Active Directory 具有 Domain Admins 组之外的多个管理级别。
本文描述有关如何管理 Active Directory 以及相关角色和权限的信息（主要是一些常见的和攻击当中经常提到的权限）。

Domain Admins 是大多数人在讨论 Active Directory 管理时所考虑的 AD 组。默认情况下这个组对所有加入域的服务器和工作站、域控制器和 Active Directory 上具有完全管理权限。

Enterprise Admins 是林根域的一个组，对 AD 林中的每个域都具有完全的 AD 权限，通过林中每个域中的 Administrators 组的成员身份授予此权限。

Administrators 在 AD 域，是对 Active Directory 和域控制器具有默认的管理员权限的一个组，并提供了这些权利给 Domain Admins 和 Enterprise Admins 以及任何其他成员的组。

Schema Admins 是林根域中的一个组，可以修改 Active Directory 林模式。

由于 Administrators 组是为 AD 和域控制器提供完全权限的域组，因此监视此组的成员身份（包括所有嵌套组）非常重要。Active Directory PowerShell cmdlet "Get-ADGroupMember" 可以提供组成员身份信息。

```
PS C:\Users\Administrator\Desktop> Get-ADGroupMember

位于命令管道位置 1 的 cmdlet Get-ADGroupMember
请为以下参数提供值:
(请键入 !? 以查看帮助。)
Identity: Administrators


distinguishedName : CN=Domain Admins,CN=Users,DC=yunying,DC=lab
name              : Domain Admins
objectClass       : group
objectGUID        : 03ee27fb-ff46-4ab6-bd2f-ce6a269bcfd6
SamAccountName    : Domain Admins
SID               : S-1-5-21-4054579877-26337388-655639334-512

distinguishedName : CN=Enterprise Admins,CN=Users,DC=yunying,DC=lab
name              : Enterprise Admins
objectClass       : group
objectGUID        : eecb5035-28dc-4513-b32a-c8d7bc2f4752
SamAccountName    : Enterprise Admins
SID               : S-1-5-21-4054579877-26337388-655639334-519

distinguishedName : CN=Administrator,CN=Users,DC=yunying,DC=lab
name              : Administrator
objectClass       : user
objectGUID        : a5fd57d0-9761-4692-8378-e38e10a6d96b
SamAccountName    : Administrator
SID               : S-1-5-21-4054579877-26337388-655639334-500



PS C:\Users\Administrator\Desktop>
```

Active Directory 中的默认组通常具有广泛的权限 - 比通常所需的权限要多得多。因此，我们不建议使用这些组进行委派。
在可能的情况下，执行自定义委派以确保遵循最小权限原则。以下组应添加"DC"前缀，因为默认情况下范围适用于域控制器。此外，他们在域控制器上拥有更高的权限，应该被视为域控制器管理员。

Backup Operators 被授予在域控制器上登录，关闭和执行备份/恢复操作的功能（通过默认域控制器策略 GPO 分配）。虽然关联权限提供了升级到 AD 管理员的路径，但该组无法直接修改 AD 管理员组。备份操作员可以安排可能提供升级路径的任务。他们还能够清除域控制器上的事件日志。

Print Operators 被授予管理打印机和在域控制器上加载/卸载设备驱动程序以及管理 Active Directory 中的打印机对象的功能。默认情况下，该组可以登录到域控制器并将其关闭。该组无法直接修改 AD 管理员组。

Server Operators 被授予在域控制器上登录，关闭和执行备份/恢复操作的功能（通过默认域控制器策略 GPO 分配）。虽然关联权限提供了升级到 AD 管理员的路径，但该组无法直接修改 AD 管理员组。

Remote Desktop Users 是一个域组，旨在轻松提供对系统的远程访问。在许多 AD 域中，此组将添加到默认域控制器策略 GPO 中的“允许通过终端服务登录”权限，为 DC 提供潜在的远程登录功能。

还有几个重要的权限：

Replicating Directory Changes All（复制目录更改所有）

这个权限可以进行 DCsync 的操作从而导出域内所有的账号以及密码 HASH 值。

FIM, Riverbed, SharePoint 等应用默认有这样的服务账户可以在域控权限下授予这样的权限，其中 Exchange 就是一个例子。

DS-Replication-Get-Changes（复制目录更改）

创建或删除子项，删除子树，读取和写入属性，检查子项和对象本身，从目录添加和删除对象以及使用扩展权限读取或写入的权限。它提供对象和所有属性的完全权限，包括机密属性（如 LAPS 本地管理员密码和 BitLocker 恢复密钥）。在许多情况下，不需要完全控制权限，但是比确定所需的实际权限更容易委派和工作。

GenericAll：GenericAll =完全控制

创建或删除子项，删除子树，读取和写入属性，检查子项和对象本身，从目录添加和删除对象以及使用扩展权限读取或写入的权限。

它提供对象和所有属性的完全权限，包括机密属性（如 LAPS 本地管理员密码和 BitLocker 恢复密钥）。在许多情况下，不需要完全控制权限，但是比确定所需的实际权限更容易委派和工作。

示例：可以在 OU 中具有与服务器关联的计算机对象的所有计算机对象上委派服务器层组。另一种常见配置是为桌面支持组的工作站 OU 中的所有计算机对象委派“完全控制”，并为“帮助台”的“用户 OU”中的所有用户对象委派“完全控制”。

GenericWrite：

提供对所有属性的写访问权限。

有权读取此对象的权限，写入此对象的所有属性，并对此对象执行所有经过验证的写入。

WriteDACL：提供修改对象安全性的功能，可以导致对象的完全控制。

修改对象安全描述符中的 DACL 的权限。

示例：可以授予服务帐户在 AD 中执行委派的权限。如果攻击者可以猜出这个密码（或者可能通过 Kerberoasting 破解它），他们现在可以在相关对象上设置自己的权限，这可能导致对

象的完全控制，这可能涉及暴露 LAPS 控制的本地管理员密码。