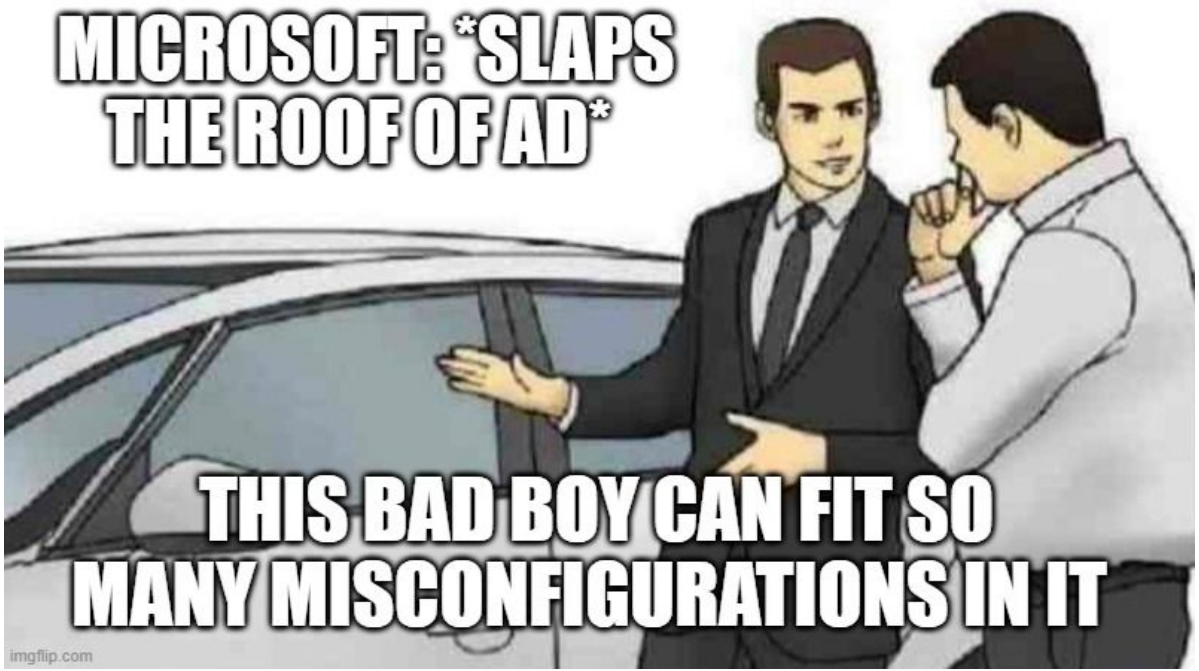
Practical Insights into AD Tiering

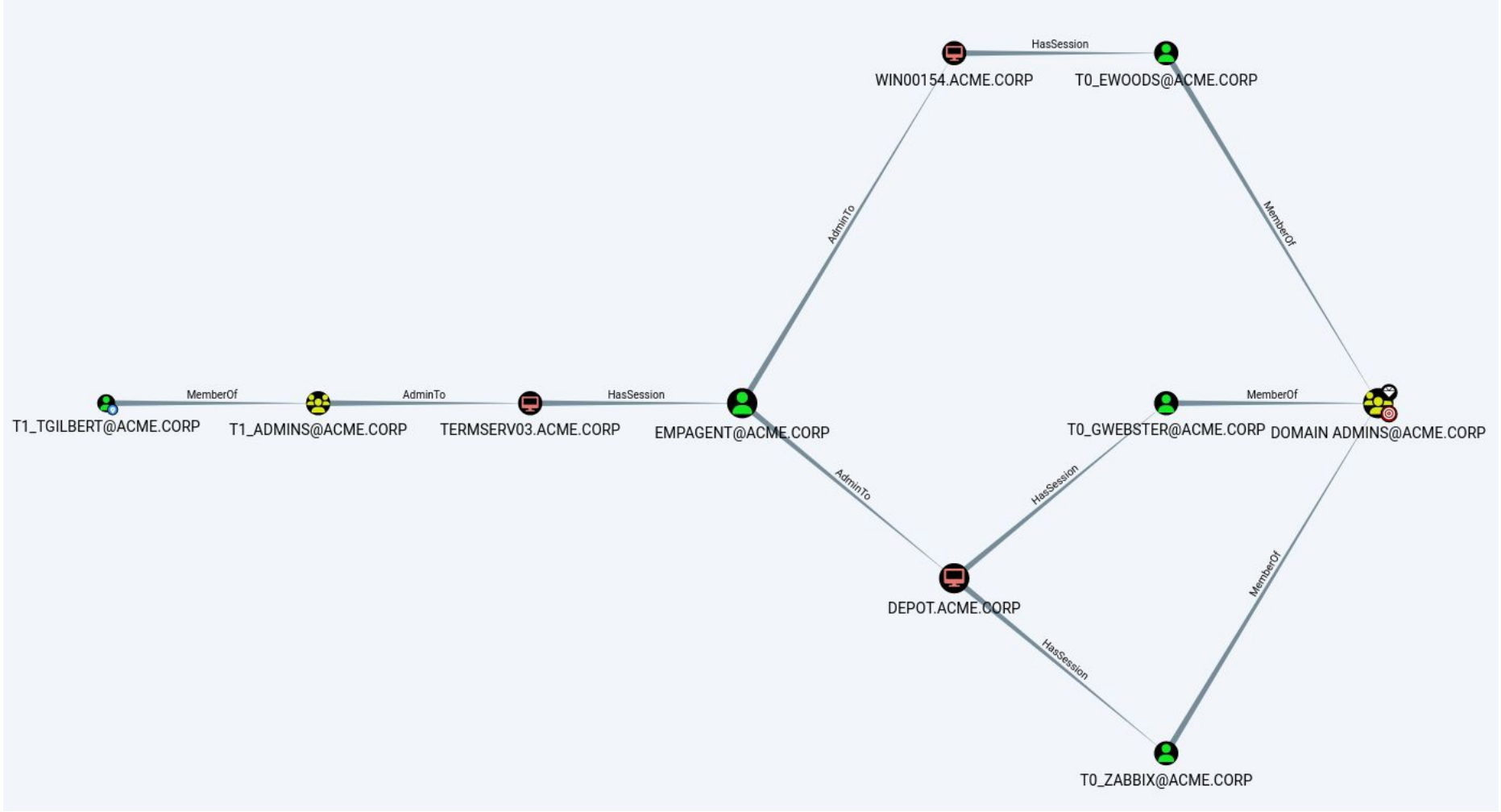
Why we like tiering

Limit credential exposure

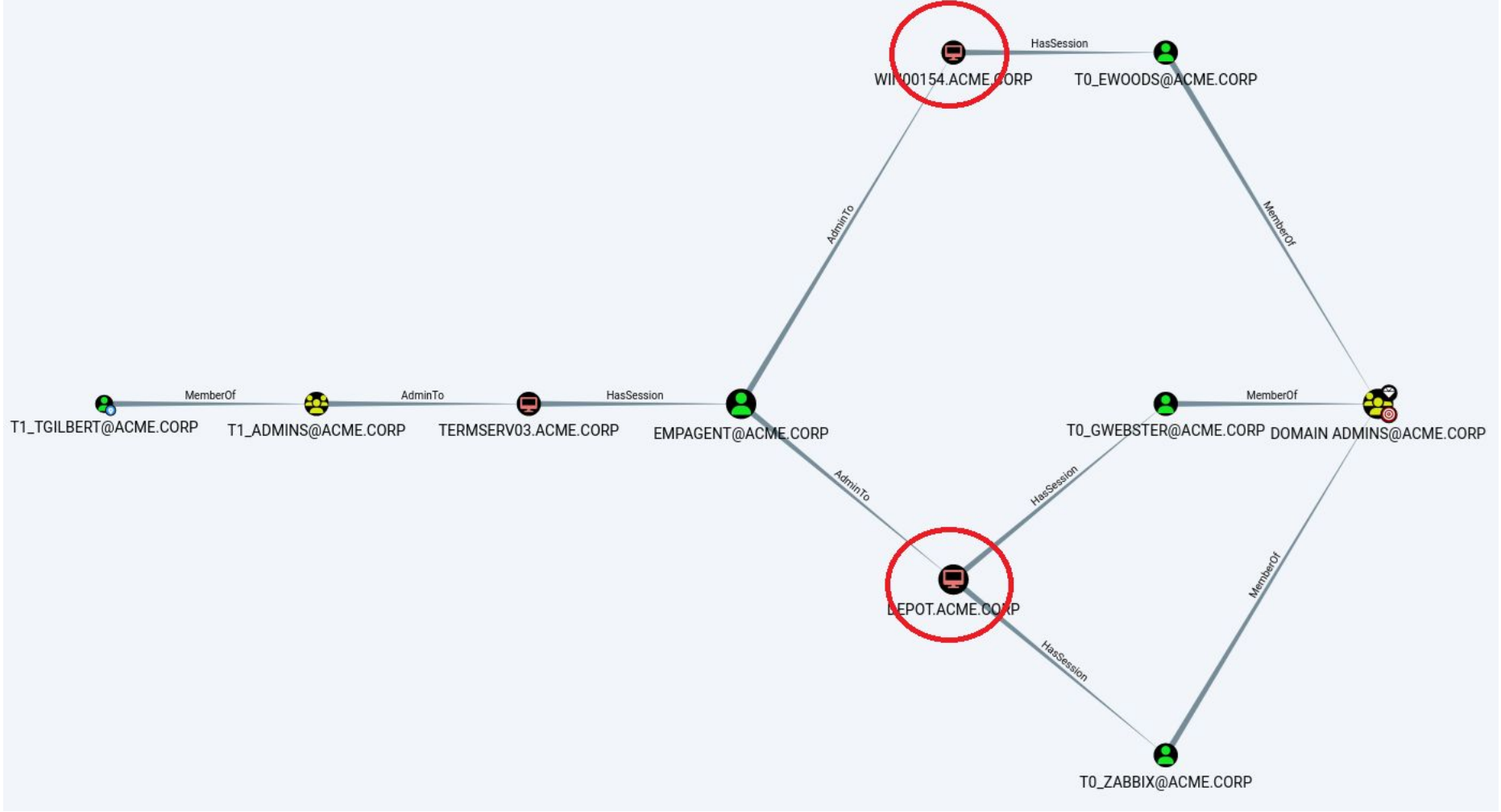
Limit lateral movement

Clean up





Borrowed from blog.syss.com



Borrowed from blog.syss.com

The rules

1. Credentials from a higher tier must not be exposed to a lower tier system

2. Lower tier systems can use services provided by higher tiers (GPO, file server…)

3. Any object that can manage a higher tier is a member of the higher tier

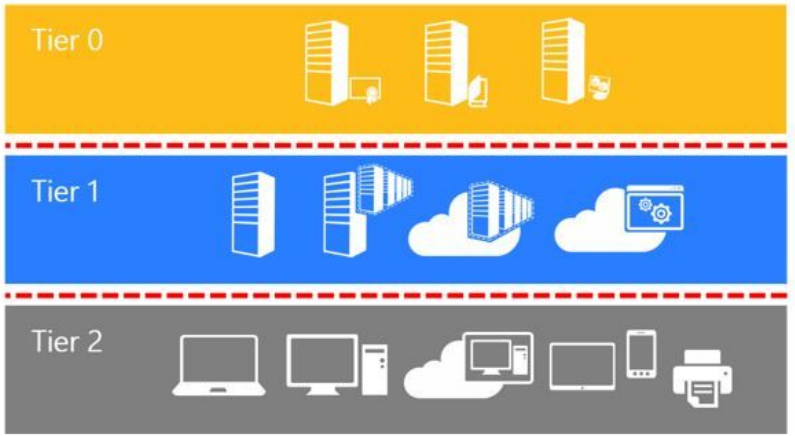
Classify AD objects

What tiers do objects belong to?

Tier 0 - Everything that can take control of the domain

Tier 1 - The servers that cannot take control of the domain and the associated users and groups

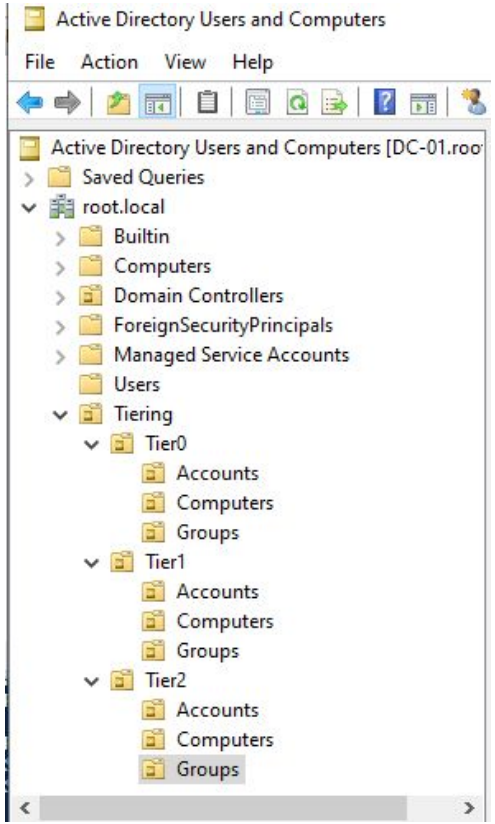
Tier 2 - The workstations and associated users and groups



https://specterops.github.io/TierZeroTable/

Name	Type	IdP	Identification	Description	Compromise by default	Compromise by configuration	Is Tier Zero
Account Operators	DC group	Active Directory	SID: S-1-5-32-548	The Account Operators group	YES - Takeover	N/A - Compromise by	YES
Administrator	AD user	Active Directory	SID: S-1-5-21-<domain>-500	The Administrator	YES - Takeover	N/A - Compromise by	YES
Administrators	DC group	Active Directory	SID: S-1-5-32-544	Members of the Administrators	YES - Takeover	N/A - Compromise by	YES
AdminSDHolder	AD container	Active Directory	DistinguishedName:	The purpose of the	YES - Takeover	N/A - Compromise by	YES
Allowed RODC Password	AD group	Active Directory	SID: S-1-5-21-<domain>-571	The purpose of this security	NO	YES - Takeover	NO
Application Administrator	Entra ID role	Entra ID	Template ID: 9b895d92-	This is a privileged role.	NO	YES - Takeover	IT DEPENDS
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551	Members of the Backup	YES - Takeover	N/A - Compromise by	YES
Cryptographic Operators	DC group	Active Directory	SID: S-1-5-32-569	Members of this group are	NO	NO	YES
Denied RODC Password	AD group	Active Directory	SID: S-1-5-21-<domain>-572	Passwords of members of the	NO	YES - Takeover	NO
Distributed COM Users	DC group	Active Directory	SID: S-1-5-32-562	Members of the Distributed COM	YES - Takeover	N/A - Compromise by	YES

Make a tiering OU structure



Move everything

Move users, groups and computers (if we dare)

Move ACLs or break inheriting (if we dare)

What information do we need

ACL in AD

On servers we need:

- User rights assignments
- Members of the local administrators group
- Members of the local remote desktop users group
- Basically everyone with a permission to logon

How to get user rights

PowerShell

Get-UserRights.ps1

```
"Privilege","PrivilegeName","Principal","ComputerName"
"SeAssignPrimaryTokenPrivilege","Replace a process level token","NT AUTHORITY\NETWORK SERVICE","DC-01"
"SeAssignPrimaryTokenPrivilege","Replace a process level token","NT AUTHORITY\LOCAL SERVICE","DC-01"
"SeCreateSymbolicLinkPrivilege","Create symbolic links","BUILTIN\Administrators","DC-01"
"SeDebugPrivilege","Debug programs","BUILTIN\Administrators","DC-01"
"SeDelegateSessionUserImpersonatePrivilege","Obtain an impersonation token for another user in the same session","BUILTI
"SeEnableDelegationPrivilege","Enable computer and user accounts to be trusted for delegation","BUILTIN\Administrators",
"SeImpersonatePrivilege","Impersonate a client after authentication","NT AUTHORITY\LOCAL SERVICE","DC-01"
"SeImpersonatePrivilege","Impersonate a client after authentication","NT AUTHORITY\NETWORK SERVICE","DC-01"
"SeImpersonatePrivilege","Impersonate a client after authentication","BUILTIN\Administrators","DC-01"
"SeImpersonatePrivilege","Impersonate a client after authentication","NT AUTHORITY\SERVICE","DC-01"
"SeIncreaseBasePriorityPrivilege","Increase scheduling priority","BUILTIN\Administrators","DC-01"
"SeIncreaseBasePriorityPrivilege","Increase scheduling priority","Window Manager\Window Manager Group","DC-01"
"SeIncreaseQuotaPrivilege","Adjust memory quotas for a process","NT AUTHORITY\LOCAL SERVICE","DC-01"
"SeIncreaseQuotaPrivilege","Adjust memory quotas for a process","NT AUTHORITY\NETWORK SERVICE","DC-01"
"SeIncreaseQuotaPrivilege","Adjust memory quotas for a process","BUILTIN\Administrators","DC-01"
"SeIncreaseWorkingSetPrivilege","Increase a process working set","BUILTIN\Users","DC-01"
"SeInteractiveLogonRight","Allow log on locally","NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS","DC-01"
"SeInteractiveLogonRight","Allow log on locally","BUILTIN\Backup Operators","DC-01"
"SeInteractiveLogonRight","Allow log on locally","BUILTIN\Print Operators","DC-01"
"SeInteractiveLogonRight","Allow log on locally","BUILTIN\Account Operators","DC-01"
"SeInteractiveLogonRight","Allow log on locally","BUILTIN\Administrators","DC-01"
"SeInteractiveLogonRight","Allow log on locally","BUILTIN\Server Operators","DC-01"
"SeLoadDriverPrivilege","Load and unload device drivers","BUILTIN\Print Operators","DC-01"
"SeLoadDriverPrivilege","Load and unload device drivers","BUILTIN\Administrators","DC-01"
"SeMachineAccountPrivilege","Add workstations to domain","NT AUTHORITY\Authenticated Users","DC-01"
"SeManageVolumePrivilege","Perform volume maintenance tasks","BUILTIN\Administrators","DC-01"
"SeNetworkLogonRight","Access this computer from the network","NT AUTHORITY\Authenticated Users","DC-01"
"SeNetworkLogonRight","Access this computer from the network","BUILTIN\Administrators","DC-01"
"SeNetworkLogonRight","Access this computer from the network","BUILTIN\Pre-Windows 2000 Compatible Access","DC-01"
"SeNetworkLogonRight","Access this computer from the network","NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS","DC-01"
"SeNetworkLogonRight","Access this computer from the network","Everyone","DC-01"
```

How to get local users and groups

PowerShell. Or if a tool is bought that can see this, then use that.

Get-LocalGroupMembership.ps1

```
GroupName,MemberName,MemberType,ComputerName
"Administrators","LOCAL\Administrator","User","File-01"
"Administrators","ROOT\ServiceAccount","User","File-01"
"Remote Desktop Users","ROOT\Benny","User","File-01"
"Remote Desktop Users","LOCAL\RemoteUser1","User","File-01"
```

How to get batch job service details

PowerShell

Get-LocalBatchAndServiceDetails.ps1

How to run the scripts

Put scripts in sysvol/fileshare and push it out

WinRM

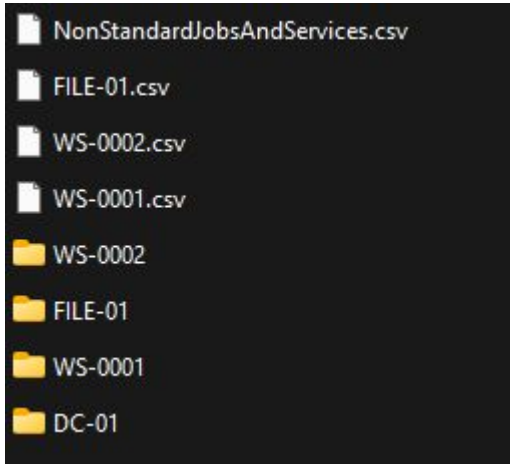
GPO

SCCM

PsExec

Analyse the data

AggregateData.ps1




```
"ComputerName","UserRightAssignment","User","GroupName","JobName","JobType",
"File-01","","LOCAL\Administrator","Administrators","","","","",""
"File-01","","ROOT\ServiceAccount","Administrators","","","","",""
"File-01","","ROOT\Benny","Remote Desktop Users","","","","",""
"File-01","","LOCAL\RemoteUser1","Remote Desktop Users","","","","",""
"File-01","","RetiredGuysAccount","","DoCriticalStuff","Batch","07-11-2005 1
"File-01","",".\administrator","","ImportantService","Service","","",""
"WS-0001","","LOCAL\Administrator","Administrators","","","","",""
"WS-0001","","ROOT\Johnny","Administrators","","","","",""
"WS-0001","","ROOT\Benny","Administrators","","","","",""
"WS-0001","","ROOT\Jenny","Administrators","","","","",""
"WS-0001","","LOCAL\RemoteUser1","Remote Desktop Users","","","","",""
"WS-0002","","LOCAL\Administrator","Administrators","","","","",""
"WS-0002","","ROOT\Johnny","Remote Desktop Users","","","","",""
"WS-0002","","LOCAL\RemoteUser1","Remote Desktop Users","","","","",""
"DC-01","SeInteractiveLogonRight","Jenny","","","","","",""
"DC-01","SeRemoteInteractiveLogonRight","Benny","","","","","",""
"DC-01","SeRemoteInteractiveLogonRight","Johnny","","","","","",""
```

ComputerName	UserRightAssignment	User	GroupName	JobName	JobType	LastRun	Created	CreatedBy
File-01		.\administrator		ImportantService	Service			
DC-01	SeRemoteInteractiveLogonRight	Benny						
DC-01	SeNetworkLogonRight	Benny						
DC-01	SeServiceLogonRight	Benny						
DC-01	SeDenyInteractiveLogonRight	Benny						
DC-01	SeDenyBatchLogonRight	Benny						
DC-01	SeAllowLogOnLocally	Benny						
File-01	SeNetworkLogonRight	Jimmy						
File-01	SeDenyNetworkLogonRight	Jimmy						
File-01	SeDenyBatchLogonRight	Jimmy						
DC-01	SeNetworkLogonRight	Consultant-Brian						
DC-01	SeBatchLogonRight	Consultant-Brian						
DC-01	SeServiceLogonRight	Consultant-Brian						
DC-01	SeDenyNetworkLogonRight	Consultant-Brian						
File-01	SeInteractiveLogonRight	Consultant-Brian						
File-01	SeRemoteInteractiveLogonRight	Consultant-Brian						
File-01	SeNetworkLogonRight	Consultant-Brian						
File-01	SeBatchLogonRight	Consultant-Brian						
File-01	SeServiceLogonRight	Consultant-Brian						
WS-0001	SeInteractiveLogonRight	Consultant-Brian						
WS-0001	SeBatchLogonRight	Consultant-Brian						
WS-0001	SeServiceLogonRight	Consultant-Brian						
WS-0001	SeDenyInteractiveLogonRight	Consultant-Brian						
WS-0001	SeDenyNetworkLogonRight	Consultant-Brian						
WS-0001	SeDenyBatchLogonRight	Consultant-Brian						
WS-0001	SeDenyServiceLogonRight	Consultant-Brian						
WS-0002	SeDenyBatchLogonRight	Consultant-Brian						
WS-0002	SeAllowLogOnLocally	Consultant-Brian						

WS-0001	SeRemoteInteractiveLogonRight	Johnny						
WS-0001	SeServiceLogonRight	Johnny						
WS-0001	SeDenyNetworkLogonRight	Johnny						
WS-0001	SeAllowLogOnLocally	Johnny						
WS-0002	SeBatchLogonRight	Johnny						
WS-0002	SeDenyInteractiveLogonRight	Johnny						
WS-0002	SeDenyNetworkLogonRight	Johnny						
WS-0002	SeDenyBatchLogonRight	Johnny						
WS-0002	SeDenyServiceLogonRight	Johnny						
WS-0002	SeAllowLogOnLocally	Johnny						
File-01		LOCAL\Administrator	Administrators					
WS-0001		RetiredGuysAccount	Administrators					
WS-0002		LOCAL\Administrator	Administrators					
File-01		LOCAL\RemoteUser1	Remote Desktop Users					
WS-0001		LOCAL\RemoteUser1	Remote Desktop Users					
WS-0002		LOCAL\RemoteUser1	Remote Desktop Users					
File-01		RetiredGuysAccount		DoCriticalStuff	Batch	07-11-2005 13:50:50		RetiredGuysAccount
File-01		ROOT\Benny	Remote Desktop Users					
WS-0001		ROOT\Benny	Administrators					
WS-0001		ROOT\Jenny	Administrators					
WS-0001		ROOT\Johnny	Administrators					
WS-0002		ROOT\Johnny	Remote Desktop Users					
File-01		ROOT\ServiceAccount	Administrators					

Next step?

Create users

Create groups

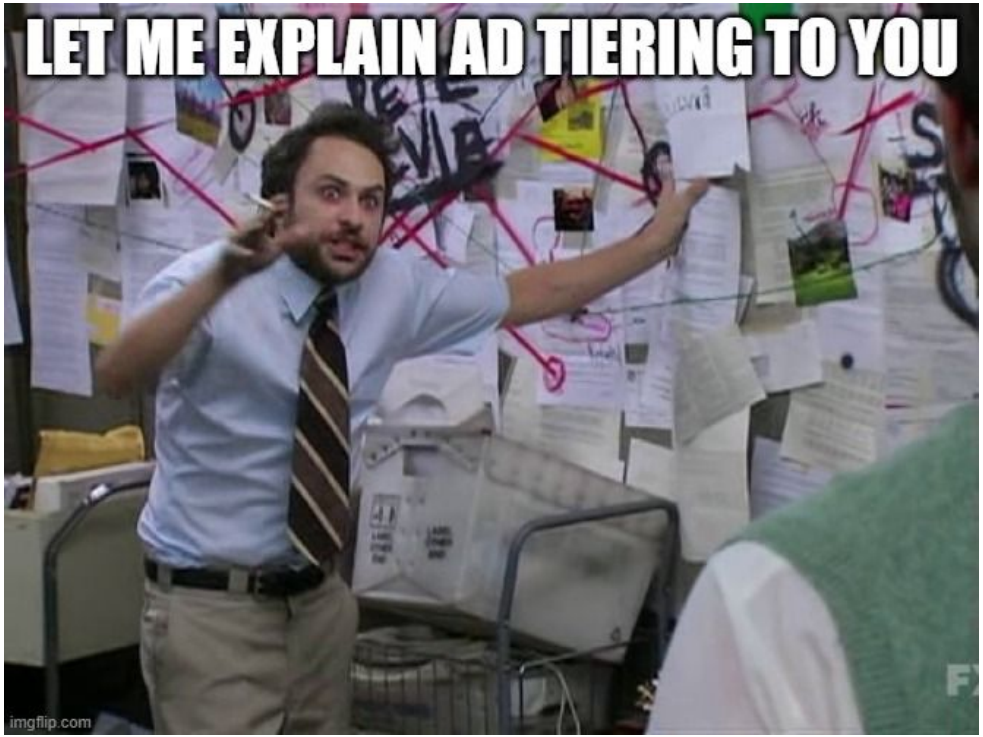
Assign access

The different ways of doing it

Allow model

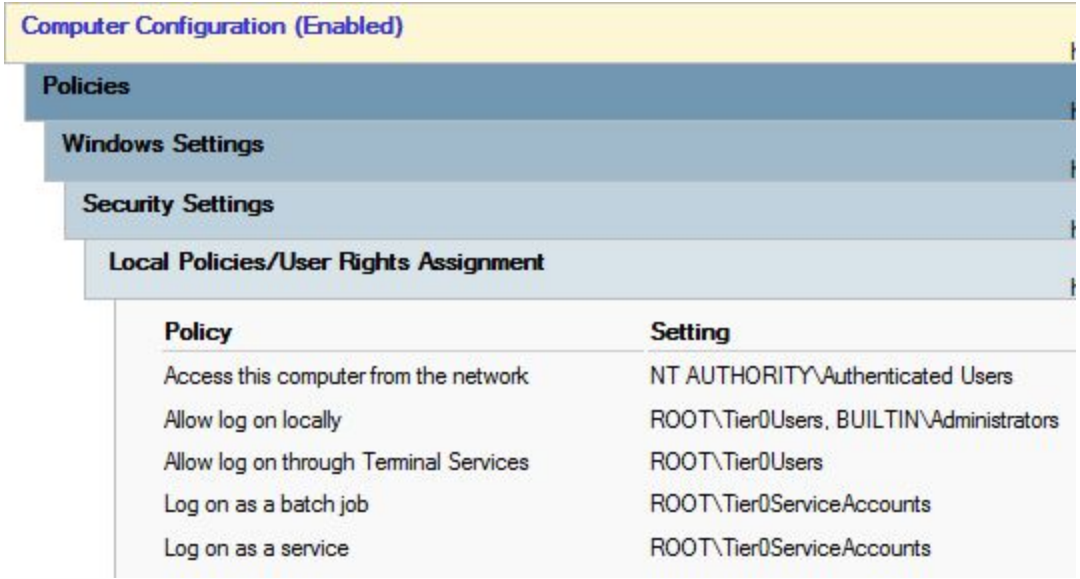
Block model

Allow and block



Create and apply GPOs

Allow



Deny

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Deny log on as a batch job	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0Users
Deny log on as a service	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0Users
Deny log on locally	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0ServiceAccounts
Deny log on through Terminal Services	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0ServiceAccounts

Allow and deny

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	NT AUTHORITY\Authenticated Users
Allow log on locally	ROOT\Tier0Users, BUILTIN\Administrator
Allow log on through Terminal Services	ROOT\Tier0Users
Deny log on as a batch job	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0Users
Deny log on as a service	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0Users
Deny log on locally	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0ServiceAccounts
Deny log on through Terminal Services	ROOT\Tier2Users, ROOT\Tier2ServiceAccounts, ROOT\Tier1Users, ROOT\Tier1ServiceAccounts, ROOT\Tier0ServiceAccounts
Log on as a batch job	ROOT\Tier0ServiceAccounts
Log on as a service	ROOT\Tier0ServiceAccounts

GPO tattooing

Find any potential GPO conflict

Run Get-GPOConflicts.ps1

```
Policy: OldGPO includes restriction: SeServiceLogonRight
Policy: OldGPO includes restriction: SeDenyBatchLogonRight
Policy: OldGPO includes restriction: SeDenyServiceLogonRight
Policy: ForgottenGPO includes restriction: SeRemoteInteractiveLogonRight
Policy: Default Domain Controllers Policy includes restriction: SeInteractiveLogonRight
Policy: Default Domain Controllers Policy includes restriction: SeNetworkLogonRight
Policy: Default Domain Controllers Policy includes restriction: SeBatchLogonRight
```

Maintain tiering

Lots of automation and/or alarms and lots of powershell

It all depends of how each AD is setup

Things to look for:

1. Users in no tiering group at all. Only BTG accounts should be outside tiering
2. Users in more than one tiering groups
3. Computers outside where the GPOs are applied

Adalanche, BloodHound or Forestdruid for analysis.