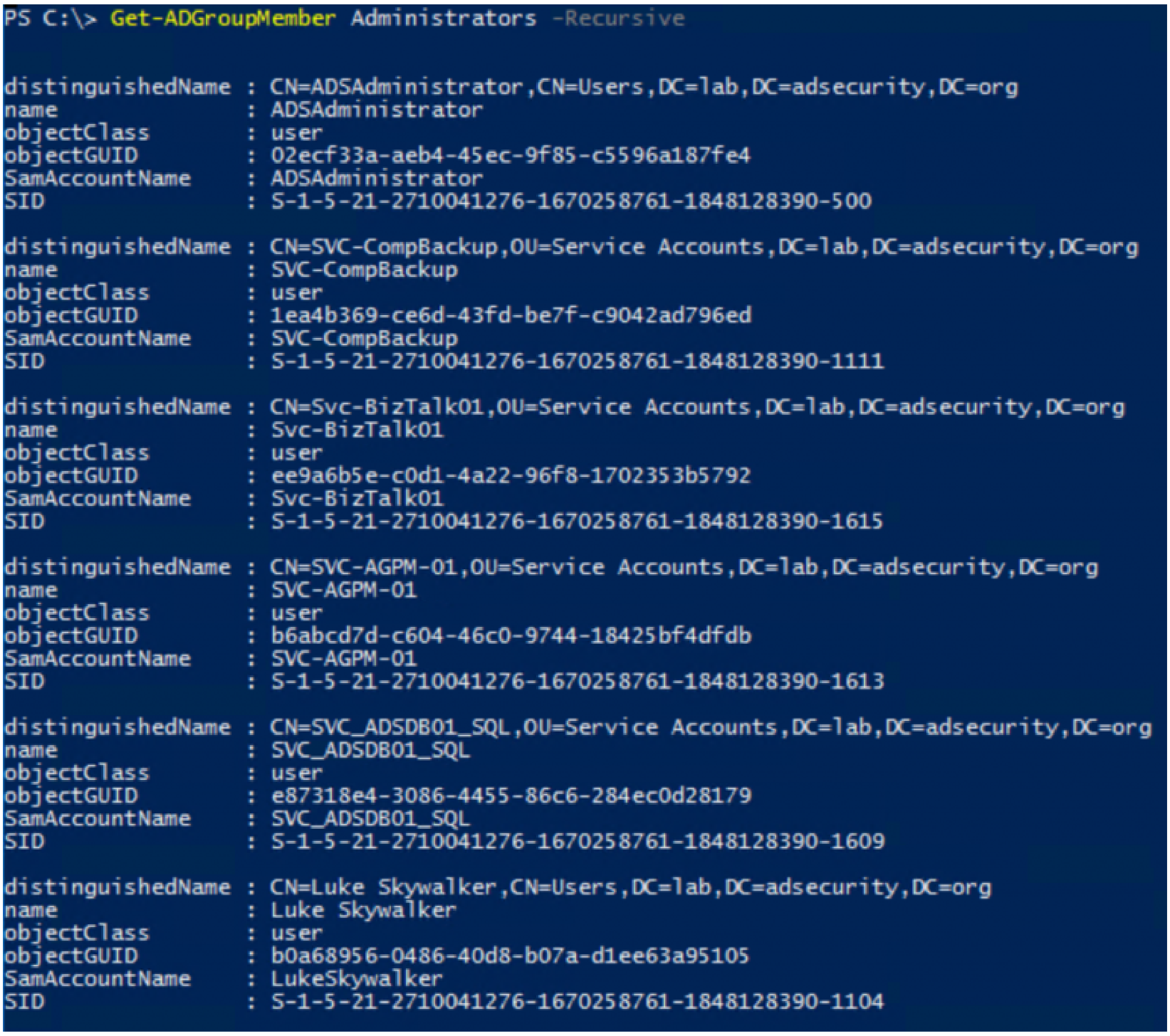
Sean Metcalf August 10, 2017

Active Directory has several levels of administration beyond the Domain Admins group. In a previous post, I explored: "Securing Domain Controllers to Improve Active Directory Security" which explores ways to better secure Domain Controllers and by extension, Active Directory. For more information on Active Directory specific rights and permission review my post "Scanning for Active Directory Privileges & Privileged Accounts."

This post provides information on how Active Directory is typically administered and the associated roles & rights.

- **Domain Admins** is the AD group that most people think of when discussing Active Directory administration. This group has full admin rights by default on all domain-joined servers and workstations, Domain Controllers, and Active Directory. It gains admin rights on domain-joined computers since when these systems are joined to AD, the Domain Admins group is added to the computer's Administrators group.
- **Enterprise Admins** is a group in the forest root domain that has full AD rights to every domain in the AD forest. It is granted this right through membership in the Administrators group in every domain in the forest.
- **Administrators** in the AD domain, is the group that has default admin rights to Active Directory and Domain Controllers and provides these rights to Domain Admins and Enterprise Admins, as well as any other members.
- **Schema Admins** is a group in the forest root domain that has the ability to modify the Active Directory forest schema.

Since the Administrators group is the domain group that provides full rights to AD and Domain Controllers, it's important to monitor this group's membership (including all nested groups). The Active Directory PowerShell cmdlet "Get-ADGroupMember" can provide group membership information.



```
PS C:\> Get-ADGroupMember Administrators -Recursive

distinguishedName : CN=ADSAdministrator,CN=Users,DC=lab,DC=adsecurity,DC=org
name              : ADSAdministrator
objectClass       : user
objectGUID        : 02ecf33a-aeb4-45ec-9f85-c5596a187fe4
SamAccountName    : ADSAdministrator
SID               : S-1-5-21-2710041276-1670258761-1848128390-500

distinguishedName : CN=SVC-CompBackup,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name              : SVC-CompBackup
objectClass       : user
objectGUID        : 1ea4b369-ce6d-43fd-be7f-c9042ad796ed
SamAccountName    : SVC-CompBackup
SID               : S-1-5-21-2710041276-1670258761-1848128390-1111

distinguishedName : CN=Svc-BizTalk01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name              : Svc-BizTalk01
objectClass       : user
objectGUID        : ee9a6b5e-c0d1-4a22-96f8-1702353b5792
SamAccountName    : Svc-BizTalk01
SID               : S-1-5-21-2710041276-1670258761-1848128390-1615

distinguishedName : CN=SVC-AGPM-01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name              : SVC-AGPM-01
objectClass       : user
objectGUID        : b6abcd7d-c604-46c0-9744-18425bf4dfdb
SamAccountName    : SVC-AGPM-01
SID               : S-1-5-21-2710041276-1670258761-1848128390-1613

distinguishedName : CN=SVC_ADSDB01_SQL,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name              : SVC_ADSDB01_SQL
objectClass       : user
objectGUID        : e87318e4-3086-4455-86c6-284ec0d28179
SamAccountName    : SVC_ADSDB01_SQL
SID               : S-1-5-21-2710041276-1670258761-1848128390-1609

distinguishedName : CN=Luke Skywalker,CN=Users,DC=lab,DC=adsecurity,DC=org
name              : Luke Skywalker
objectClass       : user
objectGUID        : b0a68956-0486-40d8-b07a-d1ee63a95105
SamAccountName    : LukeSkywalker
SID               : S-1-5-21-2710041276-1670258761-1848128390-1104
```

Default groups in Active Directory often have extensive rights – many more than typically required. For this reason, we don't recommend using these groups for delegation. Where possible, perform custom delegation to ensure the principle of least privilege is followed. The following groups should have a "DC" prefix added to them since the scope applies to Domain Controllers by default. Furthermore, they have elevated rights on Domain Controllers and should be considered effectively Domain Controller admins.

- **Backup Operators** is granted the ability to logon to, shut down, and perform backup/restore operations on Domain Controllers (assigned via the Default Domain Controllers Policy GPO). This group cannot directly modify AD admin groups, though associated privileges provides a path for escalation to AD admin. Backup Operators have the ability to schedule tasks which may provide an escalation path. They also are able to clear the event logs on Domain Controllers.
- **Print Operators** is granted the ability to manage printers and load/unload device drivers on Domain Controllers as well as manage printer objects in Active Directory. By default, this group can logon to Domain Controllers and shut them down. This group cannot directly modify AD admin groups.
- **Server Operators** is granted the ability to logon to, shut down, and perform backup/restore operations on Domain Controllers (assigned via the Default Domain Controllers Policy GPO). This group cannot directly modify AD admin groups, though associated privileges provides a path for escalation to AD admin.

To a lesser extend, we’ll group Remote Desktop Users into this category as well.

> **Remote Desktop Users** is a domain group designed to easily provide remote access to systems. In many AD domains, this group is added to the “Allow log on through Terminal Services” right in the Default Domain Controllers Policy GPO providing potential remote logon capability to DCs.

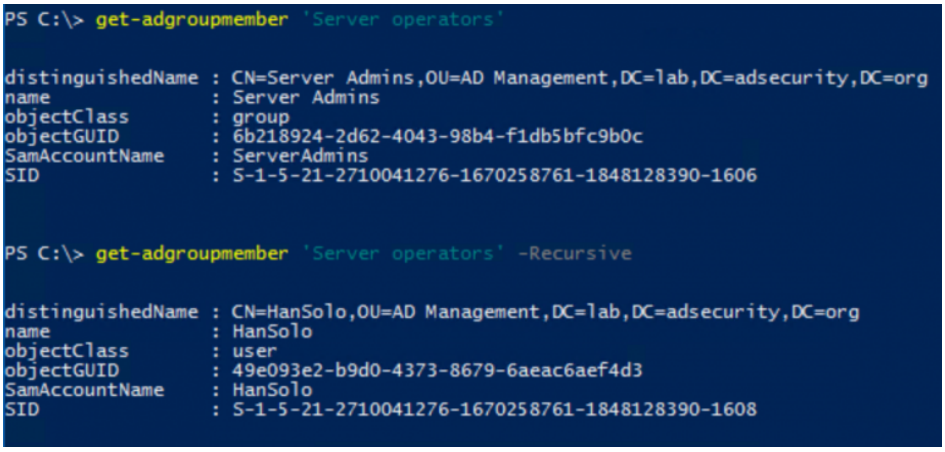
We also see that many times the following is configured via GPO linked to the Domain Controllers OU:

- **Remote Desktop Users**: often granted “Allow log on through Terminal Services” right via Group Policy linked to the Domain Controllers OU.
- **Server Operators**: granted “Allow log on through Terminal Services” right via Group Policy linked to the Domain Controllers OU.
- Server Operators: granted “Log on as a batch job” right via GPO providing the ability to schedule tasks.

Review the GPOs linked to the Domain and the Domain Controllers OU and ensure the GPO settings are appropriate.
We often find that a servers GPO is also linked to the Domain Controllers OU and it adds a “Server Admins” group to the local Administrators group. Since Domain Controllers don’t have a “local” Administrators group, the DC updates the domain Administrators group by adding Server Admins. *This scenario makes all members of Server Admins Active Directory admins.*

Any group/account granted logon locally rights to Domain Controllers should be scrutinized.

Server Operators & Backup Operators have elevated rights on Domain Controllers and should be monitored. The Active Directory PowerShell cmdlet “Get-ADGroupMember” can provide group membership information.



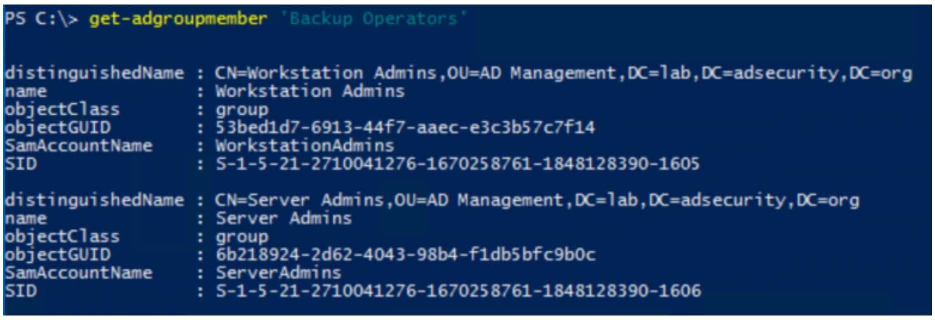
```
PS C:\> get-adgroupmember 'Server operators'


distinguishedName : CN=Server Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org
name              : Server Admins
objectClass       : group
objectGUID        : 6b218924-2d62-4043-98b4-f1db5bfc9b0c
SamAccountName    : ServerAdmins
SID               : S-1-5-21-2710041276-1670258761-1848128390-1606



PS C:\> get-adgroupmember 'Server operators' -Recursive


distinguishedName : CN=HanSolo,OU=AD Management,DC=lab,DC=adsecurity,DC=org
name              : HanSolo
objectClass       : user
objectGUID        : 49e093e2-b9d0-4373-8679-6aeac6aef4d3
SamAccountName    : HanSolo
SID               : S-1-5-21-2710041276-1670258761-1848128390-1608
```



```
PS C:\> get-adgroupmember 'Backup Operators'

distinguishedName : CN=Workstation Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org
name              : Workstation Admins
objectClass       : group
objectGUID        : 53bed1d7-6913-44f7-aaec-e3c3b57c7f14
SamAccountName    : WorkstationAdmins
SID               : S-1-5-21-2710041276-1670258761-1848128390-1605

distinguishedName : CN=Server Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org
name              : Server Admins
objectClass       : group
objectGUID        : 6b218924-2d62-4043-98b4-f1db5bfc9b0c
SamAccountName    : ServerAdmins
SID               : S-1-5-21-2710041276-1670258761-1848128390-1606
```

Other default groups with elevated rights:

- **Account Operators** has the rights to modify accounts and groups in the domain. Also has the ability to log on to Domain Controllers by default (assigned via the Default Domain Controllers Policy GPO). This group cannot directly modify AD admin groups, though associated privileges provides a path for escalation to AD admin.
- **DNSAdmins** has administrative access to Microsoft Active Directory DNS and is often granted the ability to logon to Domain Controllers.
  Note that by default, members of the DNSAdmins group are able to run a DLL on a Domain Controller which could provide privilege escalation to Domain Admin rights: https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83
- **Group Policy Creator Owners** can create, modify, and delete Group Policies in the domain.

Most of the rights granted to groups and accounts on Domain Controllers is applied by the "Default Domain Controllers Policy" Group Policy. These are typically defined in the User Rights Assignment section which we review when performing an Active Directory Security Assessment since it is often very enlightening as to who has rights to DCs. The settings in the Default Domain Controllers Policy have changed over the years from Windows 2000 to now. Note that if you promoted Active Directory with a Windows 2000 or 2003 server, this policy will still contain those original settings, even when running Windows Server 2016 (assuming no one changed the policy settings).

Sensitive Domain Controller User Rights Assignments:

- Allow log on locally
  > *This policy setting determines which users can start an interactive session on the computer. Users must have this user right to log on over a Remote Desktop Services or Terminal Services session that is running on a Windows-based member computer or domain controller.*
  > *Note:*
  > *Users who do not have this right are still able to start a remote interactive session on the computer if they have the Allow logon through Remote Desktop Services right.*

- Back-up files & directories

  This user right determines which users can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system. This user right is effective only when an application attempts access through the NTFS backup application programming interface (API) through a backup tool such as NTBACKUP.EXE. Otherwise, standard file and directory permissions apply.
  This user right is similar to granting the following permissions to the user or group you have selected on all files and folders on the system:
  Traverse Folder/Execute File
  List Folder/Read Data
  Read Attributes
  Read Extended Attributes
  Read Permissions
  Default on workstations and servers:
  Administrators
  Backup Operators
  Default on domain controllers:
  Administrators
  Backup Operators
  Server Operators

- Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)

  This policy setting determines which users can set the Trusted for Delegation setting on a user or computer object.Security account delegation provides the ability to connect to multiple servers, and each server change retains the authentication credentials of the original client. Delegation of authentication is a capability that client and server applications use when they have multiple tiers. It allows a public-facing service to use client credentials to authenticate to an application or database service. For this configuration to be possible, the client and the server must run under accounts that are trusted for delegation.Only administrators who have the Enable computer and user accounts to be trusted for delegation credential can set up delegation. Domain admins and Enterprise admins have this credential. The procedure to allow a user to be trusted for delegation depends on the functionality level of the domain.The user or computer object that is granted this right must have write access to the account control flags. A server process running on a computer (or under a user context) that is trusted for delegation can access resources on another computer by using the delegated credentials of a client. However, the client account must have Write access to the account control flags on the object.

- Force shutdown from a remote system

  This security setting determines which users are allowed to shut down a computer from a remote location on the network. This allows members of the Administrators group or specific users to manage computers (for tasks such as a restart) from a remote location.

- Log on as a batch job

  This policy setting determines which accounts can log on by using a batch-queue tool such as the Task Scheduler service. When an administrator uses the Add Scheduled Task Wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the Log on as a batch job user right. When the scheduled time arrives, the Task Scheduler service logs on the user as a batch job instead of as an interactive user, and the task runs in the user's security context.

- Log on as a service

  This policy setting determines which service accounts can register a process as a service. Running a process under a service account circumvents the need for human intervention.

- Manage auditing and security log

  Determines which users can specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys. A user with this right can use the security tab in the security permission set editor's Properties dialog box to specify auditing options for the selected object.
  This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.
  By default, only administrators have the privilege to manage auditing and the security log.
  Note:
  This policy does not allow a user to specify that file and object access auditing be enabled in general. In order for such auditing to take place, the Audit object access setting under Audit Policies must be configured.
  Audited events are viewed in the security log of the Event Viewer . ***A user with this policy can also view and clear the security log.***

- Restore files & directories

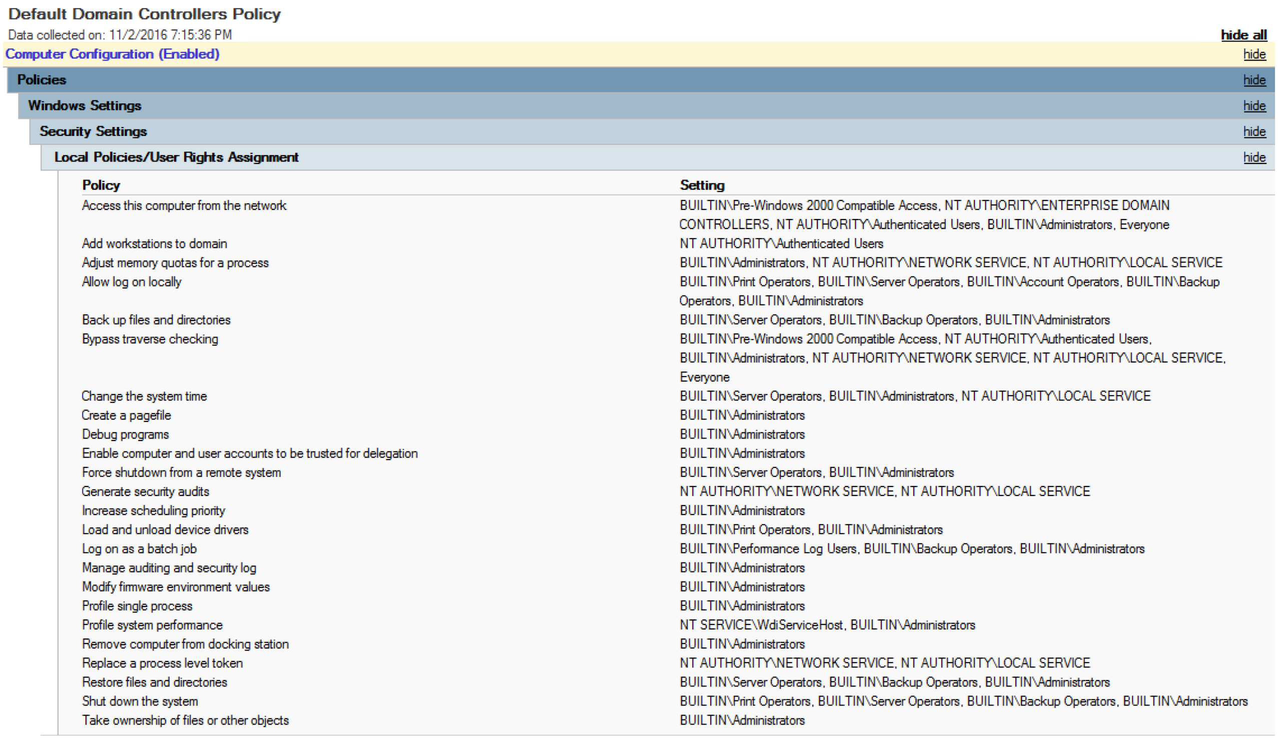
  This security setting determines which users can bypass file, directory, registry, and other persistent object permissions when they restore backed up files and directories, and it determines which users can set valid security principals as the owner of an object.
  Granting this user right to an account is similar to granting the account the following permissions to all files and folders on the system:
  Traverse folder / execute file
  Write

- Synchronize directory service data (SeSyncAgentPrivilege)
  - *Ensure that no accounts are assigned the Synchronize directory service data user right. Only domain controllers need this privilege, which they inherently have.*
  - *This policy setting determines which users and groups have authority to synchronize all directory service data, regardless of the protection for objects and properties. This privilege is required to use LDAP directory synchronization (dirsync) services. Domain controllers have this user right inherently because the synchronization process runs in the context of the System account on domain controllers.*
  - This policy when coupled with DS-Replication-Get-Changes-All likely grants the type of rights required to run Mimikatz DCSync which enables an attacker to request password hashes for all users in the domain.
- Take ownership of files or other objects (SeTakeOwnershipPrivilege)

  This policy setting determines which users can take ownership of any securable object in the device, including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes, and threads.
  *Every object has an owner, whether the object resides in an NTFS volume or **Active Directory database**. The owner controls how permissions are set on the object and to whom permissions are granted.*
  By default, the owner is the person who or the process which created the object. Owners can always change permissions to objects, even when they are denied all access to the object.

Note: Be very careful with providing the ability to logon locally and via Terminal Services to Domain Controllers since the ability to logon to a Domain Controller provides several potential escalation paths to AD administrator.

Default Domain Controllers Policy GPO (Windows Server 2012 R2)



Default Domain Controllers Policy

Data collected on: 11/2/2016 7:15:36 PM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdiServiceHost, BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Specific recommendations on how to improve the security of Domain Controllers by modifying this GPO is in the post "Securing Domain Controllers to Improve Active Directory Security."

Default Groups and the rights provided through the Default Domain Controllers Policy:

Note that the AD "Built-In" Administrators group is granted most rights.

Server Operators is provided the following rights through this GPO:

- Allow log on locally
- Back-up files & directories
- Force shutdown from a remote system
- Restore files & directories
- Shut down the system

Backup Operators is provided the following rights through this GPO:

- Allow log on locally
- Back-up files & directories
- Log on as a batch job
- Manage auditing and security log
- Restore files & directories
- Shut down the system

Print Operators is provided the following rights through this GPO:

- Allow log on locally
- Load and unload device drivers

- Shut down the system

I hope this post helps people better understand the default rights that builtin AD groups have on Domain Controllers.

(Visited 83,527 times, 8 visits today)