- **Active Directory Security Assessment - ADSA**

Active Directory

Author	Huy Kha
Contact	Huy_Kha@outlook.com

- **Summary**

Active Directory is the backbone of identities for many organizations around the world, but it is often not managed well, which open the doors for attackers to compromise it in a minute or two.

It is very expensive to recover an AD, so security needs to be enforced. ADSA contains different technical security controls and procedures to protect AD on a better state. The goal of ADSA is to help your team working together to improve the security posture of AD without pitching a third-party vendor or trying to sell you a security product.

Enjoy!

Foreword

Microsoft provides Active Directory Security Assessments for their customers, which is great, but unfortunately not everyone has the money nor the people to do these kind of Security Assessment, and since AD is the backbone of identities for many organizations. It is crucial to protect it, right?

Despite that, I wanted to purely focus on something else than AD. I started to release something similar as ADSA, but a bit of my own version, which does not mean, that you would immediately be 100% secure if you follow all of these recommendations. The goal of ADSA is to improve the security posture of AD and slow down an attacker, while trying to ensure that the recommendations will not break any stuff in production.

Different examples from real world experience has been covered, where I have managed to see these misconfigurations in production environments.

Introduction

Backups

1.1) Domain Controllers
1.2) DHCP
1.3) DNS
1.4) PKI

Domain Controllers

2.1) Hardening settings
2.2) Disabling unnecessary services
2.3) Auditing last back-up of the DC
2.4) Restore plan
2.5) Procedure for rotating the password of the KRBTGT account
2.6) Procedure for managing the password of the DSRM account
2.7) Improve auditing rules
2.8) Securing Built-in\Administrator account

Access Control List

3.1) Running periodically ACL scans
3.2) Control ACLs that has been set on the OU of the Domain Controllers
3.3) Control ACLs that has been set on the DC computer objects
3.4) Control ACLs that has been set on all Domain Admins and equivalent users
3.5) Control ACLs that has been set on groups like Domain Admins, Enterprise Admins, Administrators and equivalent with the likes of the ''Operators'' group
3.6) Control ACLs that has been set on the DNS Object
3.7) Control ACLs that has been set on GPO's that are linked to the DC
3.8) Control ACLs that has been set on the Domain Object
3.9) Run BloodHound to find more escalation paths

Best practices

4.1) Enabling Active Directory Recycle Bin
4.2) Delegating rights to restore (deleted) objects out of Recycle Bin
4.3) Do not use the following groups: Account Operators, Server Operators and Print Operators, but delegated the rights.
4.4) Enabling SID Filtering
4.5) Remove sIDHistory after migration
4.6) Tier 0 admins need to be a member of the Protected Users, group
4.7) Tier 0 admins need to have the ''Account is sensitive and cannot be delegated'' checkmark.

- **DNS**

5.1) Backup and restore plan for DNS
5.2) DnsAdmins

- **DHCP**

6.1) Backup and restore plan for DHCP

- **PKI**

7.1) Backup and restore plan for PKI
7.2) Enable auditing rules
7.3) Monitor relevant PKI event logs
7.4) Hardening settings for PKI

- **Password Policies**

8.1) Fine-Grained Password Policies for service accounts
8.2) Fine-Grained Password Policies for IT Admins
8.3) Upgrade Default Password Policy in AD

- **Weak or insecure configurations**

9.1) Accounts with SPN's in high-privileged group
9.2) Pre-authentication disabled on accounts
9.3) Servers with Unconstrained Kerberos Delegation

- **Security Check**

10.1) Ensure AdminSDHolder is in clean state
10.2) Create honey user to detect Kerberoast
10.3) Monitor high-privileged groups
10.4) Event Logs to monitor

- **MSFT Administrative Tier Model**

11.1) Deploy a Microsoft Administrative Tier Model or a similar model
11.2) Define which assets needs to be managed from a Tier 0
11.3) Best practices for managing GPO's in a Tier model.

- 1.1 – Backups of Domain Controllers

Task	Tier 0 admins
Permission Required	Domain Admins or equivalent.
Least-Privilege	Backup Operators

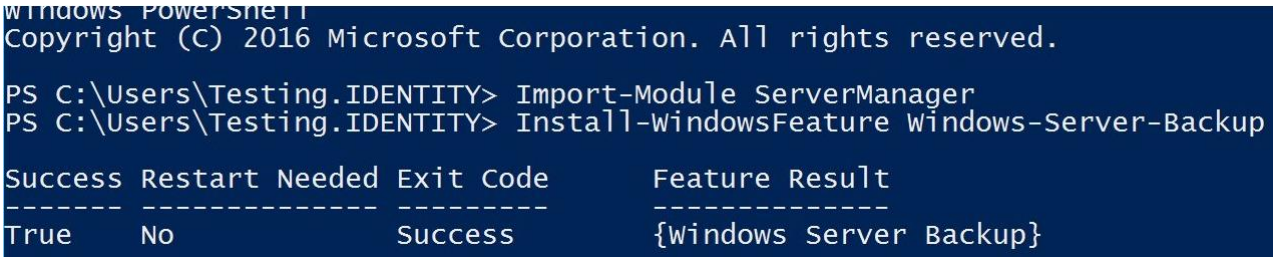
- **Summary**

Making back-ups of Domain Controllers is a crucial part of every organization, because Domain Controllers are responsible for handling authentication in a network. A DC authenticates users, it stores all the credentials of users in a DIT file, and it enforces a security policy for a Windows domain. A DC is like the keys to the kingdom of an organization, and it needs to be secure on a high level. Since Domain Controllers are so crucial. It is critical to make back-ups and store them securely.

There are different solutions in the market to make back-ups of Domain Controllers, but since the purpose of ADSA is not to pitch a vendor. We will use standard features that are available in Active Directory, which is in this case. **Windows Server Backup**.

- Log on the DC and make sure Windows Server Backup is installed.
- Run PowerShell with elevated rights

```
Import-Module ServerManager
Install-WindowsFeature Windows-Server-Backup
```



- Check if Windows Server Backup is installed

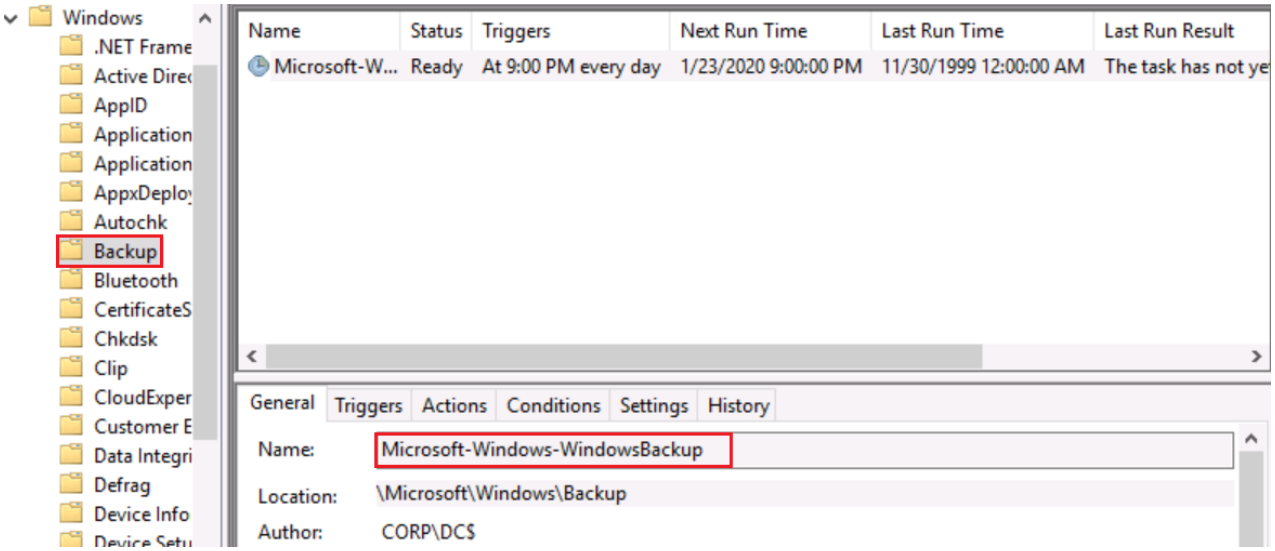
```
Get-WindowsFeature | where {$_.Name -eq "Windows-Server-Backup"}
```

```
PS C:\Users\Testing.IDENTITY> Get-WindowsFeature | where {$_.Name -eq "Windows-Server-Backup"}

Display Name                                            Name                        Install State
------------                                            ----                        -------------
[X] Windows Server Backup                               Windows-Server-Backup           Installed
```

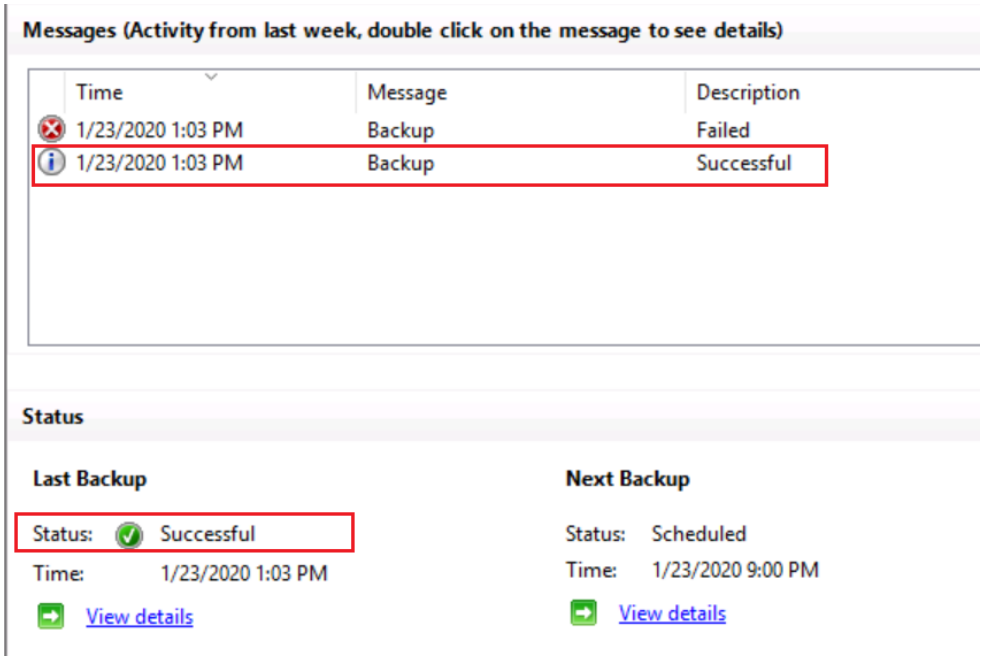
- Use Windows Server Backup to create back-ups
- There are two sort of backups: **''Backup Schedule''** and **''Backup Once''**
- In this example, **''Backup Schedule''** will be the example.

1. Open Windows Server Backup
2. Click on Backup Schedule
3. Click on Custom
4. Next
5. Click on ''Add Items''
6. Select ''System state''
7. Choose how often you want to run backups. I will keep it by default.
8. Click next
9. Select where you want to store back-ups
10. Click next
11. Select the disk to store the back-ups
12. Click next
13. Click Finish

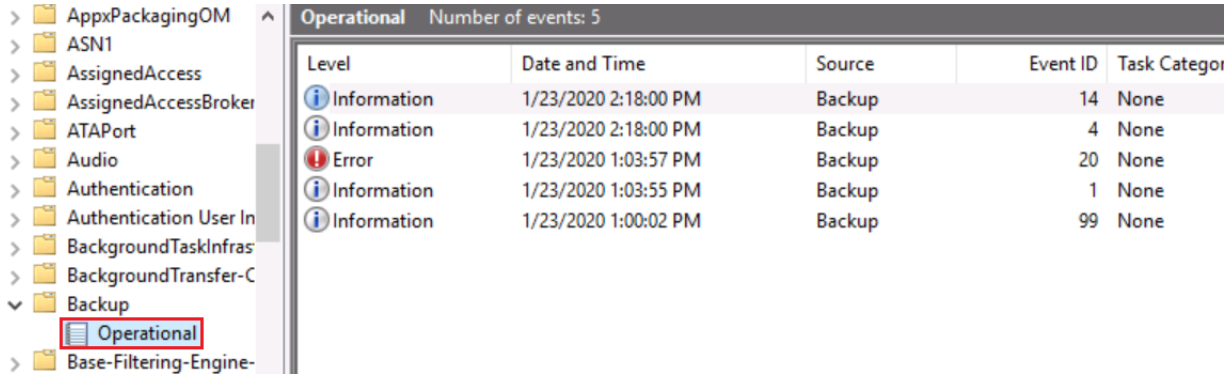
Scheduled Task with the name **''Microsft-Windows-WindowsBackup''** will be created.



After the back-up schedule has been completed. It will be displayed in the GUI of the **Windows Server Backup**.



All the event logs regarding back-ups can be found at **Microsoft-Windows-Backup\Operational**, and event **14** tells that a backup has been completed.



- 1.2 – Backups of DHCP

Task	Tier 0 admins

- **Summary**

A DHCP Server is a (network) server that automatically provides and assigns IP addresses to client devices, but not only IP addresses. It also assigns default gateways and other network parameters. DHCP is a crucial part, because DHCP allows devices to participate in a network by allocating IP addresses to clients. It verifies against AD to check if it is authorized to lease IP addresses.

- Log on the DHCP server
- Run PowerShell with elevated rights

```
Backup-DhcpServer -ComputerName "IDENTITY-DC" -Path "C:\Temp"
```

Here we are making a backup of our DHCP configuration.

We are storing our DHCP configuration in the Temp directory.

DhcpCfg is the configuration file of the DHCP

Now the second part is to restore the DHCP configuration

```
Restore-DhcpServer -ComputerName "dhcpserver.contoso.com" -Path "C:\Temp"
```

```
PS C:\Users\Testing.IDENTITY> Restore-DhcpServer -ComputerName "IdentityManager" -Path "C:\Temp"

Confirm
The DHCP server database will be restored from the file C:\Temp. Do you want to want to perform this action?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
WARNING: Please restart the DHCP server for the restored database to take effect.
PS C:\Users\Testing.IDENTITY>
```

Last, but not least. We now need to restart the DHCP server.

```
Restart-service dhcpserver
```


```
PS C:\Users\Testing.IDENTITY> Restore-DhcpServer -ComputerName "IdentityManager" -Path "C:\Temp"

Confirm
The DHCP server database will be restored from the file C:\Temp. Do you want to want to perform this action?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
WARNING: Please restart the DHCP server for the restored database to take effect.
PS C:\Users\Testing.IDENTITY>
```


Backup of DHCP has been made and restored.

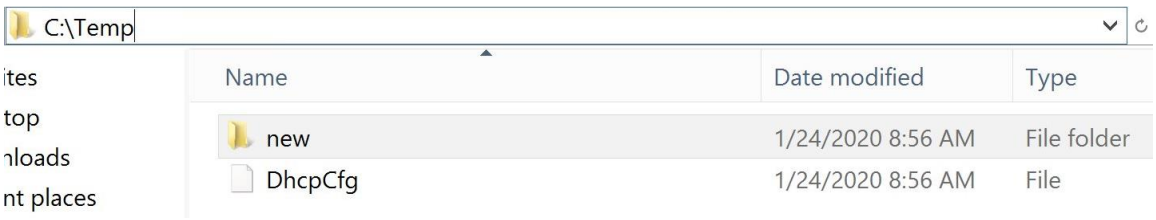
- **Recommendations**

DHCP is a very important part to backup, but since we know that ransomware, attacks are going after backups as well. It is recommended to have an offline DHCP backup as well.

What do I mean with offline backups? I made a DHCP backup and stored all the configuration data in the **C:\Temp** folder.

The entire configuration data that is stored in the **C:\Temp** folder needs to be stored somewhere else as well, which should be an offline server (without internet connection) that is NOT joined to Active Directory.

Last, but not least. A procedure needs to be in place to have a plan for making offline DHCP backups and a concrete plan on how to restore it.



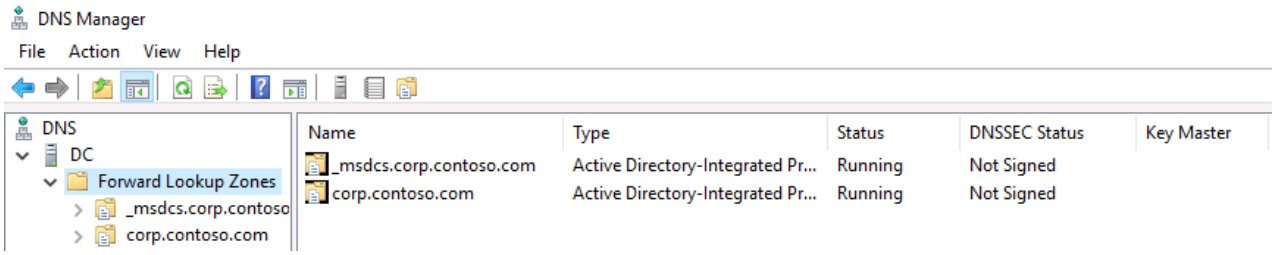
- 1.3 – Backups of DNS

Task	Tier 0 admins

- **Summary**

DNS is a resolution method for resolving hostnames to IP addresses. Active Directory relies on DNS. In Active Directory, DNS maintains a database of services that are running on a network. The list of services running are managed in the form of service records (SRV).

Service records allow a client in an active directory environment to locate to a service, like the file server for example. This is a crucial part to take in the backup plan as well. Do not leave DNS out of the backups.

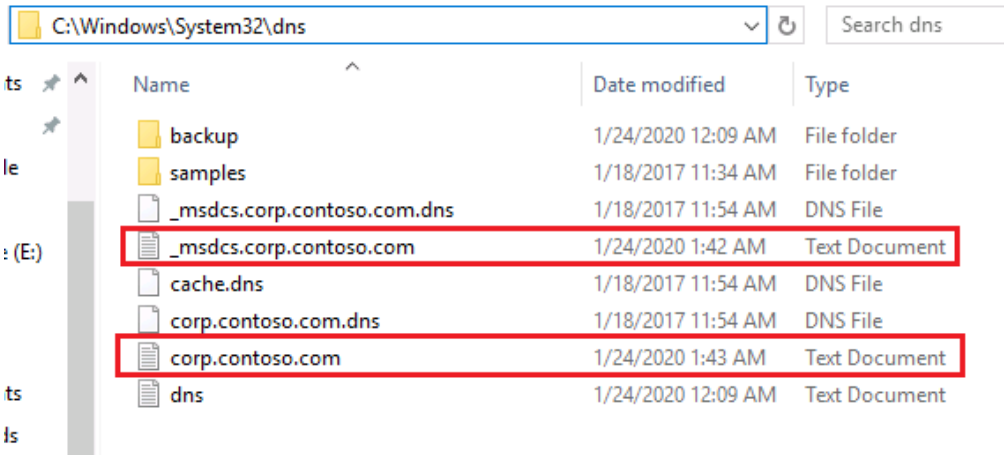


- Log on the DC
- Run PowerShell with elevated rights

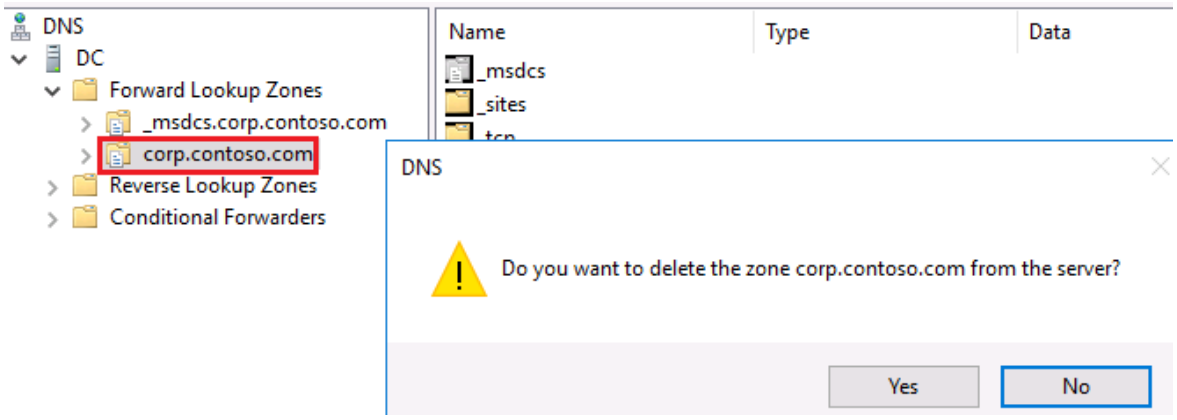
```
Dnscmd /zoneexport _msdcs.contoso.com _msdcs.contoso.com.txt

Dnscmd /zoneexport corp.contoso.com corp.contoso.com.txt
```

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> Dnscmd /zoneexport _msdcs.corp.contoso.com _msdcs.corp.contoso.com.txt

DNS Server . exported zone
  _msdcs.corp.contoso.com to file C:\windows\system32\dns\_msdcs.corp.contoso.com.txt
Command completed successfully.

PS C:\windows\system32> Dnscmd /zoneexport corp.contoso.com corp.contoso.com.txt

DNS Server . exported zone
  corp.contoso.com to file C:\windows\system32\dns\corp.contoso.com.txt
Command completed successfully.
```

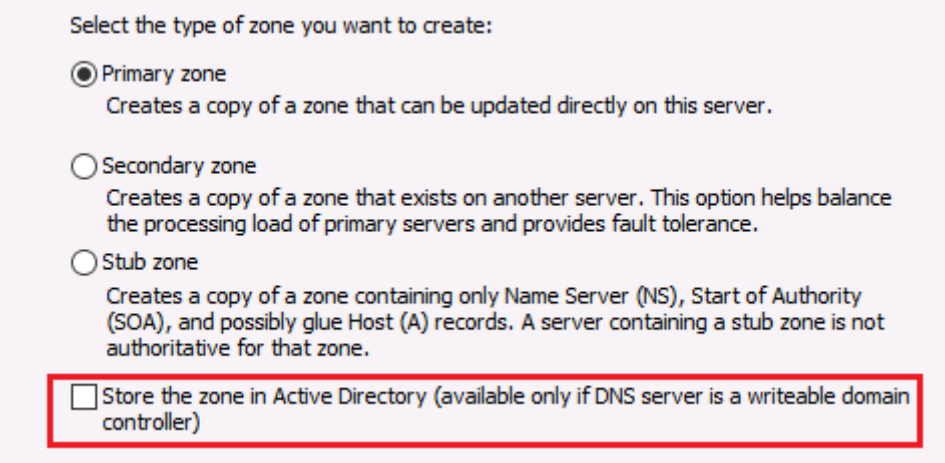
All the DNS configuration is now stored in **C:\Windows\System32\dns**



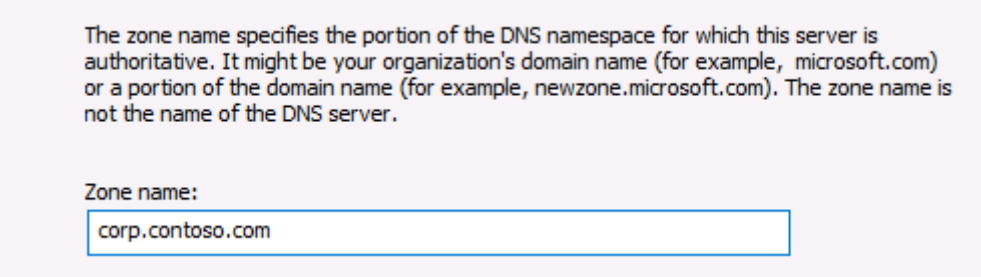
I am now going to delete the corp.contoso.com FWLZ



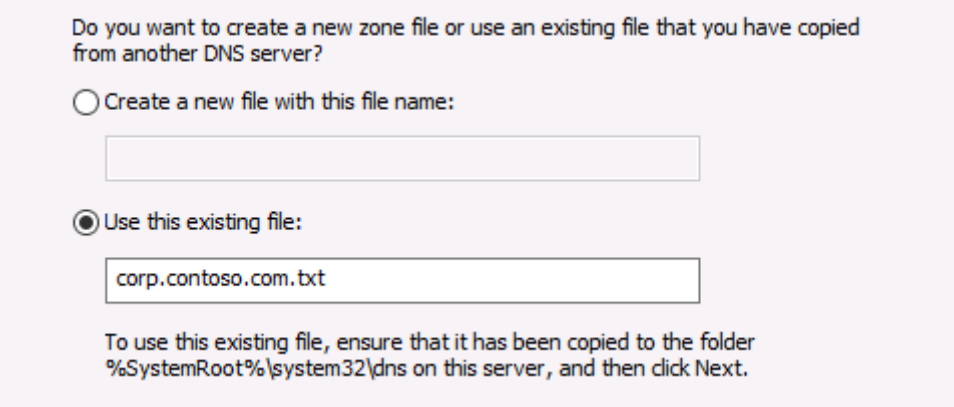
1. Create a new FWLZ and uncheck the following box



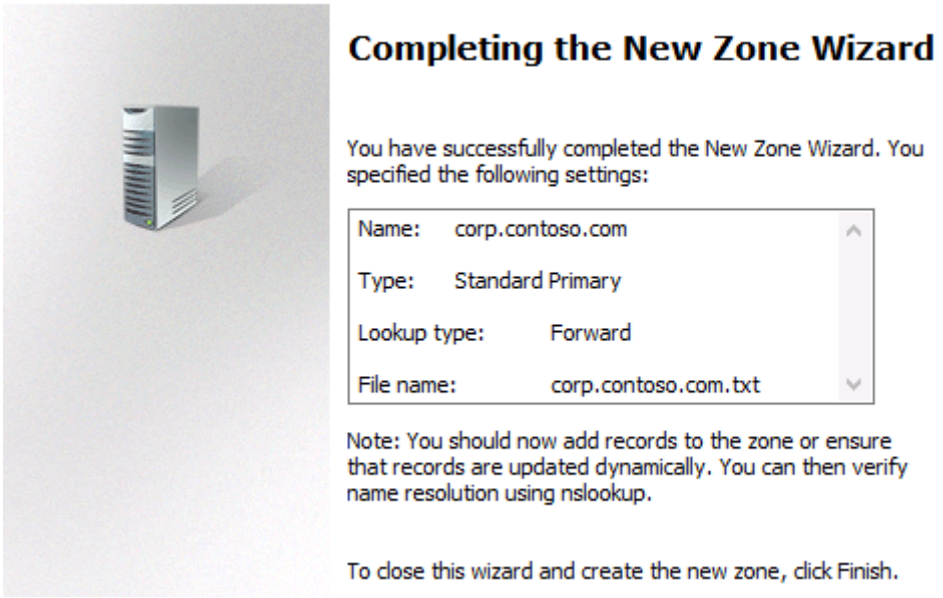
2. Type **''corp.contoso.com''** as zone name.



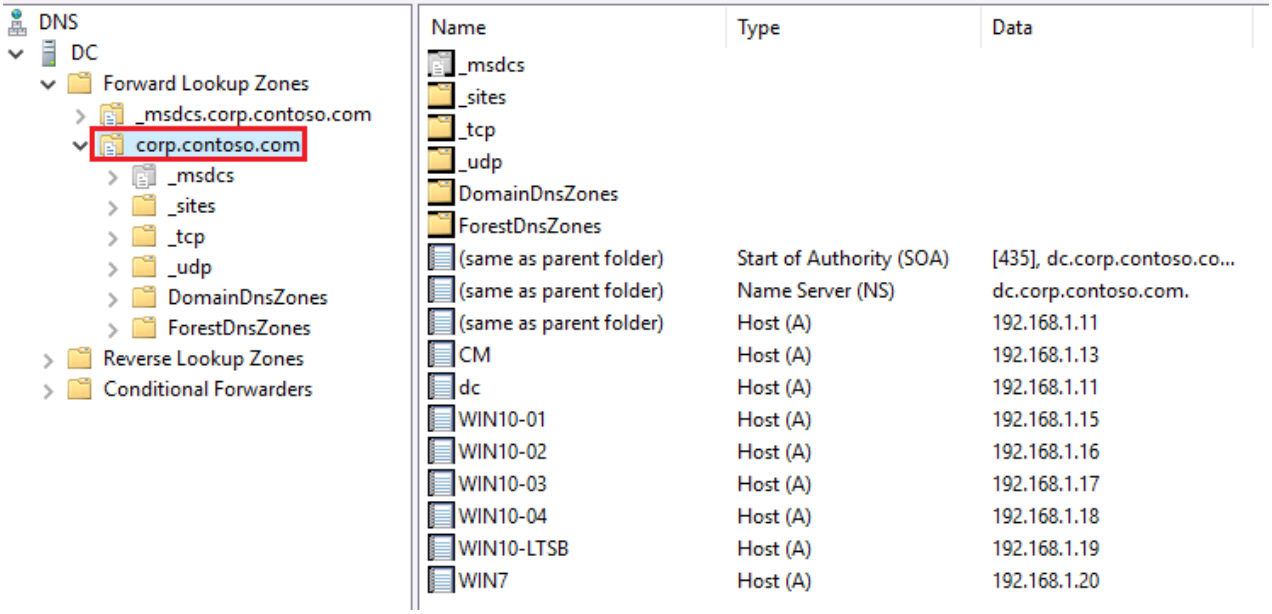
3. Select ''using existing file'' and type: **corp.contoso.com.txt**



4. Click next and then finish



5. Everything has been restored again.

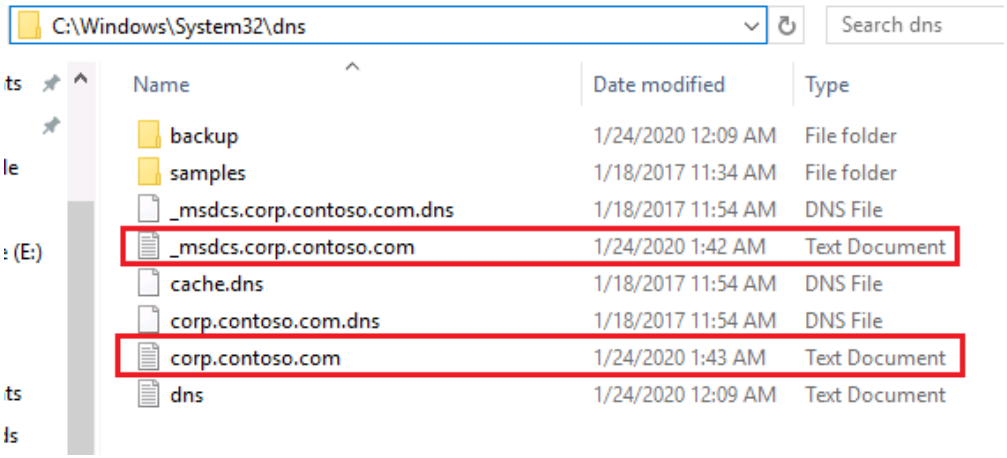


- Recommendations

Task	Tier 0 admins

Make backups of DNS, but ensure that there is also an offline backup of it. Since these are just TXT files. It is easy to backup it quickly.

The only thing that you need to do is create a procedure for making offline backups of DNS and a plan for restoring it. It is recommended to practice this procedure as well, but that's up to you.



Make sure that the DNS configuration is stored on an offline server (without internet connection) and is not joined to Active Directory.

In other words, those two TXT files that have been marked red, needs to be stored on a server that is not joined Active Directory. Again, repeat after me. ''I will store those two TXT files on a server that does not contain any connection with AD''

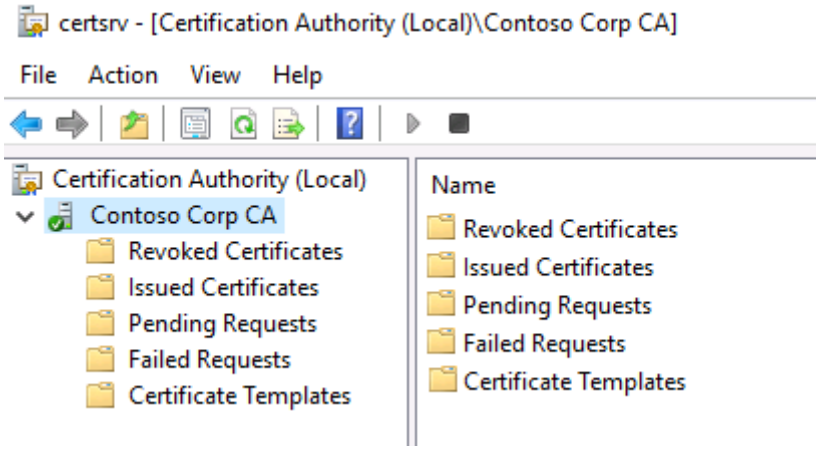
- 1.4 – Backups of PKI (AD CS)

Task	Tier 0 admins

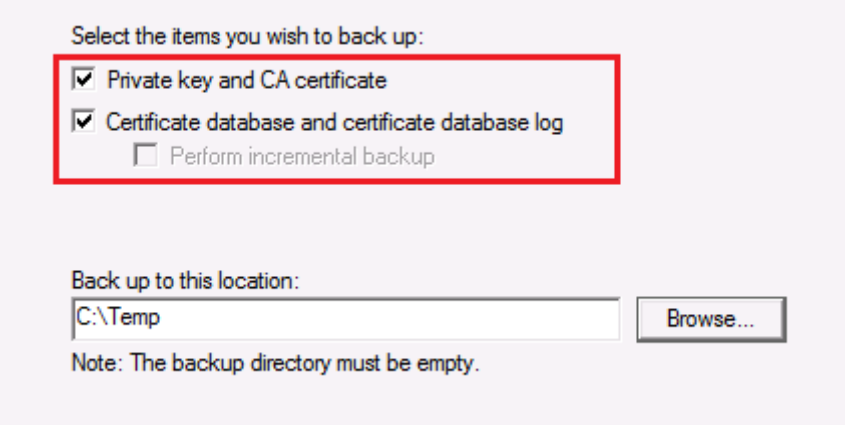
- **Summary**

Certificate Authorities are important as well, but it depends more on the purpose where PKI is used. In most organizations, I have seen so far. It is use for protecting client data.

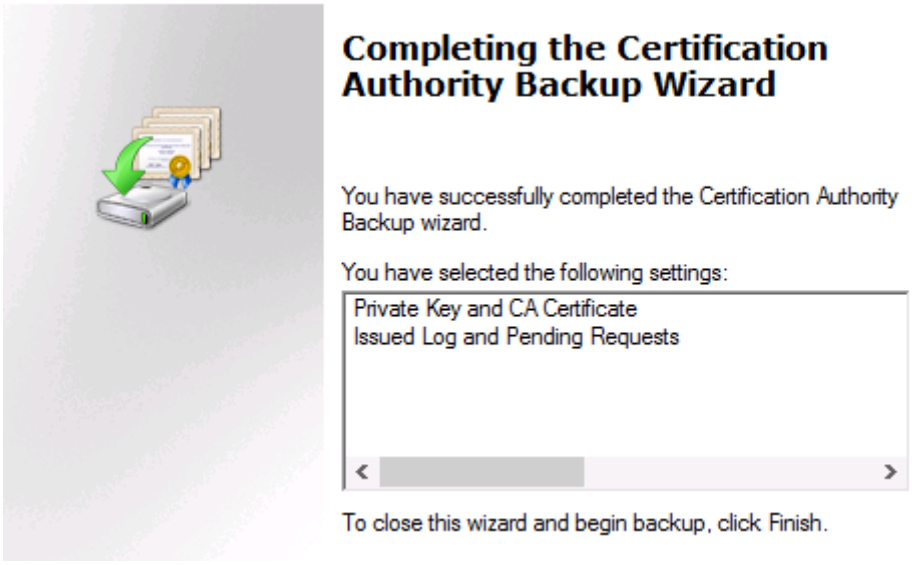
- Log on the CA server
- Open Certificate Authority



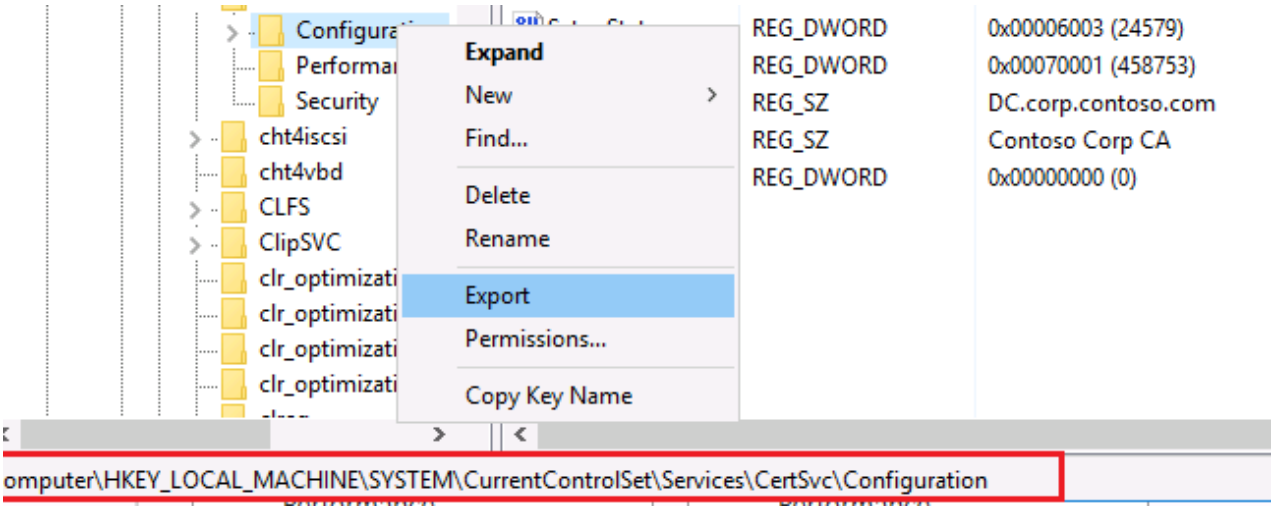
Make a backup of CA and make sure to select both checkmarks
Choose a backup location and store it over there.



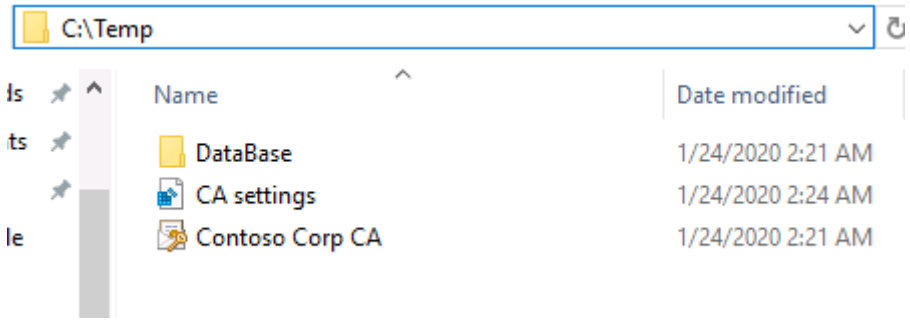
Now pick a strong password and click next to finish it.



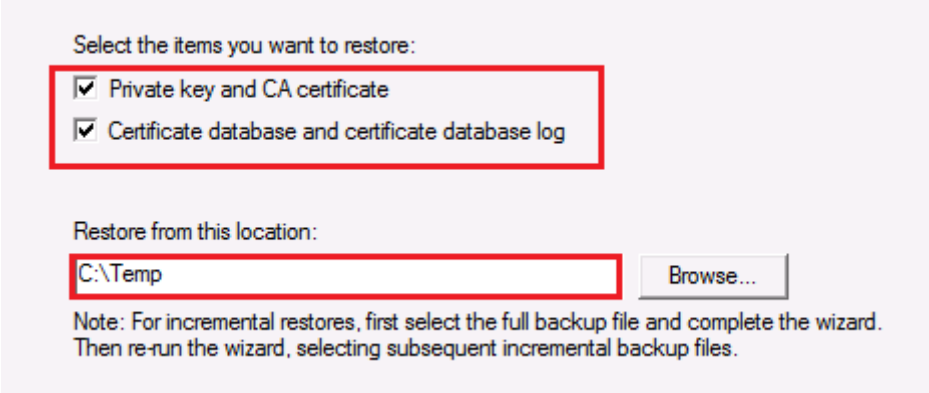
Other important thing we need to backup is the CA settings hat is stored in the following registry key: **HKLM\System\CurrentControlSet\Services\CertSVc\Configuration**



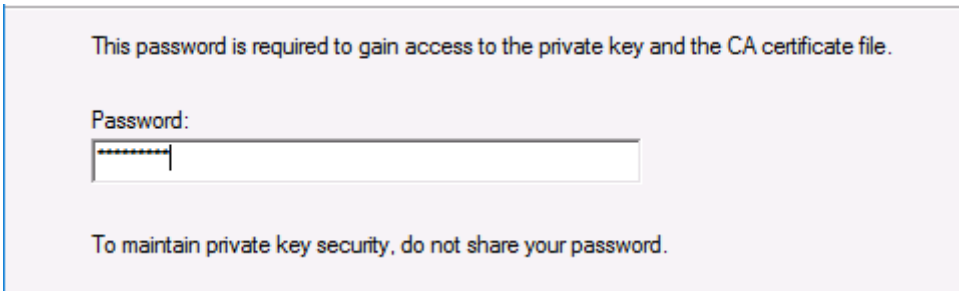
I decided to store everything in the **C:\Temp** directory and it will look like this.



- Now I am going to restore a Certificate Authority



- Type the password that you have used for your back-ups



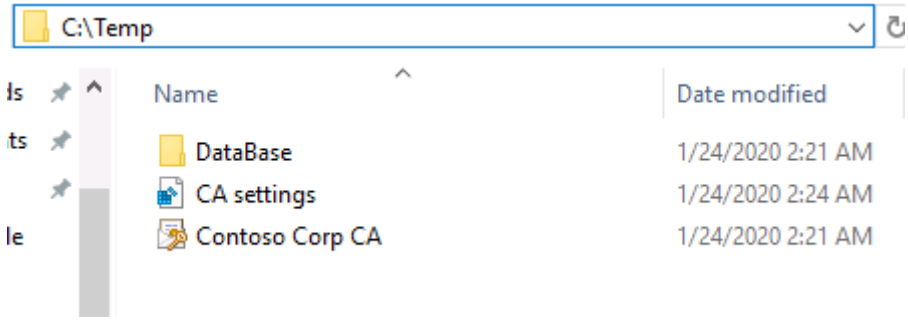
- Click next and then finish it.

- Recommendations

Make backups of PKI and store all the configuration data on an offline server that is not joined to Active Directory.

Attackers are going after back-ups as well, but I assume everybody is aware of that. Backups are important, so do not forget it. Also, do not forget to make an export of the CA setting registry key.

In other words, all of the configuration data that we just stored in the C:\Temp folder. Needs to be stored on an offline server that is again, not joined to Active Directory. Nevertheless, do not forget the password of the backup.



• 2.1 – Hardening settings for Domain Controllers

Task	Tier 0 admins

- **Summary**

Default settings of Domain Controllers are not that great. Every DC has by default the ''Default Domain Controllers Policy'' in place, but this GPO creates different escalation paths to Domain Admin if you have any members in Backup Operators or Server Operators for example. They can become Domain Admin.

Start with replacing the ''Default Domain Controllers Policy'' and replace it with a new GPO that is more security focused.

- **User Right Assignment**

Access this computer from the network	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
Add workstations to a domain	Administrators
Allow log on locally	Administrators, Backup Operators
Backup files and directories	Administrators, Backup Operators
Change the system time	LOCAL SERVICE, Administrators
Debug Programs	Administrators
Deny access to this computer from the network	Guests
Deny log on through Remote Desktop Services	Guests
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from remote system	Administrators
Load and unload device drivers	Administrators
Restore files and directories	Administrators, Backup Operators
Shutdown the system	Administrators
Take ownership of files and objects	Administrators

NOTE: Remove Backup Operators if it is not in use.

- **Security Options**

Devices: Prevent users from installing printer drivers	Enabled
Domain Controller: Allow server operator to schedule tasks	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM

The setting that has been marked in RED needs more attention, because it can break things, which means that it needs to be tested very well, before deploying it in production.

There are two NTLM audit settings that needs to be enabled to track down the use of NTLM

Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Enable auditing for domain accounts
Network security: Restrict NTLM: Audit NTM authentication in this domain	Enable all

Event 4624 with data fields like ''Authentication Package'' and ''Package name (NTLM only)'' needs to be filtered.

If you see something like NTLMV1 at Package Name. It shows you that there is an application still using NTLMv1. Disabling NTLM immediately can have break an application. Make sure this is tested properly.

- Recommendation

Configure all those recommended settings, but keep a sharp eye on the ''LAN Manager Authentication level'' – It is recommended to use Send NTLMv2 response only and refusing LM & NTLM, but to test this properly.

Start the following test phase:

- Enable the two NTLM auditing policies and start monitoring to see if there are applications using NTLMv1. If you are confident that there are no legacy apps anymore.
- Start changing the policy to: ''Send NTLMv2 response only and Refuse LM''
- Now keep monitoring and if you are confident to make the step
- Change the policy to: ''Send NTLMv2 response only. Refuse LM & NTLM''

• 2.2 – Disabling unnecessary services on Domain Controller

Summary:

By default, there are unnecessary services enabled on a Domain Controller. It is a best practice to disable unnecessary services to improve the performance of a DC. There is even a service enabled by default on a DC that can be used in an escalation path to compromise Active Directory.

- Disable the following **services**

Xbox Live Auth Manager	Stop
Xbox Live Game Save	Stop
Print Spooler	Stop

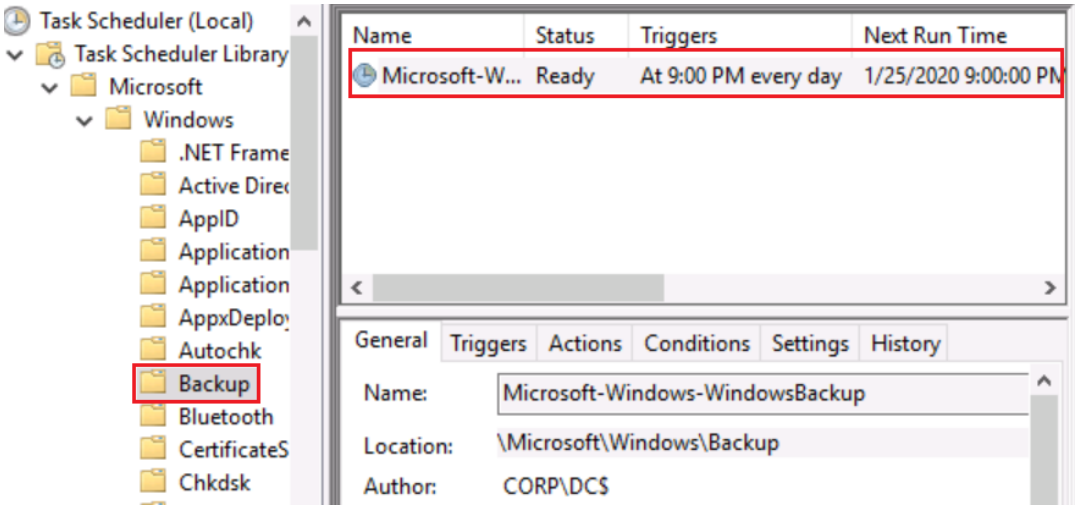
- 2.3 – Auditing the last backup of the Domain Controllers

Summary:

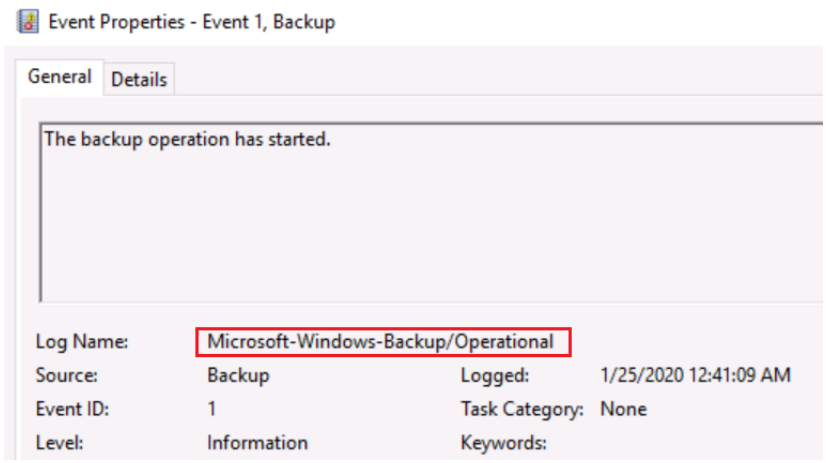
Making back-ups of Domain Controllers is the most critical part of Active Directory security, but most organizations do not perform periodically audits to see if back-ups are really in place and stored securely. We'll get later to the ''store securely'' part.

There are different backup solutions in the market to help organizations do their AD/DC backups, but since ADSA is not here to pitch a vendor. We will rely on the **Windows Server Backup** that is free for everybody. It is far from perfect, but it is at least something.

Every time when a backup has been scheduled. An scheduled task will be made and created under the location: **\Microsoft\Windows\Backup** with the name **''Microsoft-Windows-WindowsBackup''**



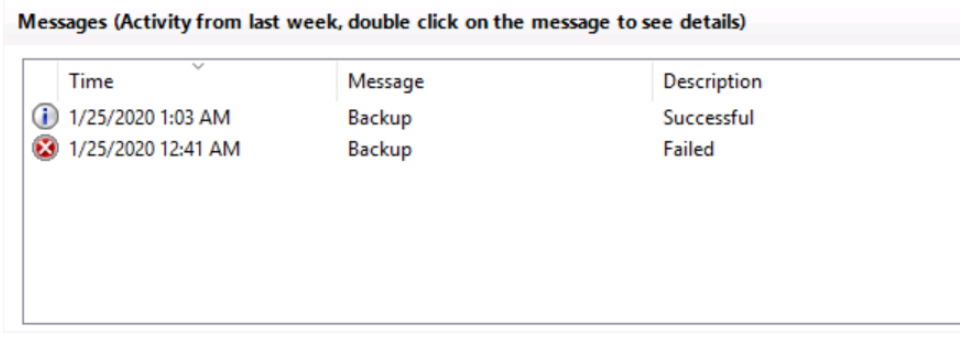
All the backup event logs are located under **Microsoft-Windows-WindowsBackup\Operational**

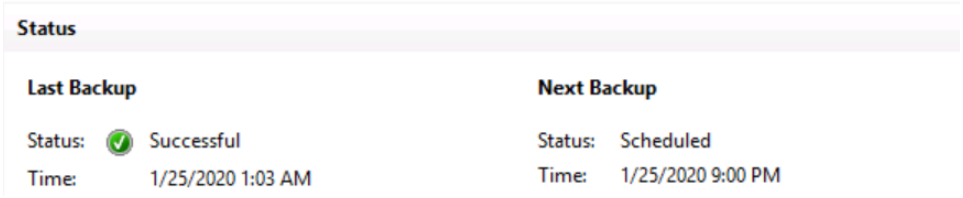


- Recommendation

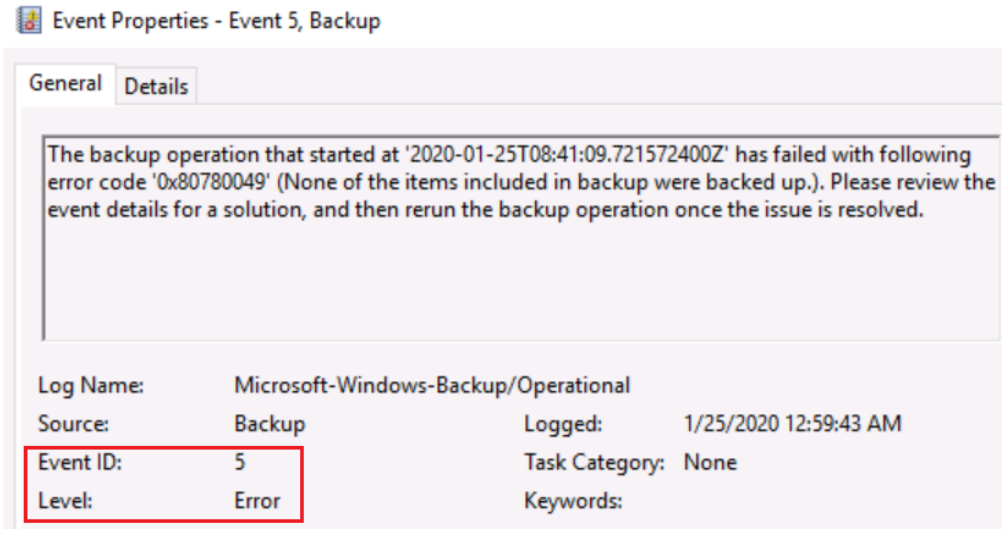
Windows Server Backup provides information about backups. Like for example. If a backup was successful or perhaps it failed. Are you aware when a backup has failed?

Here we can see that a backup has failed, but do you get any alerts in your SIEM solution that rings bells?





All the backup event logs are stored under the location: **Microsoft-Windows-Backups\Operational**

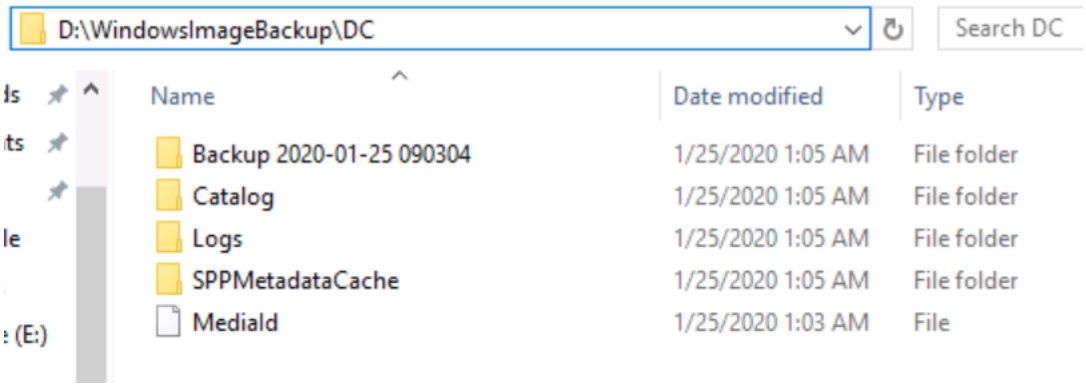


- Recommendation 2

Offline back-ups are very important. In many ransomware attacks, attackers have been leveraging to backup servers as well. Sure, back-ups have been created, but they were all hanging in the same Windows domain.

After the backup schedule has been finished. A directory folder will be made with the name ''**WindowsImageBackup**'' and it stores all the back-up data.

Ensure that you have a back-up, stored offline, and the server should not being a part of Active Directory. Do not store your backups on



The second important part is to monitor event logs of Backups. All the event logs that are related to Backups are located under **Microsoft-Windows-Backup\Operational**

Event ID	**Description**
4	The backup operation has finished successfully
5	The backup operation that started at <XYZ> has failed.

• 2.4 – Restore backup of DC

Summary:

Making back-ups is one thing, but restoring is the second part. When Active Directory is down. Most organizations won't be able to go further with their business, but without doing anything. All the problems will still be there.

A restore plan needs to be in the place to restore Active Directory. Every organization should have a restore plan, but it is difficult to judge for others on how you should develop a restore plan, because there might be companies using third party tools to do it for them.

Here are a few tips:

- DSRM or known as Directory Services Restore Mode is the break-glass account for Domain Controllers. This account should be used in disaster recovery scenarios
- Credentials of DSRM needs to be stored securely and only being access able for the right people.
- **Offline** back-ups of AD/DC should always be up and running, so you can restore them ASAP.

Practice it:

- Create a test environment in Azure for example
- Make sure you or your team has practice this restore plan ''hands-on'' or otherwise you would struggle a lot.

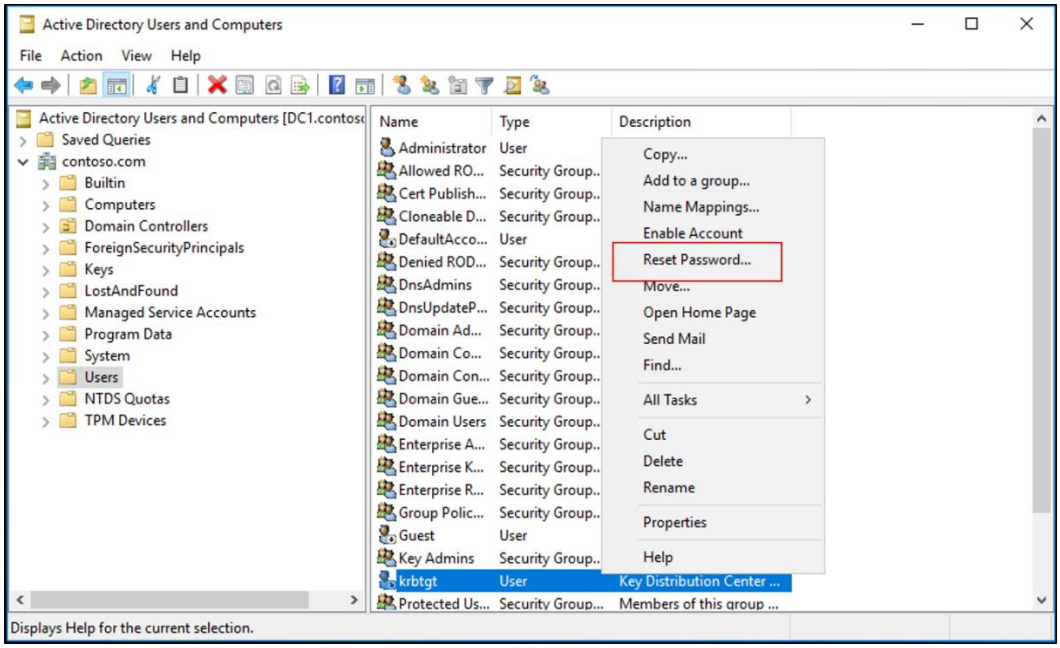
- 2.5 – Rotating the password of KRBTGT account

Summary:

A procedure for rotating the password of KRBTGT needs to be in place. KRBTGT is the security principal for the KDC. The KDC encrypts a user's TGT with the key it derives from the password of the KRBTGT account. In other words. KDC encrypts a user's TGT with the NT hash of the KRBTGT account.

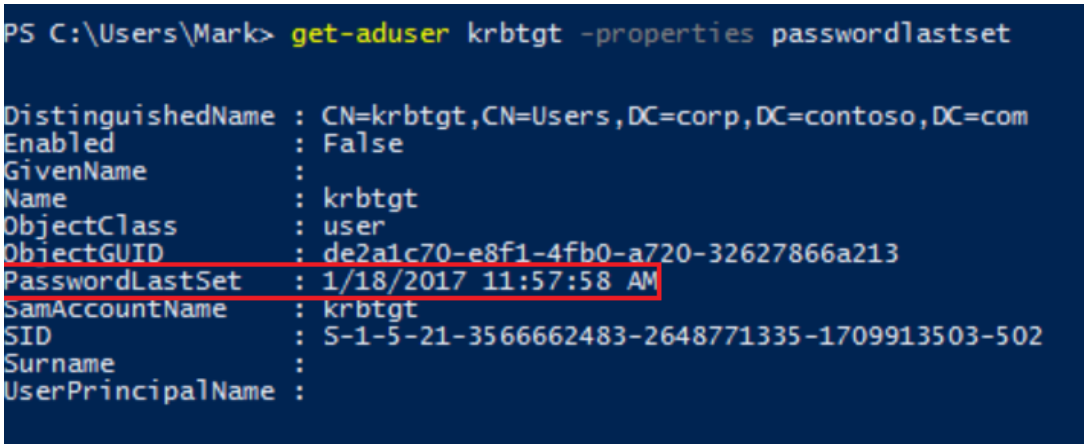
An attacker that manages to get the NT hash of the KRBTGT account can create ''Golden Tickets'' to impersonate every user in the domain, but this requires Domain Admin or equivalent.

Best practice is to reset the password twice of the KRBTGT account every half year.



- Recommendation

Start with resetting the password of the KRBTGT twice every half year, but keep in mind that you don't reset the password rapidly or otherwise Kerberos services might break.

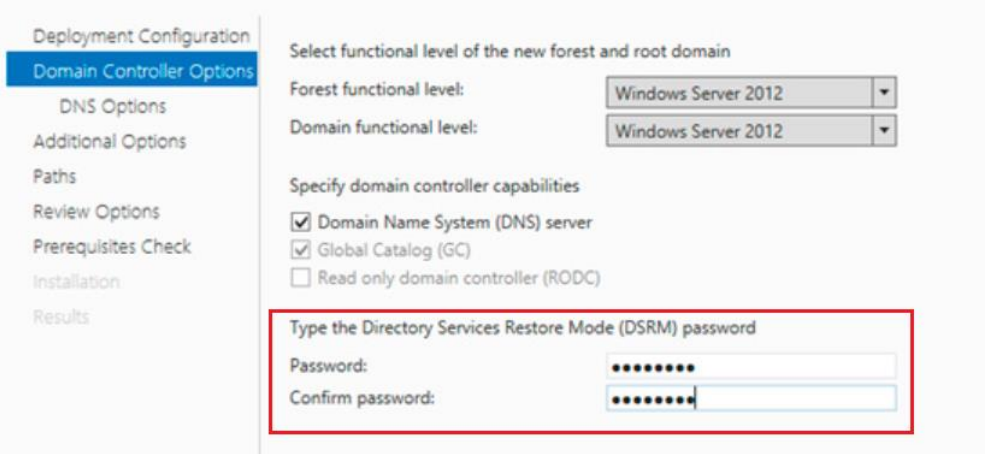


- Reset the password of the KRBTGT, but don't do it rapidly. Make sure you reset the password once, and wait. Wait until you can do the second reset. Usually it is around 10-24 hours, before you can do the second reset.
- Here is a script that can be used for validation to see if all DC's has replicated to each other. https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

- 2.6 – Rotate the password of the DSRM account

Summary:

DSRM is like the break-glass account of Domain Controllers. You have to define a password for the account, when you are promoting a member server to a DC. DSRM is like the ''Local Administrator'' on a DC. Password of the DSRM account is rarely changed, and it is a best practice to rotate this password.



- Log on the Domain Controller
- Run CMD with elevated rights
- Reset the password of the DSRM account

Ntdsutil
Set DSRM password
Reset password on Server DC – ''DC'' is the server name
Type the new password of the DSRM and press **enter**
Re-type the password of DSRM to change the password and press **enter**
Type **quit** and press **enter**
Type **quit** again and press **enter**

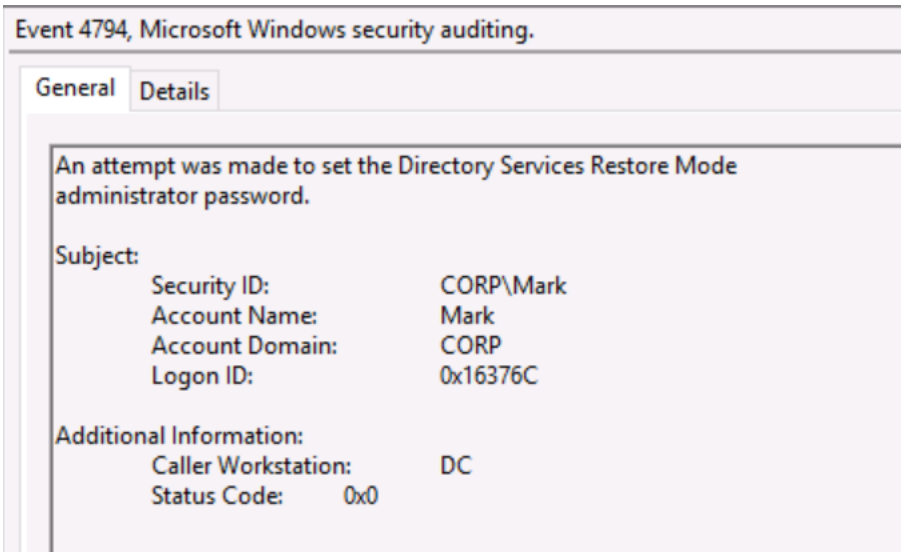
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>ntdsutil
ntdsutil: set dsrm password
Reset DSRM Administrator Password: reset password on server DC
Please type password for DS Restore Mode Administrator Account: *********
Please confirm new password: *********
Password has been set successfully.

Reset DSRM Administrator Password: quit
ntdsutil: quit
```

- Recommendation

A procedure needs to be in place to reset the password of the DSRM account. It is recommended to rotate the password of the DSRM account every half year or year.

Besides, of rotating the password of the DSRM account. It needs to be stored securely as well with limiting access to the password. Something like a Password Manager is a good begin.

Last, but not least. Monitor event log ''**4794**'' as it notifies, when someone is resetting the password of the DSRM account.



- 2.7 – Improve auditing rules

Summary:

Domain Controllers are crucial servers and solid auditing needs to be in place to track different changes. Default audit policies are not enough to have a (better) visibility in tracking potential malicious behaviour.

Logging is important, but if you don't know what to log. It can become difficult. Good news is that, Windows Security Baseline has provided some guidance around auditing policies.

- Recommendation

Default auditing policies of the Domain Controller is not enough. It gives limited visibility in changes that are made. Windows Security Baseline has solid advice for configuring audit policies of DC's.

The following audit policies are recommended to configure for Domain Controllers.

- Start with creating a GPO and configure the following ''advanced'' audit policies:

Advanced Audit Policies

Policy Path	Policy Setting	Configured setting
Account Logon	Audit Credential Validation	Failure
Account Logon	Audit Kerberos Authentication Service	Success and Failure
Audit Logon	Audit Kerberos Service Ticket Operations	Failure
Account Management	Audit Computer Account Management	Success
Account Management	Audit Other Account Management	Success
Account Management	Audit Security Group Management	Success
Account Management	Audit User Account Management	Success and Failure
Detailed Tracking	Audit PNP Activity	Success
Detailed Tracking	Audit Process Creation	Success
DS Access	Audit Directory Services Access	Failure
DS Access	Audit Directory Service Changes	Success
Logon/Logoff	Audit Account Lockout	Failure
Logon/Logoff	Audit Group Membership	Success
Logon/Logoff	Audit Logon	Success and Failure
Logon/Logoff	Audit Other Logon/Logoff Events	Success and Failure
Logon/Logoff	Audit Special Logon	Success
Object Access	Audit Detailed File Share	Failure
Object Access	Audit File Share	Success and Failure
Object Access	Audit Other Object Access	Success and Failure
Object Access	Audit Removable Storage	Success and Failure

Policy Path	Policy Setting	Configured Setting
Policy Change	Audit Policy Change	Success
Policy Change	Audit Authentication Policy Change	Success
Policy Change	Audit MPSSVC Rule-Level Policy Change	Success and Failure
Policy Change	Audit Other Policy Change Events	Failure
Privilege Use	Audit Sensitive Privilege Use	Success and Failure
System	Audit Other System Events	Success and Failure
System	Audit Security State Change	Success
System	Audit Security System Extension	Success
System	Audit System Integrity	Success and Failure

A list of recommended security event logs can be find at **10.5**

- 2.8 – Securing Built-in\Administrator account

Summary:

In every Active Directory environment, there is an ''Administrator'' account that is stored in the **Users** container. It has the **500** value at the end of the **objectSID**.

There has been a lot of misconception around this account, whether it should be disabled or not. I also felt that the purpose behind this account was a bit unclear, but Microsoft has documented information around this.

According to Microsoft:

"Use of a domain's Administrator account should be reserved only for initial build activities, and possibly, disaster-recovery scenarios."

In many environments. This account was used for some SQL deployments and it often has a SPN registered to it with as an example. ''MSSLSvc/corp.contoso.com:1433" or something similar.

Nevertheless, this account is rarely changed, and there is a huge chance that it contains a poor password.

```
PS C:\Users\Mark> Get-ADUser Administrator -Properties passwordlastset


DistinguishedName : CN=Administrator,CN=Users,DC=corp,DC=contoso,DC=com
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 938584cc-6b6e-46be-b3a7-0da1307720aa
PasswordLastSet   : 1/18/2017 11:27:11 AM
SamAccountName    : Administrator
SID               : S-1-5-21-3566662483-2648771335-1709913503-500
Surname           :
UserPrincipalName :
```

• Recommendations

Many environment have disabled this account, but it is recommended to enable the Administrator account, because it can logon without access to a Global Catalog server.

When can I use the Administrator account?

I am sure that you could use it for other purposes as well, but like Microsoft recommends it. It is an account that is mainly in use for disaster recovery scenarios, so pleas avoid using this account for unnecessary tasks.

- Disaster Recovery purposes
- Promoting a Domain Controller

Before enabling this account. It is highly recommended to create a GPO and link it to the **workstations** and **servers** OU to deny logon access for the Administrator account. Since this account is a member of the Domain & Enterprise Admins group. It can access everything.

User Right Assignment

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on through Remote Desktop

After you have created the GPO and linked it to the OU of the workstations and servers, which should deny logon access to the Administrator account. It is time to follow the other best practices, and that is the following:

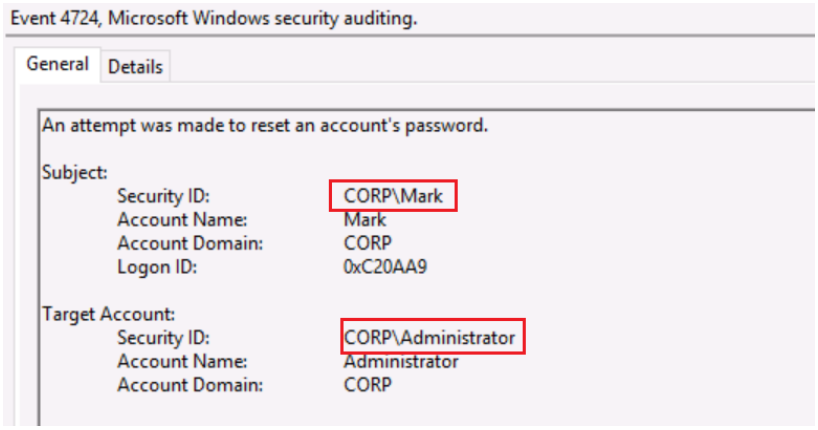
- Ensure the ''Account is sensitive and cannot be delegated'' checkmark is enabled
- Remove the SPN if it has one
- Rotate the password every half year or year
- Protect the account from a Tier 0 operations
- Monitor logon activities with it.

- Recommendations 2

Monitoring activities around this account important and here are the recommendations:

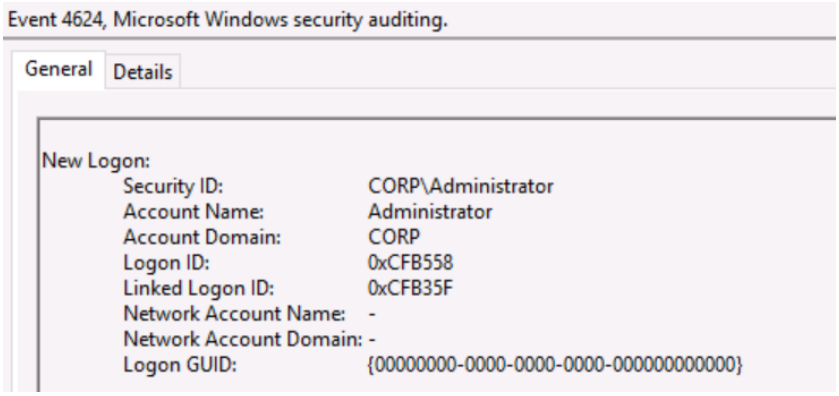
- Monitor when someone is changing the password of the Administrator account

Event ID	Description
4742	An attempt was made to reset an account's password



- Monitor logon activities with the Administrator account

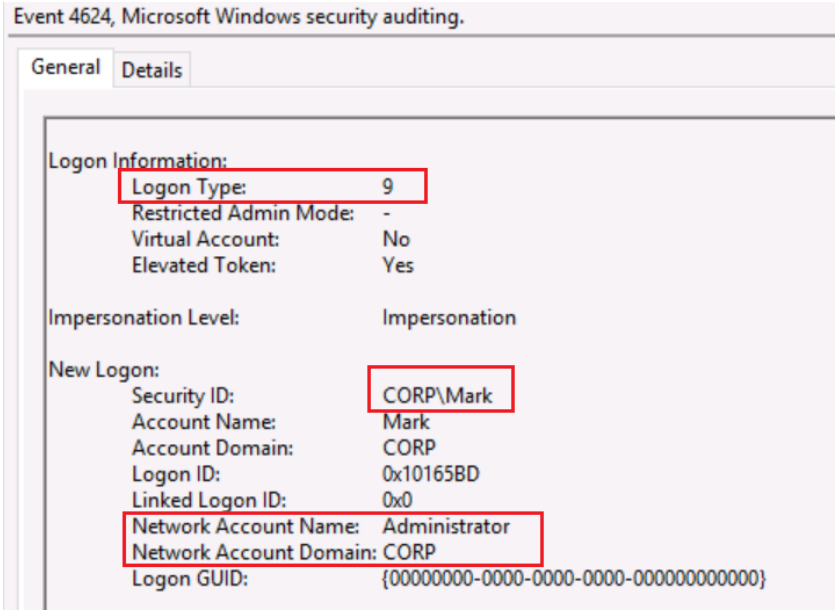
Event ID	Description
4624	An account successfully logged on



- Monitor when someone does a ''Run as'' with the Administrator account ;-)

Event ID	Description	Logon Type
4624	An account was successfully logged on	9

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>runas /USER:CORP\Administrator /netonly cmd
Enter the password for CORP\Administrator:
Attempting to start cmd as user "CORP\Administrator" ...
```



Look at the Logon Type 9, which is NewCredentials. Mark did a ''Run as'' with the Administrator account and Logon type 9 means the following:

"A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections." – Eventlogxp.com

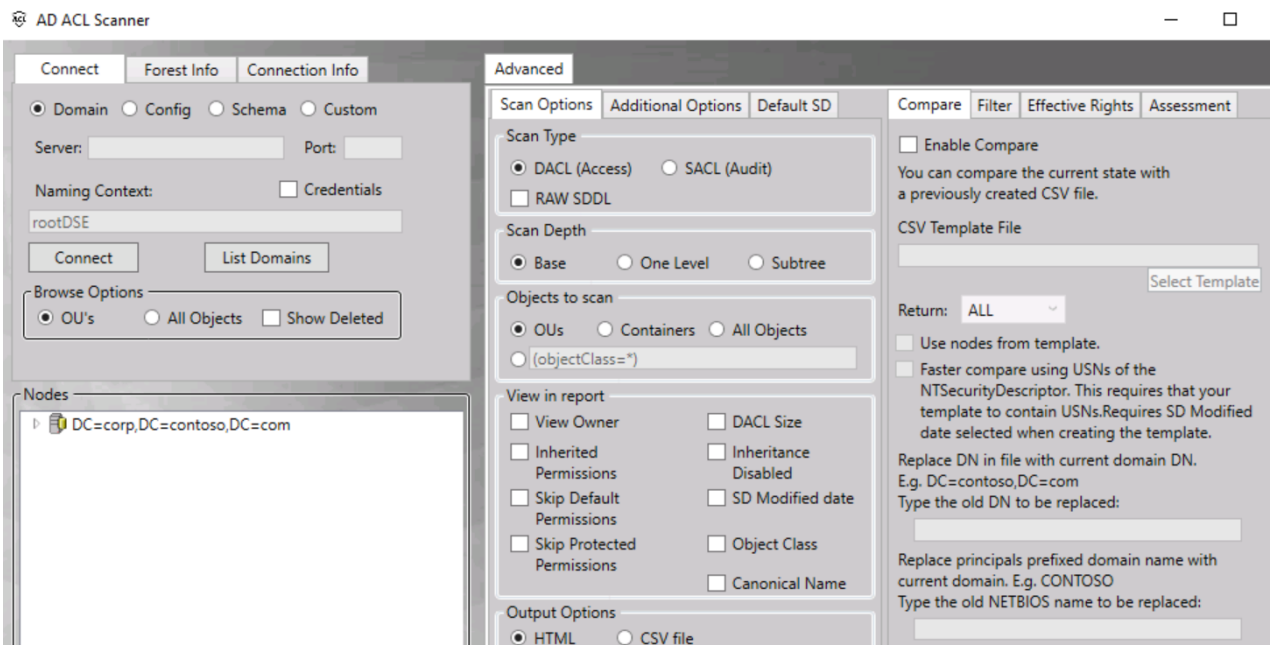
- 3.1 – Running periodically AD ACL Scans

Summary:

A former Microsoft PFE made a great tool to scan all the different ACL's in an environment. ACL/ACE's are often set by admins for temporary tasks, but they are never revoked again. Which means that all of these ACLs are staying for years in an environment, which creates multiple escalation paths for attackers as well.

There are many tools on the internet, where attackers are mapping out an entire environment to discover different escalation paths through ACLs. This tool can be used as a low user without admin rights.

- Start with using **AD ACL Scanner** to get an overview of all the ACLs in an environment
- **AD ACL Scanner**: https://github.com/canix1/ADACLScanner

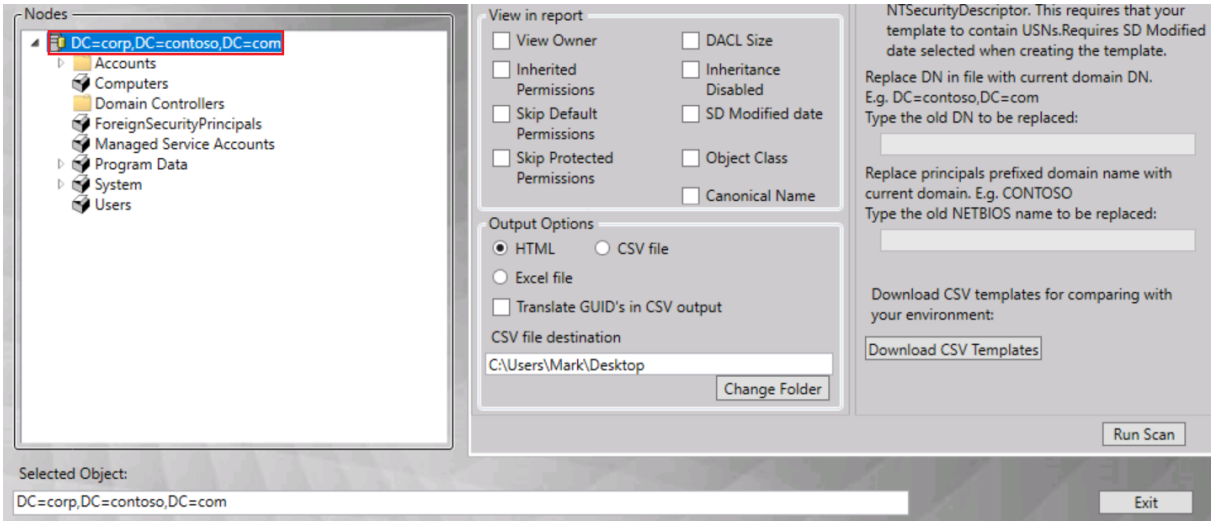


Reference:

https://docs.microsoft.com/en-us/archive/blogs/pfesweplat/forensics-active-directory-acl-investigation

- Recommendation 1

Start with running ACL scans on objects in Active Directory. In this screenshot. I am now doing an ACL scan on the Domain Object or known as the Domain Naming Context.

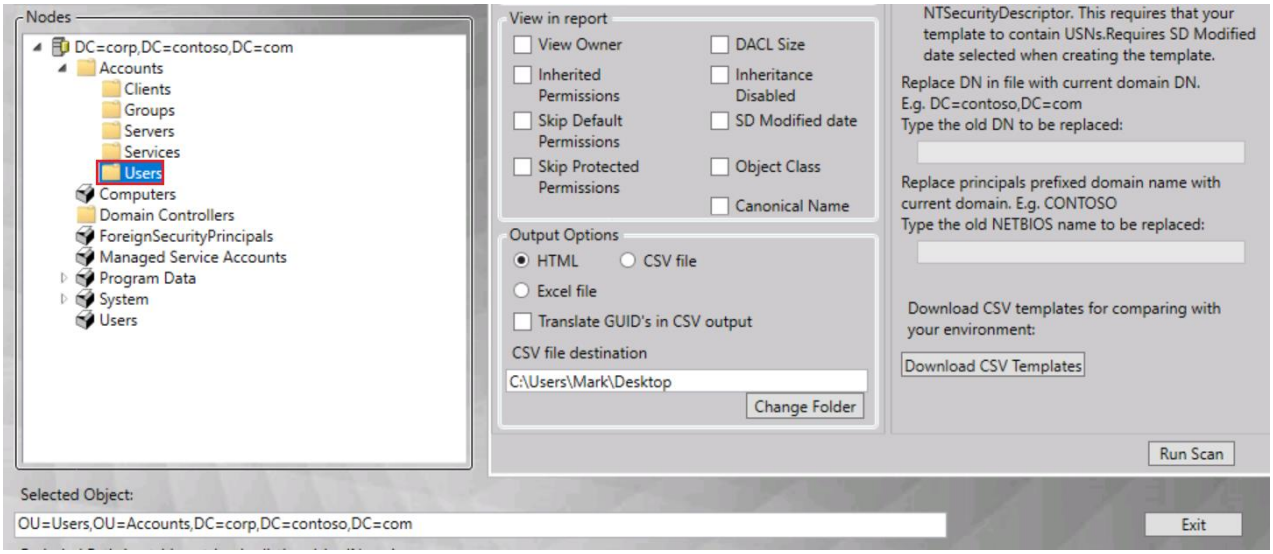


After the scan has been finished. A report will be made to display all the ACLs that has been set on the Domain Object.

Object	Trustee	Access	Inherited	Apply To	Permission
DC=corp,DC=contoso,DC=com					
DC=corp,DC=contoso,DC=com	Everyone	Deny	False	This Object Only	Delete
DC=corp,DC=contoso,DC=com	Everyone	Allow	False	This Object Only	Read All Properties
DC=corp,DC=contoso,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List
DC=corp,DC=contoso,DC=com	NT AUTHORITY\Authenticated Users	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List
DC=corp,DC=contoso,DC=com	NT AUTHORITY\SYSTEM	Allow	False	This Object Only	Full Control
DC=corp,DC=contoso,DC=com	BUILTIN\Administrators	Allow	False	This object and all child objects	CreateChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDacl, WriteOwner
DC=corp,DC=contoso,DC=com	BUILTIN\Pre-Windows 2000 Compatible Access	Allow	False	This Object Only	ReadProperty, ReadControl
DC=corp,DC=contoso,DC=com	BUILTIN\Pre-Windows 2000 Compatible Access	Allow	False	This object and all child objects	ListChildren
DC=corp,DC=contoso,DC=com	CORP\Domain Admins	Allow	False	This Object Only	CreateChild, Self, WriteProperty, ExtendedRight, GenericRead, WriteDacl, WriteOwner
DC=corp,DC=contoso,DC=com	CORP\Enterprise Admins	Allow	False	This object and all child objects	Full Control

- Recommendation 2

Now instead of scanning ACLs on the Domain Object. We are now going to scan for ACLs on an OU, which is in this example. The OU ''**Users**''



Here is the ACL scan result on the OU ''**Users**''

Object	Trustee	Access	Inherited	Apply To	Permission
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com					
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	Everyone	Deny	False	This Object Only	DeleteTree, Delete
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	NT AUTHORITY\Authenticated Users	Allow	False	This Object Only	Read Permissions,List Contents,Read All Properties,List
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	NT AUTHORITY\SYSTEM	Allow	False	This Object Only	Full Control
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	CORP\Domain Admins	Allow	False	This Object Only	Full Control
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	BUILTIN\Account Operators	Allow	False	This Object Only	Create/Delete user
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	BUILTIN\Account Operators	Allow	False	This Object Only	Create/Delete group
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	BUILTIN\Account Operators	Allow	False	This Object Only	Create/Delete computer
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	BUILTIN\Account Operators	Allow	False	This Object Only	Create/Delete inetOrgPerson
OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com	BUILTIN\Print Operators	Allow	False	This Object Only	Create/Delete printQueue

All the results can be exported in CSV files for later use and I recommend running periodically ACL scans to find potential misconfigurations.

- Recommendation 3

Understanding the permissions that can be abused by an attacker is something to be aware of. This list of examples will give you a better understanding on how it can be used by an attacker.

GenericAll	Full control	Full control on an object with the likes of a user or group • Take-over the account by resetting password • Add yourself to a group
GenericWrite	Write all properties	Write permissions on an object with the likes of a user or group • Set an SPN and disable Pre authentication for an account • Add yourself to a group
WriteDacl	Modify permission	Modify permission on an object with the likes of a user or group • Assign yourself Full control on an object and take over the account or group
WriteOwner	Modify owner	Modify owner on an object with the likes of a user or group • Take ownership rights of a user or group and own the user or group

AllExtendedRights	All extended rights	• Reset password of user • Replicate Directory Changes • Replicate Directory Changes All Never delegate AllExtend-edRights or equivalent on the Domain Object. Only service accounts that synchronize passwords should have Repli-cation permissions with the likes of Azure AD Connect for example.

Write gpLink	Write gpLink	• Ability to link a GPO to an OU
Write Members	Write Members	• Add yourself to a group
Write userAccountControl	Write userAccountControl	• Disable Pre-auth for accounts
Write account restrictions	Write account restrictions	• Includes userAc-countControl • Disable Pre-auth for accounts
Write servicePrincipalName	Write servicePrincipalName	• Write an SPN for an account to request a ST and crack it offline
Write msDs-AllowedToAc-tOnBehalfOfOtherIdentity	Write msDS-AllowedToAc-tOnBehalfOfOtherIdentity	• Act on behalf of other identities to services. • Write msDS-Al-lowedToActOnBe-halfOfOtherIdentity on Computer Objects can be used for Re-source Based Con-strained Delegation attacks

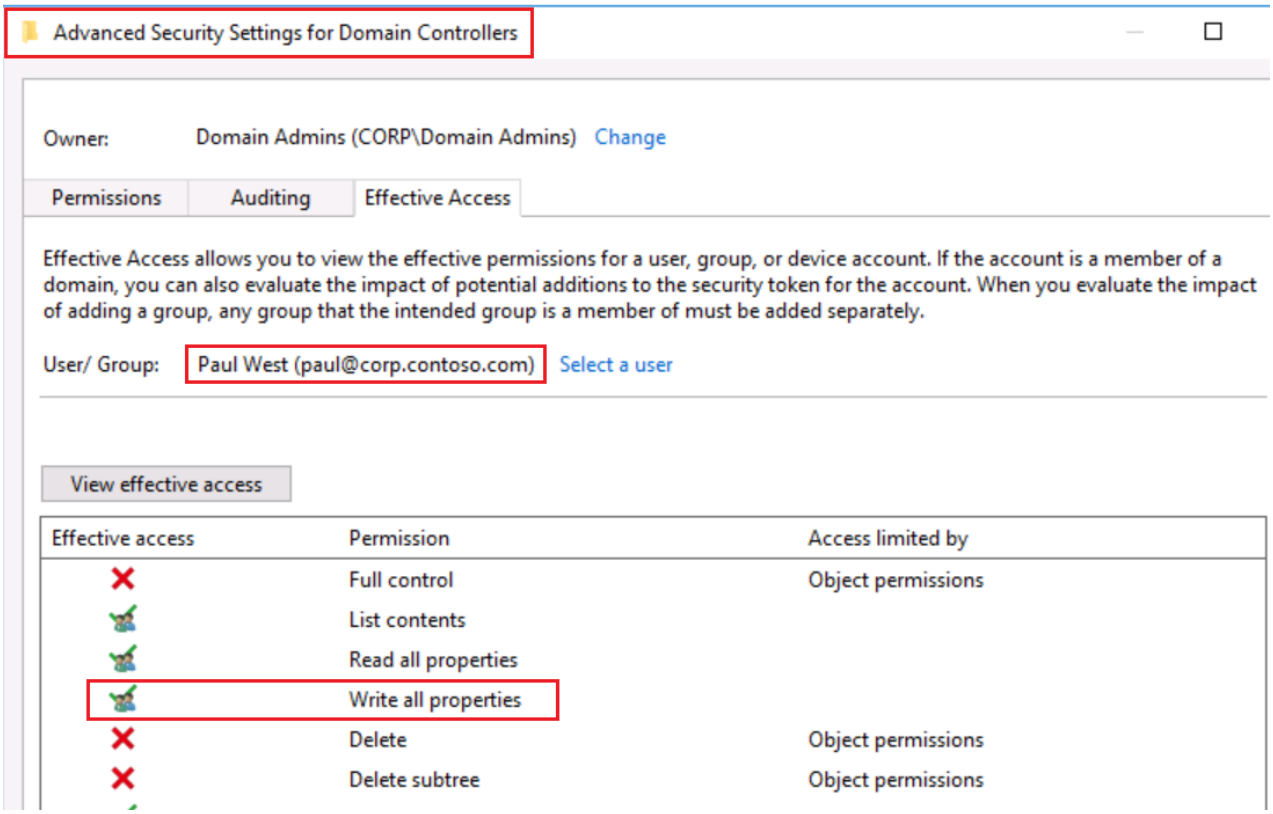
- 3.2 – Manage ACEs set on OU=Domain Controllers

Summary:

ACLs that has been set on the OU of Domain Controllers is a risk, because if an attacker is able to link an arbitrary GPO or disable a GPO. It can weak the security of the Domain Controllers.

This is an example, where **Paul West** has **"Write all properties"** permissions on the OU of the Domain Controllers. **Paul West** can unlink the GPOs that are linked to the OU of the Domain Controllers to weak the security of the DC's.

- Do NOT delegate permissions on the OU of the Domain Controllers
- Look if permissions has been delegated on the OU of the Domain Controllers and remove them ASAP!



- 3.3 – Manage ACEs on Domain Controller Computer Objects

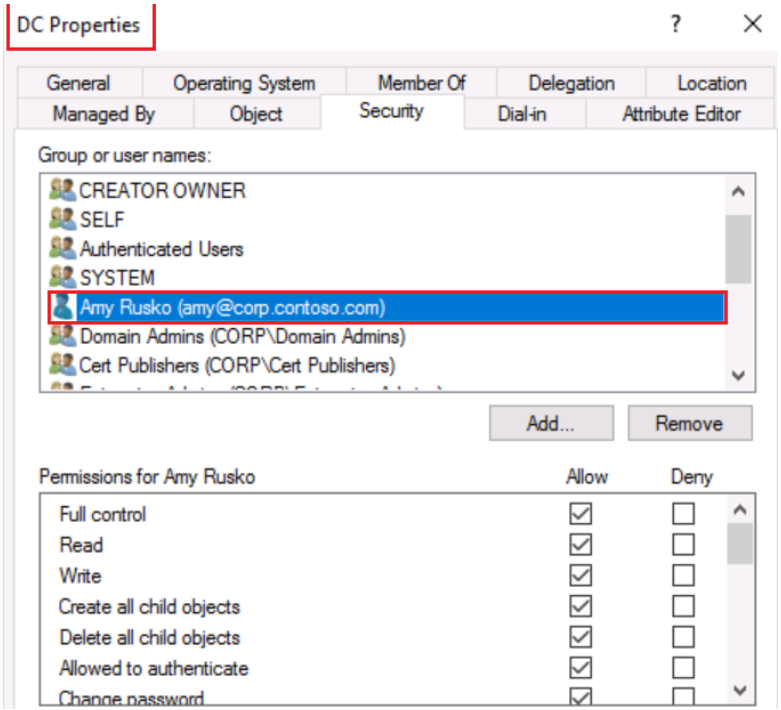
Summary:

Users with ''GenericAll'' or equivalent on the DC Computer Objects can perform a Resource Based Constrained Delegation attack to get code execution on the Domain Controller. For more information to see how this attack path works. Check out https://identityaccess.management/2020/01/17/attacking-active-directory-for-fun-and-profit/

If a user has, the rights to write to the property **''ms-DS-Allowed-To-Act-On-Behalf-Of-Other-Identity''** on the **DC computer object**. It can act on behalf of that service, which is the DC in this example. This gives an attacker the ability to move laterally to the DC and get code execution on it.

Here is an example where we have a user that has ''Full control'' permission on the DC computer object. I have seen this many times, never don't do this. Attackers can now get code executions on the DC if you do this.

- Check for all ACLs that has been set on all the DC Computer Objects and if you discover something like this example. Remove it ASAP. There is no reason to delegate permissions on Computer Objects.



- 3.4 – Manage ACEs of users that are part of Domain Admins or equivalent

Summary:

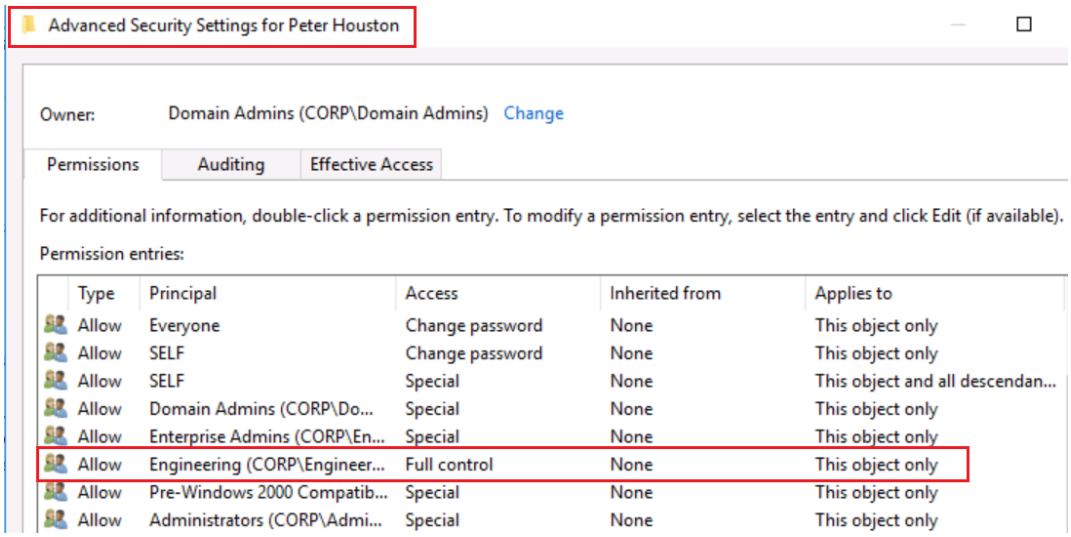
Wrong delegated permissions set on users that are part of Domain Admins is a huge risk, because it means that certain users or groups might be able to take-over an account and become Domain Admin.

Here is an example where we have three users in Domain Admins.

```
PS C:\Users\Mark> Get-ADGroupMember -Identity "Domain Admins"


distinguishedName : CN=Administrator,CN=Users,DC=corp,DC=contoso,DC=com
name              : Administrator
objectClass       : user
objectGUID        : 938584cc-6b6e-46be-b3a7-0da1307720aa
SamAccountName    : Administrator
SID               : S-1-5-21-3566662483-2648771335-1709913503-500

distinguishedName : CN=Mark Hassall,OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com
name              : Mark Hassall
objectClass       : user
objectGUID        : 5e3432fb-336b-4a7b-b3cd-9f6ffb4b2a9c
SamAccountName    : Mark
SID               : S-1-5-21-3566662483-2648771335-1709913503-1103

distinguishedName : CN=Peter Houston,OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com
name              : Peter Houston
objectClass       : user
objectGUID        : e4330610-dcfc-4c68-85c0-68fd2fdfd95a
SamAccountName    : Peter
SID               : S-1-5-21-3566662483-2648771335-1709913503-1104
```

Now when looking at all the ACLs that is set on Peter Houston. There is a group called **"Engineering"** that has **"Full control"** permissions on the user **Peter Houston**.

Everyone from **"Engineering"** can now take-over the account of **Peter** by resetting his password.



Remove all the delegated permissions that has been set on **all** the users in Administrators, Domain Admins, Enterprise Admins, etc. They don't need it.

- 3.5 – Manage ACEs that has been set on AD groups like Domain Admins or equivalent

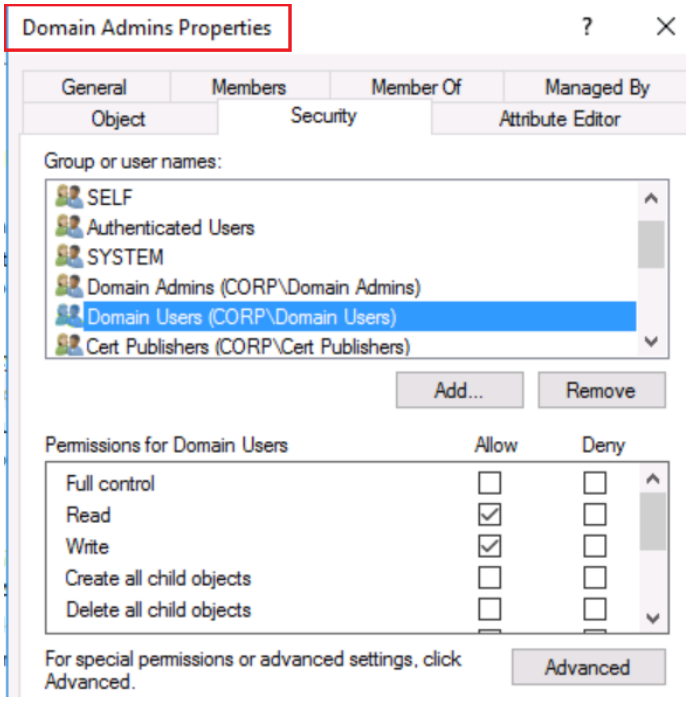
Summary:

AD ACL Scanner can automate this of course, but a quick check is to look, what kind of ACLs that has been on groups like Administrators, Domain Admins and Enterprise Admins.

If an ACL has been delegated on one of these groups, it creates escalation paths for attackers to escalate their privileges to a Domain Admin for example.

Here is an example, where Domain Users has ''Write all properties'' on the Domain Admins, group. Allowing everyone to make themselves a Domain Admin.

- Remove delegated users or groups from Administrators, Domain Admins, Enterprise Admins and equivalent. This creates different escalation paths to Domain Admin.



- 3.6 – Manage ACEs that has been set on the DNS Object

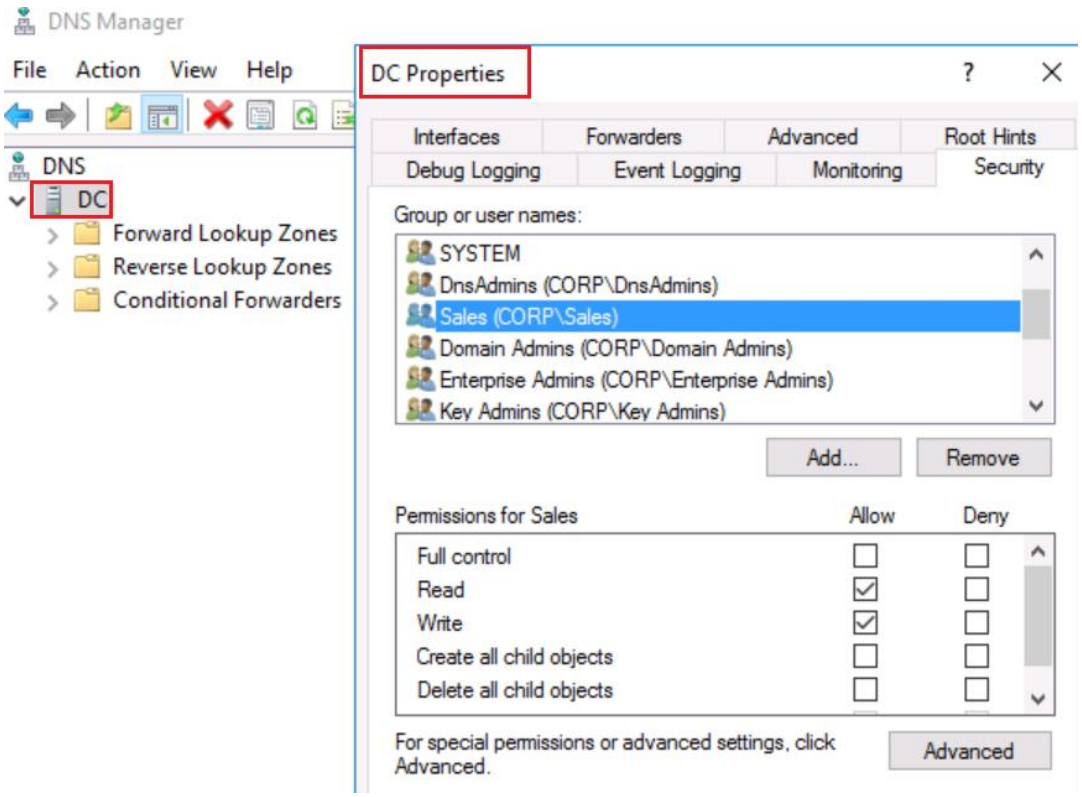
Summary:

By default, Domain Controllers are DNS servers. Security Researchers have discovered a way to execute a DLL as SYSTEM on the DC to escalate privileges to a Domain Admin.

Since DnsAdmins has by default ''Full control'' permission on the DNS Object. Everyone from DnsAdmins can become a Domain Admin.

Here is an example, where the group Sales has ''Write all properties'' permission on the DNS Object, which allows everyone from Sales executing a DLL as SYSTEM on the DC and escalate their privileges to a Domain Admin.

- Users or groups with ''Full control'' or ''Write all properties'' is unnecessary, because nobody needs that amount of rights. It is rarely that someone needs full admin rights on DNS Management. Read permissions on the DNS Object is enough to create DNS records, since ''Authenticated Users'' have ''Create all child objects'' on the FWLZ
- Remove users or groups that have been delegated on the DNS object with ''Full control'' or ''Write all properties'' permission.



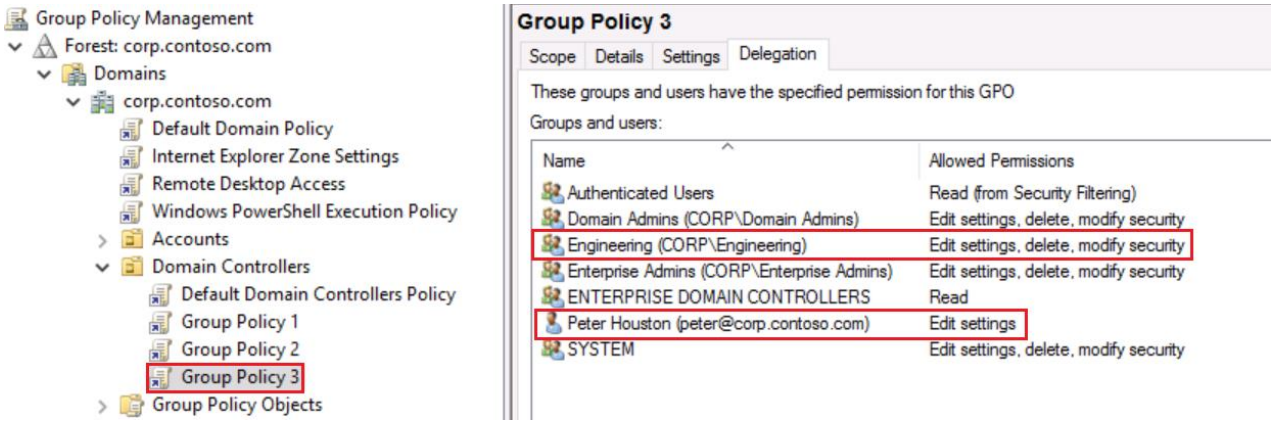
- 3.7 – Manage ACEs that has been set on GPOs linked to Domain Controllers

Summary:

GPOs that are linked to the Domain Controller contains different settings. All of the GPOs that are linked to the Domain Controller needs to be managed from a Tier 0. Do not delegate permissions on these GPOs, because everyone who can edit these GPOs can become a Domain Admin.

Here is an example, where a GPO called **"Group Policy 3"** is linked to the OU of the Domain Controllers, but permissions has been delegated. **Engineering** has full rights and **Paul** can edit the GPO, which means that everyone from Engineering and Paul can become Domain Admin.

- Revoke the delegated permissions on GPOs that are linked to the Domain Controller. All of these GPOs needs to be managed from a Tier 0.



- 3.8 – Manage ACEs that has been set on the Domain Object

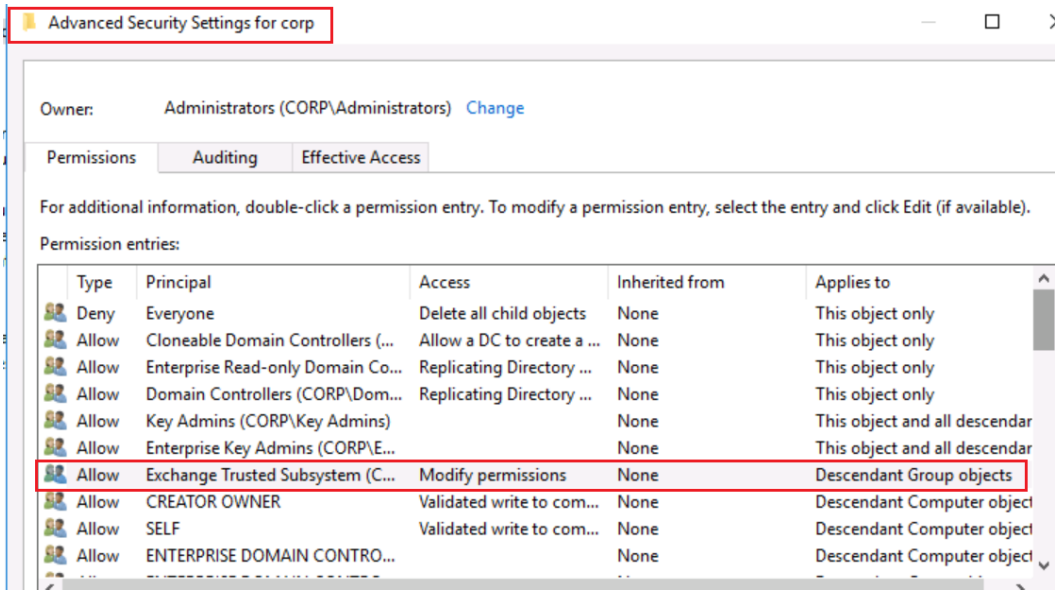
Summary:

Delegating rights on the Domain Object is not something you should consider, because it creates different escalation paths to Domain Admin. I do see it a lot though, where admins decides to delegate rights on the Domain Object by assigning users or groups ''Full control'' permissions, because it makes the job ''easier''

Users with ''GenericAll'' or equivalent can replicate secrets from the Domain Controller and obtain credentials for every user in AD with the likes of the Administrator account.

This is an example that many organizations have in their environment, which are the default, Exchange groups with wide permissions in AD. This group or known as Exchange Trusted Subsystem has ''Modify'' permissions right on the Domain Object and is a member of the group ''Exchange Windows Permissions''

- Exchange Trusted Subsystem and Exchange Windows Permissions don't need to have modify permissions on the Domain Object.
- If you remove ''Modify permission'' from Exchange Trusted Subsystem. A small functionality will break in the Exchange Management Console, which is assigning ''Send as'' permissions to users. This can of be delegated to resolve the problem
- Look if other users and groups have been delegated on the Domain Object and try to see if you can remove them and find another way.



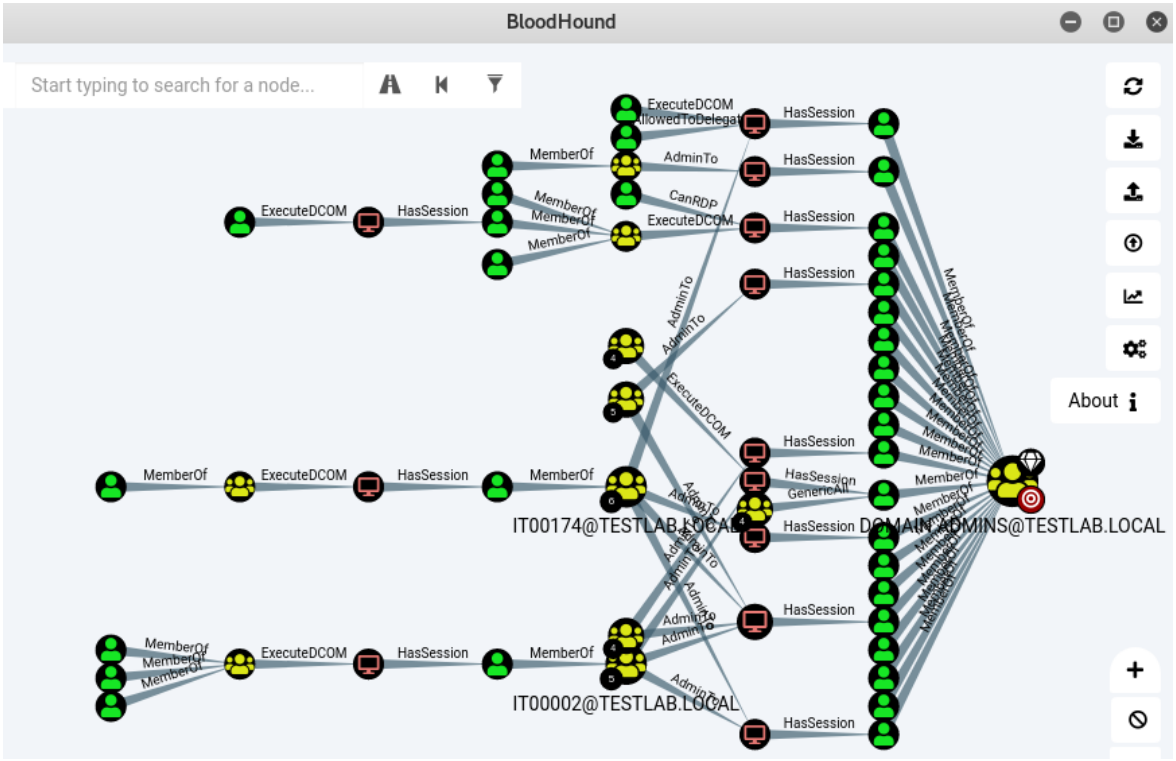
- 3.9 – Run BloodHound

Summary:

BloodHound can find all these ACL/ACEs paths much quicker than looking manually to it and it will probably discover more escalation paths. It is a great tool to discover wrong-delegated permissions in Active Directory.

It looks something like this and I can recommend everybody to use it to secure their AD.

Download BloodHoundAD: https://github.com/BloodHoundAD/BloodHound



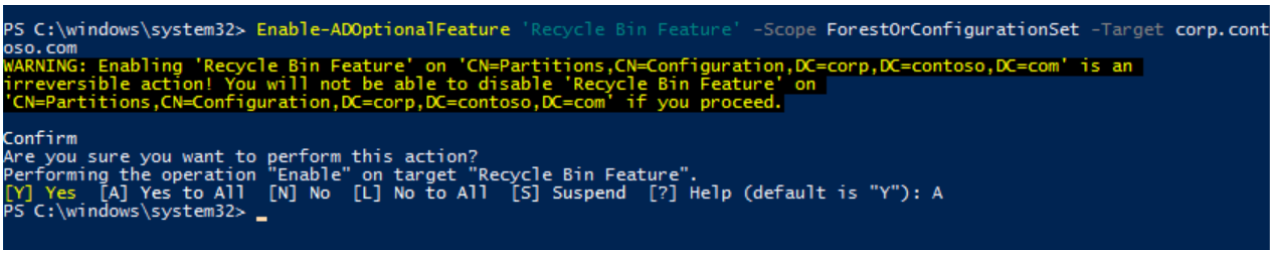
- 4.1 – Enable Active Directory Recycle Bin

Summary:

Accidently deleting an object can be stressful, but good thing is that, there is something called Active Directory Recycle Bin. This feature is not enabled by default, but when enabled. It allows users to restore deleted objects.

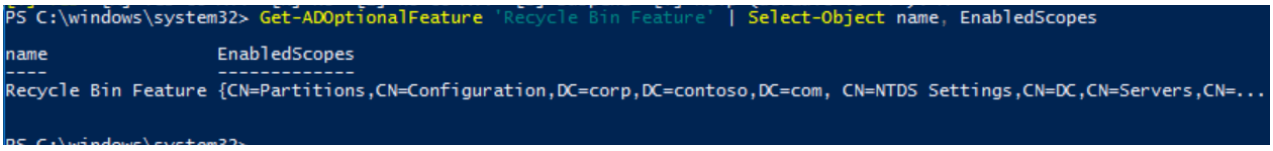
- Enable Active Directory Recycle Bin
- Domain Admin or equivalent can enable it
- Run PowerShell with elevated rights

```
Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet –Target corp.contoso.com
```



- Check if Active Directory Recycle Bin is enabled

```
Get-ADOptionalFeature “Recycle Bin Feature” | select-object name, EnabledScopes
```



- 4.2 - Delegate rights to restore deleted objects

Summary:

Restoring deleted objects requires Domain Admin by default, but this can be delegated to other groups, so DA is not required. Giving unnecessary permissions is a no-go.

- Run PowerShell with elevated rights (DA is required)

```
dsacls "CN=Deleted Objects,DC=corp,DC=contoso,DC=com" /takeownership
```

I have a group in AD that is called ''Tier1'' – I want to delegate this group to have the permissions to restore deleted objects in Active Directory.

- Run the following command

```
dsacls "CN=Deleted Objects,DC=corp,DC=contoso,DC=com" /g CORP\ Tier1:LCRPWP
```

Everyone that is a member of the ''Tier1'' group can now restore deleted objects.

- 4.3 – Do not use legacy built-in groups in AD

Summary:

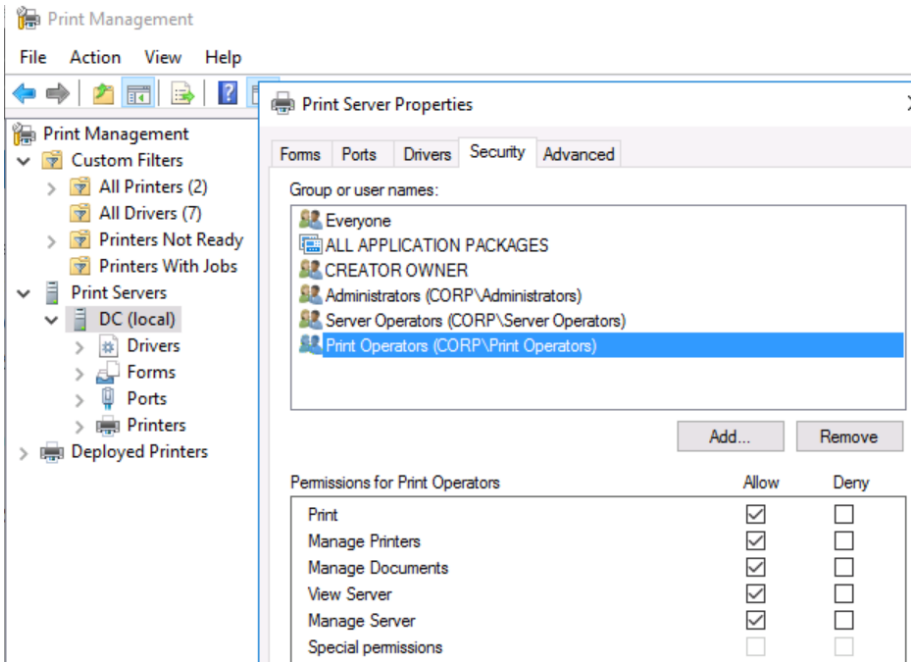
Legacy groups in AD were made in the year of 2003, when security was not a hot topic. Groups with the likes of Account Operators, Backup Operators, Server Operators and Print Operators have more rights than needed, and can escalate their privileges to a Domain Admin.

For more information: https://identityaccess.management/2020/01/17/attacking-active-directory-for-fun-and-profit/

If you have any members in those groups that have been mention. Try to find a way to keep this groups empty. Microsoft recommends keeping Account Operators empty, because it has wide permissions.

> **Note** By default, this built-in group has no members, and it can create and manage users and groups in the domain, including its own membership and that of the Server Operators group. This group is considered a service administrator group because it can modify Server Operators, which in turn can modify domain controller settings. As a best practice, leave the membership of this group empty, and do not use it for any delegated administration. This group cannot be renamed, deleted, or moved.

Print Operators can be empty as well, because all the rights can be delegated for this group. Print Management itself is a part of RSAT.



- 4.4 – Enable SID Filtering

Summary:

SID Filtering is a topic that admins are familiar with when they have to deal with domain migration. When you setup a trust between domains or forest, SID filtering is enabled by default in Windows 2003 or higher. Microsoft introduced SID filtering to mitigate privilege escalation techniques.

An attacker in a trusted domain can modify the SID history for a user, which could grant elevated privileges in the trusting domain.

During an Active Directory migration. A SID History is used for migrated accounts in the trusted domain to get access to resources in that domain, but this only works. When SID Filtering is NOT enabled. This means that if users want to access in a trusted domain. SID Filtering needs to be disabled, and that is why attackers have been leveraging this attack vector.

When SID filtering is enabled, the only SIDs that are used as part of a user's token are from the trusted domain itself. SIDs from other trusting domains are not included. SID filtering makes things more secure

This is an example when SID Filtering is enabled and we want to access the SQL database in a trusted domain. We can't.

- Recommendation

SID Filtering makes things more secure, but it can cause some problems with transitive trust.

When enabling SID filtering. It requires a lot of planning and testing, before you can enable it, if you haven't done it yet.

- Check if SID Filtering is enabled

```
netdom trust contoso.com /domain:fabrikan.com /quarantine
```

- Enable SID Filtering

```
netdom trust <contoso.com> /Domain:<fabrikan.com> /Quarantine:Yes
```

Contoso.com is the trusting domain in this example.

Fabrikan.com is the trusted domain in this example.

- 4.5 – Remove SID History

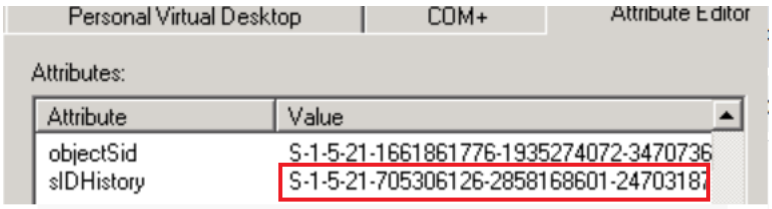
Summary:

MITRE explains it like the following.

"The Windows security identifier (SID) is a unique value that identifies a user or group account. An account can hold additional SIDs in the SID-History Active Directory attribute, allowing inter-operable account migration between domains

Adversaries may use this mechanism for privilege escalation. With Domain Administrator (or equivalent) rights, harvested or well-known SID values may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators."

- Here we can see a **SIDHistory** attribute from a user that has been migrated.



- Identify users with a SIDHistory value

```
Get-aduser -filter * -properties sidhistory | Where sidhistory
```

- Recommendations

After you have enabled SID Filtering. It is recommended to clean the all the SIDHistory attributes in AD.

- Clean-up SIDHistory

```
Netdom trust contoso.com /domain:fabrikam.com /enablesidhistory:No
```

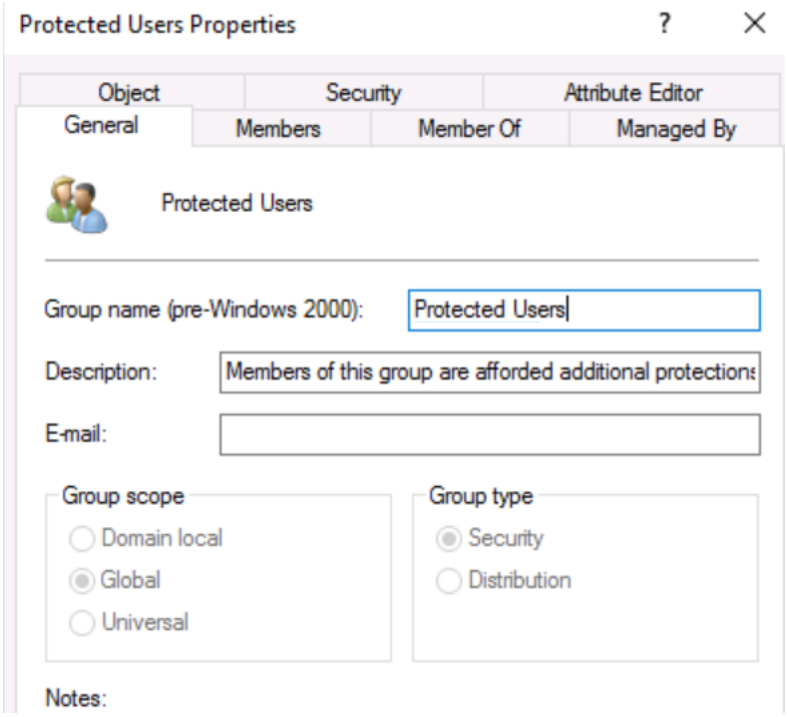
Contoso.com is the trusting domain and fabrikam.com is the trusted domain.

- 4.6 – Tier 0 admins needs to be a member of the Protected Users, group

Summary:

Protected Users is a group that was introduced in Windows Server 2012 R2. The primary idea behind Protected Users is to prevent credentials from being abused when they log in.

A best practice is to add your Tier 0 admins that manage the critical servers like Domain Controllers, Azure AD Connect, ADFS, etc. In the Protected Users group of Active Directory.

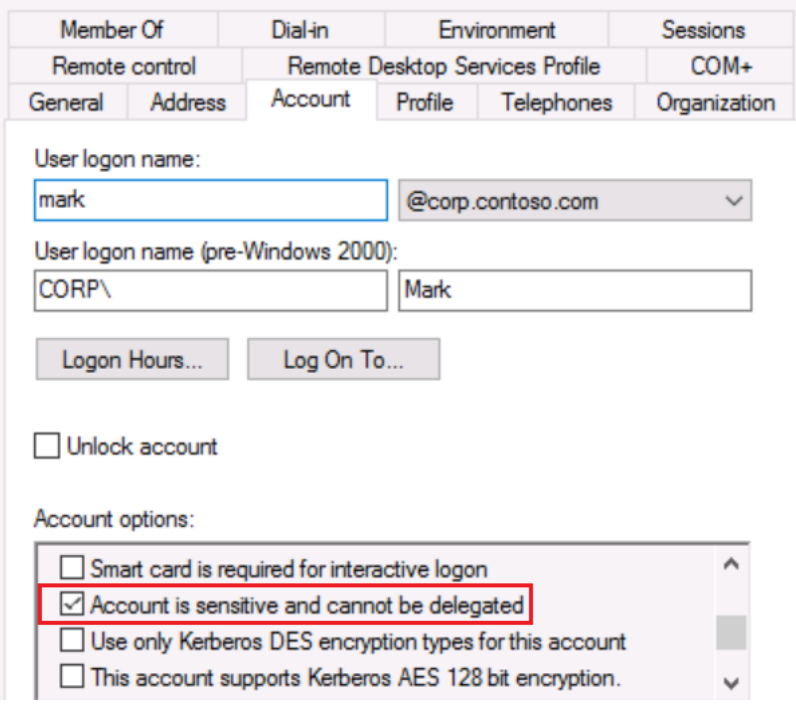


- 4.7 – Tier 0 admins need to have the ''Account is sensitive and cannot be delegated'' checkmark

Summary:

Account is sensitive and cannot be delegated, ensures that an account's credentials cannot be forwarded to other computers or services on the network that supports Unconstrained Delegation.

- Ensure that Tier 0 admins have the ''Account is sensitive and cannot be delegated'' checkmark on.



• 5.1 – Backup and restore plan for DNS

Summary:

Having a backup is one thing, but restoring is the second part. DNS is a critical component in AD and it is important to cover DNS as well in a Disaster Recovery plan for example.

All the backup of DNS needs to be stored securely, like mention before. However, that does not mean, you should store all the back-up data on member servers in AD.

Attackers are going after backup servers and since many organizations manage AD very poorly. It is required to have offline back-ups.

- **Recommendations: Self-Assessment**
- What is our backup procedure for DNS? – Do we make backups every day, week or months?
- Can we confirm that our backup is stored offline as well?
- Have we practice a DNS restore?

- 5.2 - DnsAdmins

Summary:

As mention before. DNS is a critical component in AD, and usually. Users who need to do ''something'' with DNS. Are part of the DnsAdmins group in Active Directory.

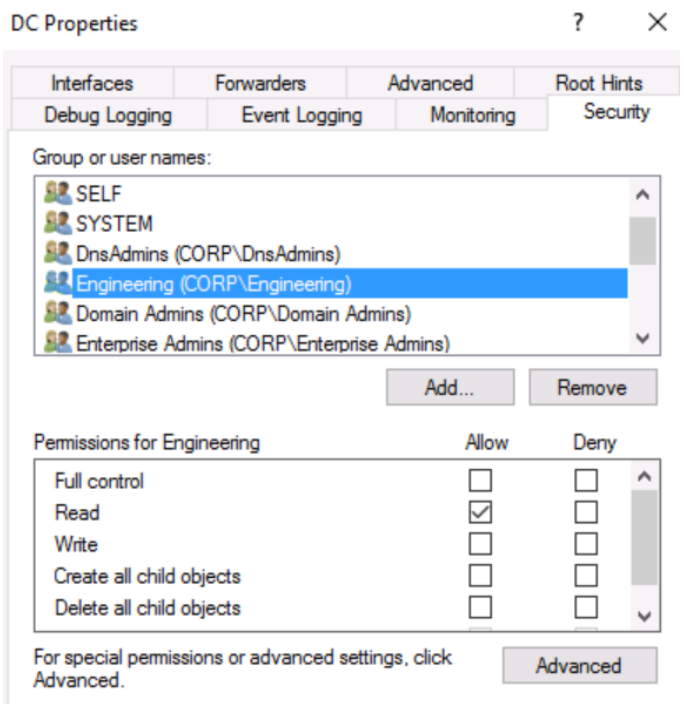
Since this group has elevated rights and often has more rights than needed. It is recommended to keep it very limited.

- **Recommendation:**

DNS Management does not require full DnsAdmins right. Users often need to create some DNS records, and that is it mainly. Because it is rarely, that someone needs to create a new Forward Lookup Zone.

Delegating a group on the DNS Object with only ''Read'' permission is enough. From there they are allowed to create DNS records.

In this example. Engineering is a group that has Read permission on the DNS Object. Everyone in Engineering can now create a DNS record, because by default, Authenticated Users has ''Create all child objects'' on the Forward Lookup Zones.



- 6.1 – Backup and restore plan for DHCP

Summary:

Like DNS, DHCP is also a crucial part to cover as well. Ensure that a backup and restore plan is in place, when restoring a DHCP backup.

Recommendations: Self-Assessment

- What is the backup procedure for DHCP? – Do we make backups every days, weeks or months?
- Can we confirm that we DHCP backups, stored offline?
- When was the last time that you have practiced a DHCP restore?

• 7.1 – Backup and restore plan for AD CS

Summary:

PKI is a Tier 0 component, especially at financial institutions. Having back-ups of PKI and being able to restore is very important.

However, it depends a lot, on what PKI is used for. A proper risk assessment needs to be done on PKI to understand the business value behind it. What happens when an attacker has compromised your PKI?

Recommendations: Self-Assessment

- What is the backup procedure for PKI?
- Are backups of PKI stored offline as well?
- When was the last time that you have restored PKI?

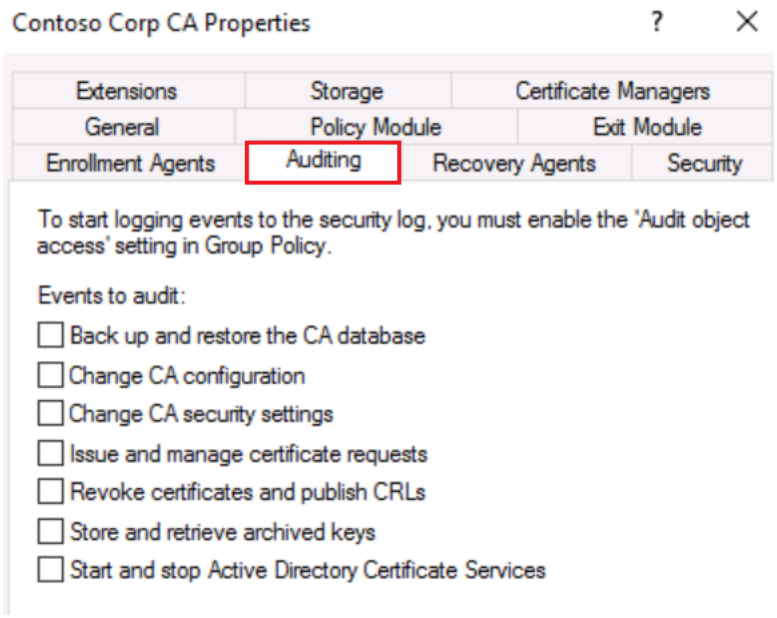
- 7.2 – Enable auditing rules on PKI

Summary:

Enable auditing rules is important, but it depends a lot, on what PKI is used for in the business. A proper risk assessment needs to be done to understand if it is worth to collect AD CS event logs.

In our example. PKI is a critical component for an organization, which means that it needs to be secure at a high-level.

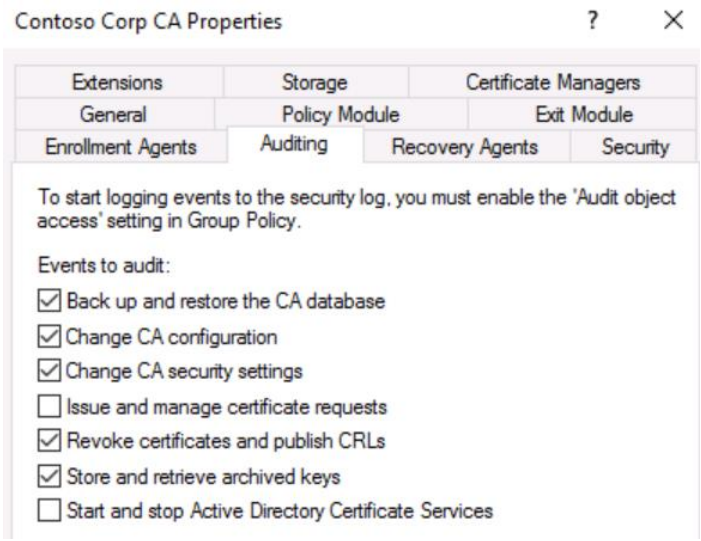
An important aspect is to enable auditing rules to collect visibility.



- Recommendations

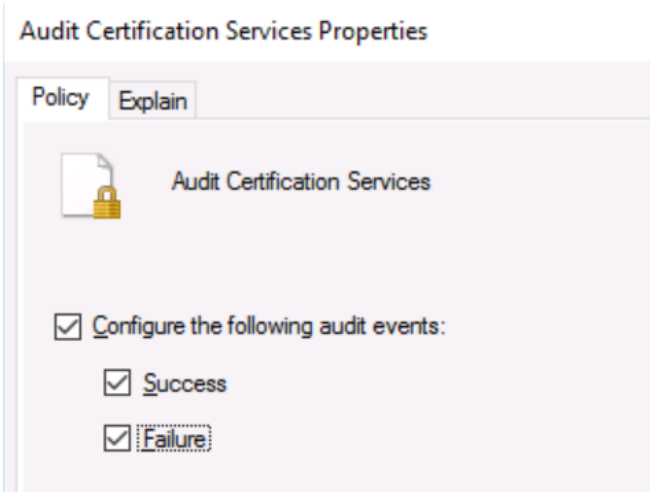
Start with enable the auditing rules, but don't enable all the auditing rules immediately, because it can cause a lot of noise.

1. These are the auditing rules that I would recommend enable



2. Enable the following audit policy at Advanced Audit Policy

- **Audit Certification Services:** Success and Failure



• 7.3 – Monitor relevant PKI event logs

Summary:

After enabling the audit policies at the PKI level. There are different event logs that should form a basic for an organization. All of these event logs might be worth to load in a SIEM solution and monitor it, but as said before. A risk assessment needs to be done on PKI first to understand if it is worth to monitor PKI.

Here are a few examples:

Event ID	Description	Priority
4882	The security permissions for Certificate Services changed	
4890	The certificate manager settings for Certificate Services changed.	
4900	Certificate Services template security was updated.	
4896	One or more rows have been deleted from the certificate database.	
4891	A configuration entry changed in Certificate Services.	
4873	A certificate request extension changed.	
4877	Certificate Services backup completed.	
4879	Certificate Services restore completed.	

- 7.4 – Hardening settings for PKI

Summary:

Create a GPO with the following security settings that needs to be applied on the PKI servers.

- Security Options

Accounts: Administrator account status	Disabled
Accounts: Rename Administrator account	PKIAccount
Accounts: Rename Guest account	PKIGuest
Devices: Restrict CD-ROM access to locally logged on-user only	Enabled
Network Security: LAN Manager authentication level	Send NTLMv2 responses only. Refuse LM & NTLM
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (always)	Enabled

It is understandable if IT Admins are creating a new local Administrator account as their ''break-glass'' account.

- 8.1 – Fine-Grained Password Policies for Service Accounts

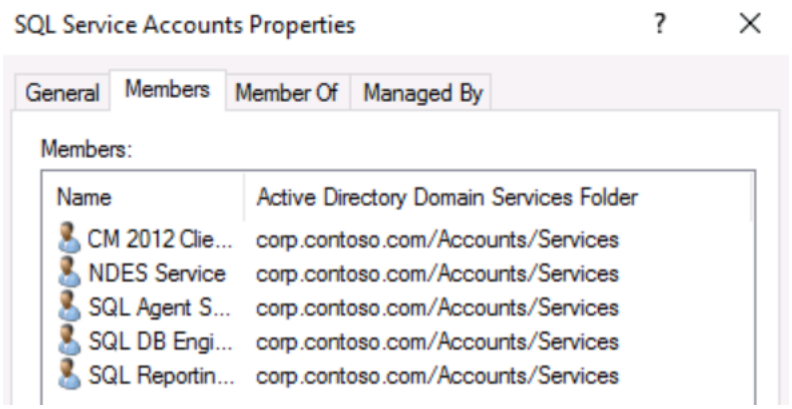
Summary:

Service accounts often have poor passwords, which makes it likely that attackers are going after those accounts. Service accounts are rarely changed, but to enforce that service accounts will have a strong password.

This is an example where I have a few SQL service accounts that I just created.

Name	Type	Description
CM 2012 Client Network Acess	User	Service account used as the network access account for Confi...
NDES Service	User	Service account used by NDES.
SQL Agent Service Account	User	Service account used to run SQL Server 2012 Agent service
SQL DB Engine Service Account	User	Service acount used to run SQL Server 2012 database engine
SQL Reporting Service Account	User	Service account userd to run SQL Server 2012 reporting services

All the service accounts are part of the SQL service accounts group.



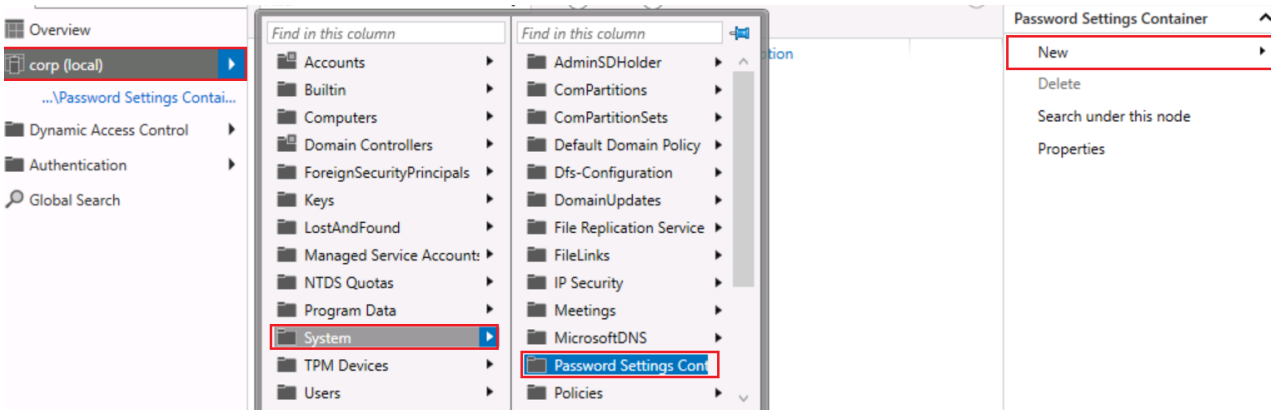
It is recommended to enforce them having a strong for service accounts, but we had great features like Managed-Service accounts. Unfortunately, not all of those service accounts were able to support it.

- Recommendation

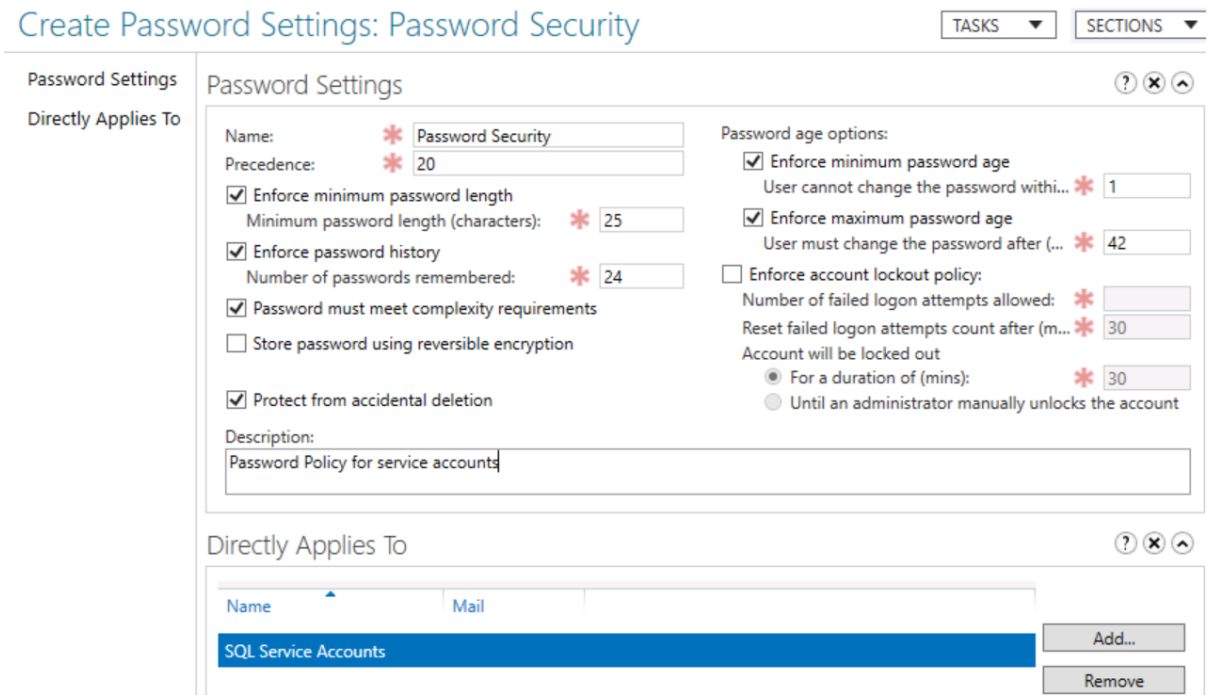
Start with enforcing service accounts having at least a 20 long character as a password.

Open **Active Directory Administrative Center** and follow the instruction below:

- Click on corp (local)
- Click on System
- Click on Password Settings Container
- Click New

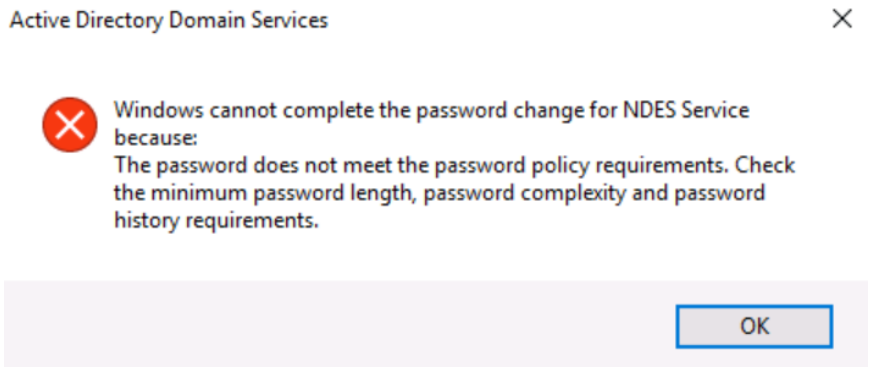


Here I am configuring the password settings for the service accounts.



Now when resetting a service account that is part of the SQL Service Accounts group, and you have picked a poor password. It will be denied.

Every time, when an account is part of the ''SQL Service Accounts'' group. Password settings will be applied to the account.

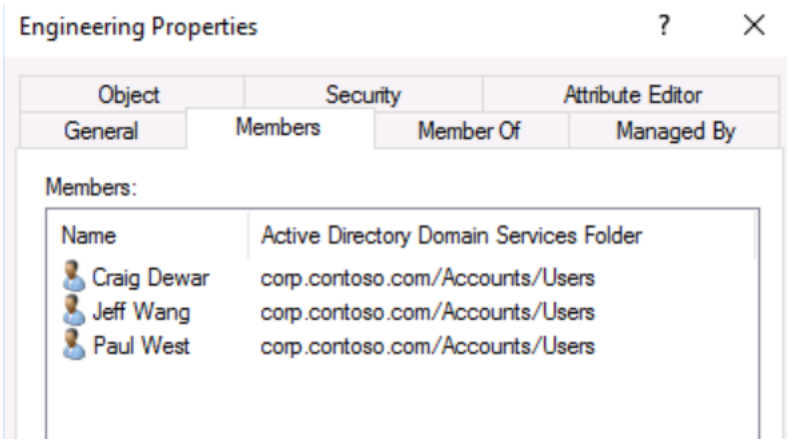


- 8.2 – Fine-Grained Password Policy for IT Admins

Summary:

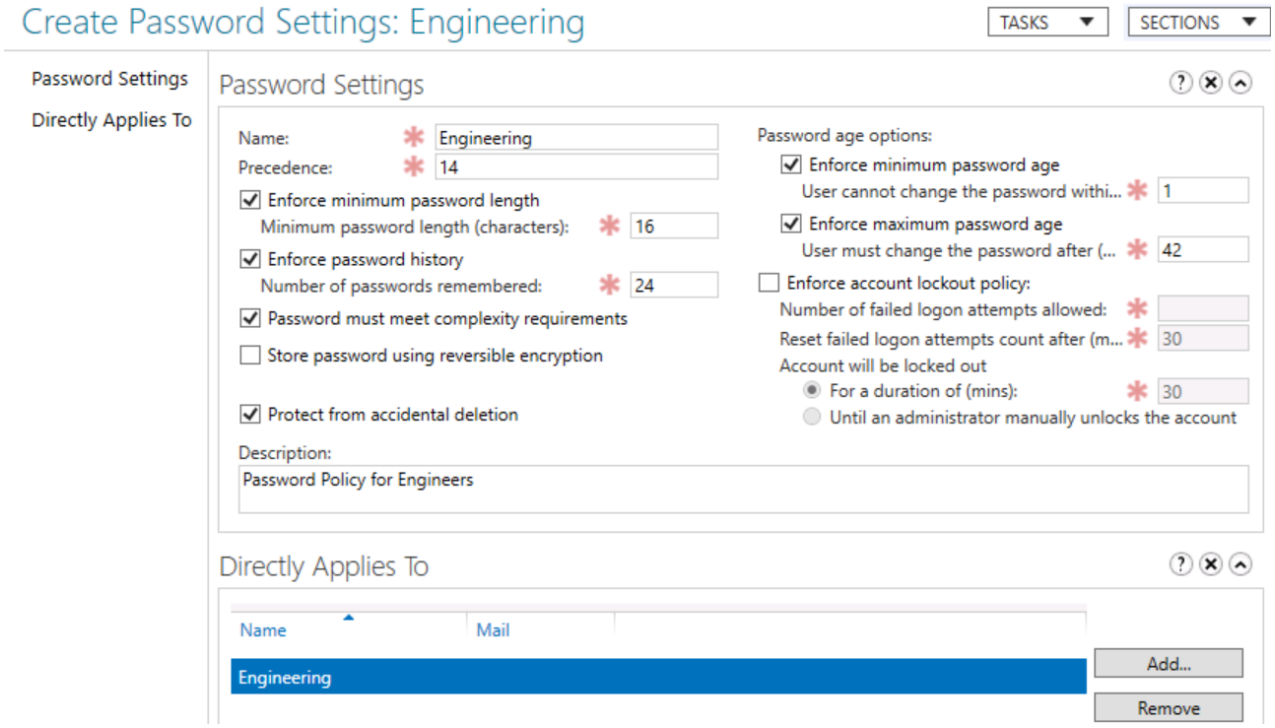
High-privileged users in a Windows network, which are usually IT Admins. Need to have a strong password as well. Creating a fine-grained password policy for those accounts with a minimum of 14-16 character would be great.

In this example. I have three members in the ''Engineering'' department. All of them have access to lots of systems in the network, and I want to be sure that they have a strong password.



- Recommendation

Create a Fine-Grained Password Policy for IT Admins with the goal to enforce a longer password.

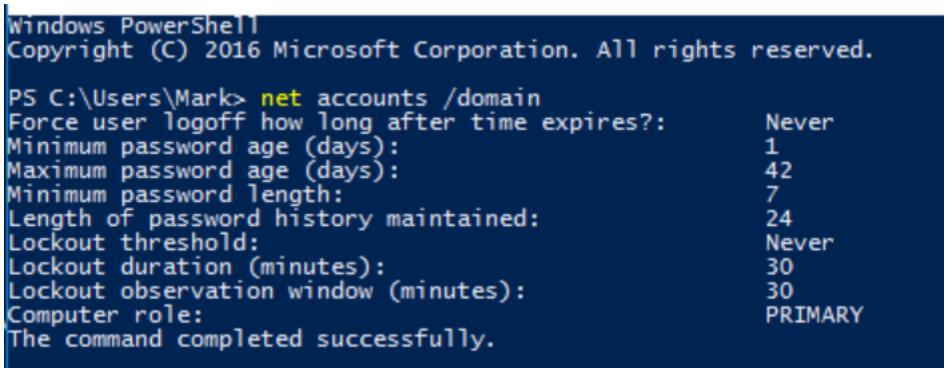


- 8.3 – Upgrade Default Password Policy

Summary:

Default Password Policy in AD makes it much easier for attackers to perform Password spraying attacks to obtain credentials.

A default password policy is often around 7-8 characters. Up to you to increase the password policy to something like at least 12-14 characters.



- 9.1 – Accounts with SPN in Domain Admins

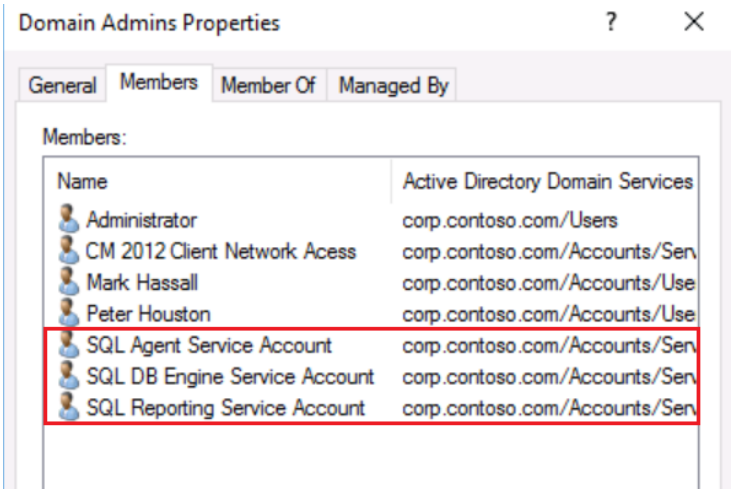
Summary:

Accounts that have a SPN and are a member of Domain Admins group or equivalent is a huge risk. Every attacker is able to request a service ticket from that SPN account and is able to export those tickets, and crack it offline.

Service accounts are everywhere. It is difficult to give clear in-depth details on what groups you should check, because you might have custom-delegated groups with service accounts in it.

Start with looking if you have accounts with a SPN in groups like Administrators, Domain Admins, Enterprise Admins, Account Operators, DnsAdmins.

- This is a common example, where we have a few SQL service accounts in Domain Admins.



Service accounts are rarely changed, so it is not a surprise if an attacker is able to crack that password very easily.

```
PS C:\Users\Mark> net user SQLAgent /do
User name                    SQLAgent
Full Name                    SQL Agent Service Account
Comment                      Service account used to run SQL Server 2012 Agent service
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/18/2017 12:04:29 PM
Password expires             Never
Password changeable          1/19/2017 12:04:29 PM
Password required            Yes
User may change password     Yes
```

- Recommendation

(Service) Accounts with a SPN, should never be a part of the Domain Admins group. Vendors are often requiring this, but why do you want this actually?

Every Domain Admin is a risk more for an organization. There is no reason to assign someone Domain Admin, rights.

Try to contact your vendor to understand what rights it needs. Besides of that, stop accepting vendors requiring Domain Admins, right. Push back. Don't make any deals with them.

Domain Admins is only required for the following tasks:

- Raise Domain Functional Level
- Promote a Domain Controller

All the other rights can be delegated.

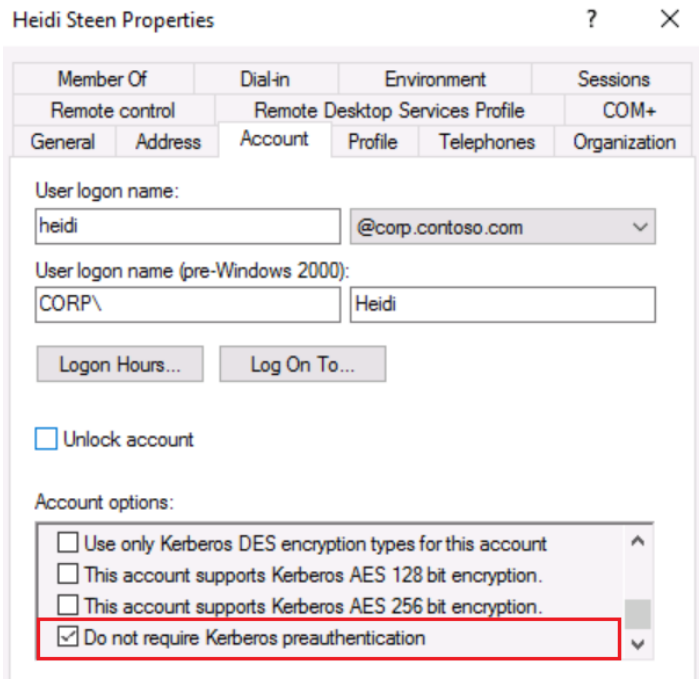
- 9.2 – Accounts with Pre-Authentication disabled

Summary:

When pre-authentication is disabled. Every person on the network is able to request authentication data, so the KDC will return an encrypted TGT, which can cracked offline.

Usually this feature is set on service accounts for compatibility reasons.

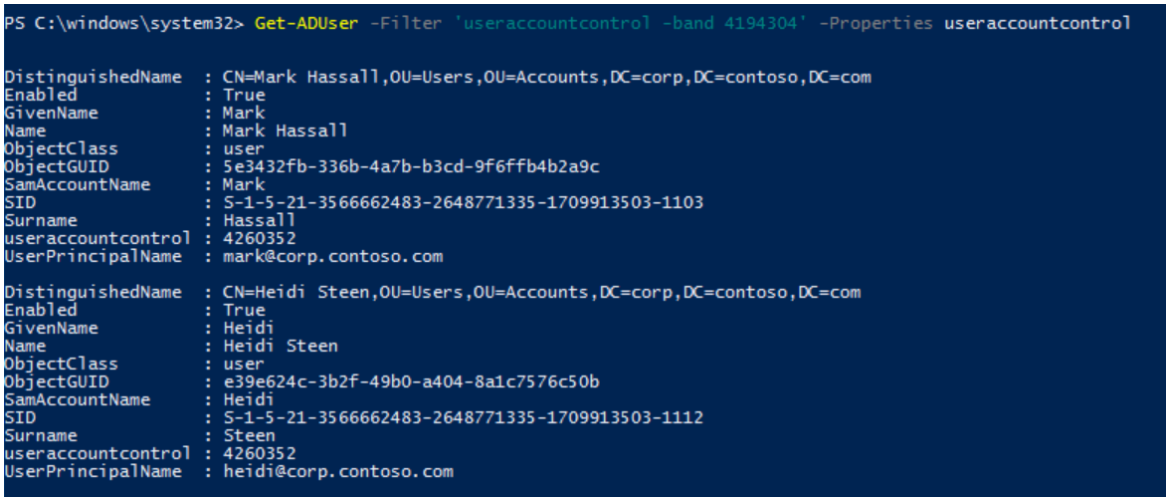
- Here is an example where we can see that an account has pre-authentication disabled.



- Recommendations

First thing is to get an overview of all the accounts that have pre-authentication disabled.

```
Get-ADUser -Filter 'useraccountcontrol -band 4194304' -Properties useraccountcontrol
```



The second part is to look if those accounts are still in use, if not. Disable them, and later on. Delete them. This setting is usually set on service accounts, but if pre-authentication is disabled on a regular user account. It is a finding.

- 9.3 – Servers with Unconstrained Delegation

Summary:

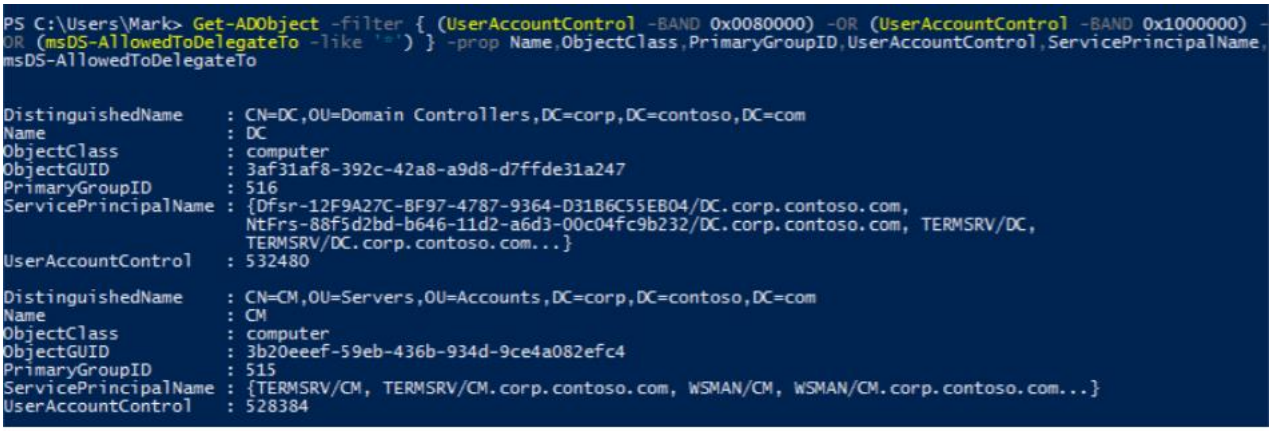
Unconstrained Delegation gives the ability to a service to impersonate a user to every other Kerberos services on the network.

The risk behind Unconstrained Delegation is that when a user signs into a server with Unconstrained Delegation. A TGT of the user will be attached with TGS to represent it later to the service, so when a user access the server. TGT will extracted into the memory and the service will be able to impersonate the user to every Kerberos services.

This is a serious risk, and Microsoft has recommended. Never ever use this kind of configuration again.

- Find servers with Unconstrained Delegation

```
Get-ADObject -filter { (UserAccountControl -BAND 0x0080000) -OR (UserAccountControl -BAND 0x1000000) -OR (msDS-AllowedToDelegateTo -like '*') } -prop Name,ObjectClass,PrimaryGroupID,UserAccountControl,ServicePrincipalName,msDS-AllowedToDelegateTo
```



- Recommendation

Servers with Unconstrained Delegation are dangerous, but they have configured from ten years ago. In that time, security was not a huge topic.

- Tier 0 admins needs to be part of the Protected Users group in AD and the ''Account is sensitive and cannot be delegated'' checkmark needs to be enabled.
- Limit, but also monitor the local Administrators group on the Unconstrained Delegation servers.
- Try if possible. Limit as much as connection to the Unconstrained Delegation servers.
- Block internet access on Unconstrained Delegation servers

- 10.1 – Ensure AdminSDHolder is in a clean state

Summary:

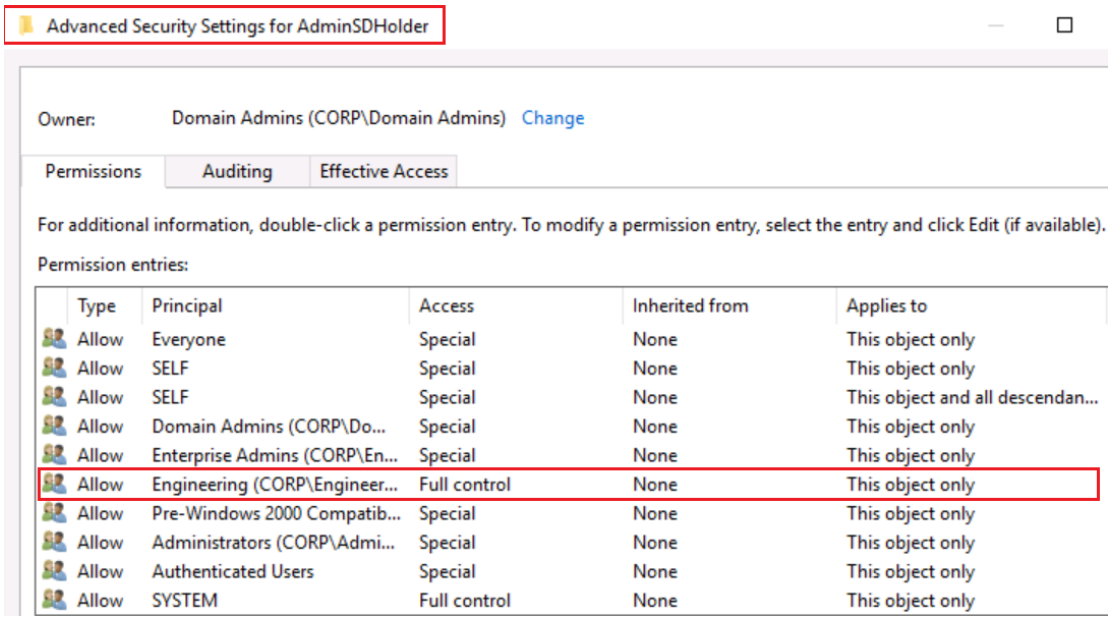
AdminSDHolder is a container inside active directory that maintains a master list of permissions for objects that are members of privileged groups (AdminCount=1) in active directory.

Every hour, there is a mechanism called an ''SDProp'' that will compare the permissions of an account that is part of a high-privileged group with the likes of Domain Admin to the security permissions of the AdminSDHolder.

If an attacker or an insider is able to modify the ACL of the AdminSDHolder. All the permissions will be applied on the protected objects, which gives an attacker a sort of ''persistence''

I can guarantee that I see this a lot in environments.

- Here is an example where ''Engineering'' has been ''Full control'' permissions on the AdminSDHolder container



- Recommendations

Be careful when delegating permissions on the AdminSDHolder container. Users or groups with ''Full control'' or ''Write all properties'' and equivalent, creates escalation paths to all the high-privileged groups in AD.

It is recommended to keep the AdminSDHolder in a clean state, which means that no users or groups should been delegated on the object.

- 10.2 – Create fake service account to detect Kerberoast

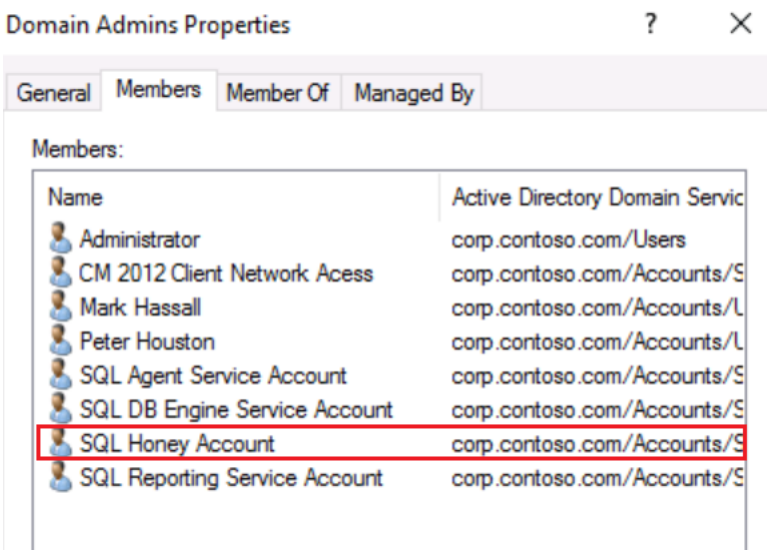
Summary:

Every (service) account that contains a SPN is actually at risk, because every authenticated user has the rights to request the service ticket from that account and crack it offline.

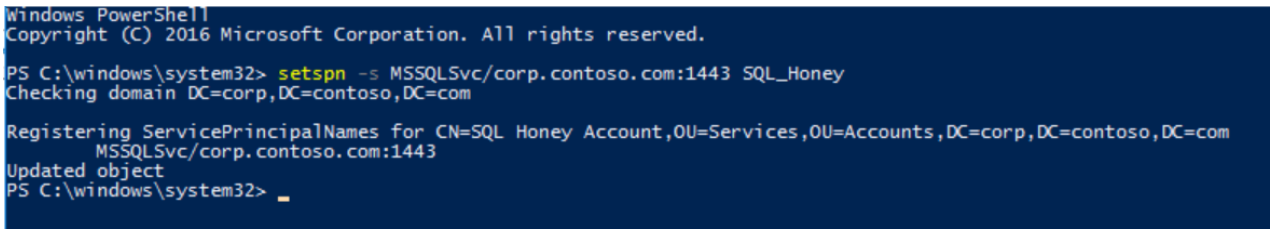
It is not here to sell you FUD, but to make you aware how easy it is nowadays. Which is also why service accounts need to have a strong password with at least of 20 characters.

A great way to catch an attacker is to create a fake service account that contains a SPN.

- Here is a fake service account in Domain Admin.



- A fake SPN has been assigned to the service account

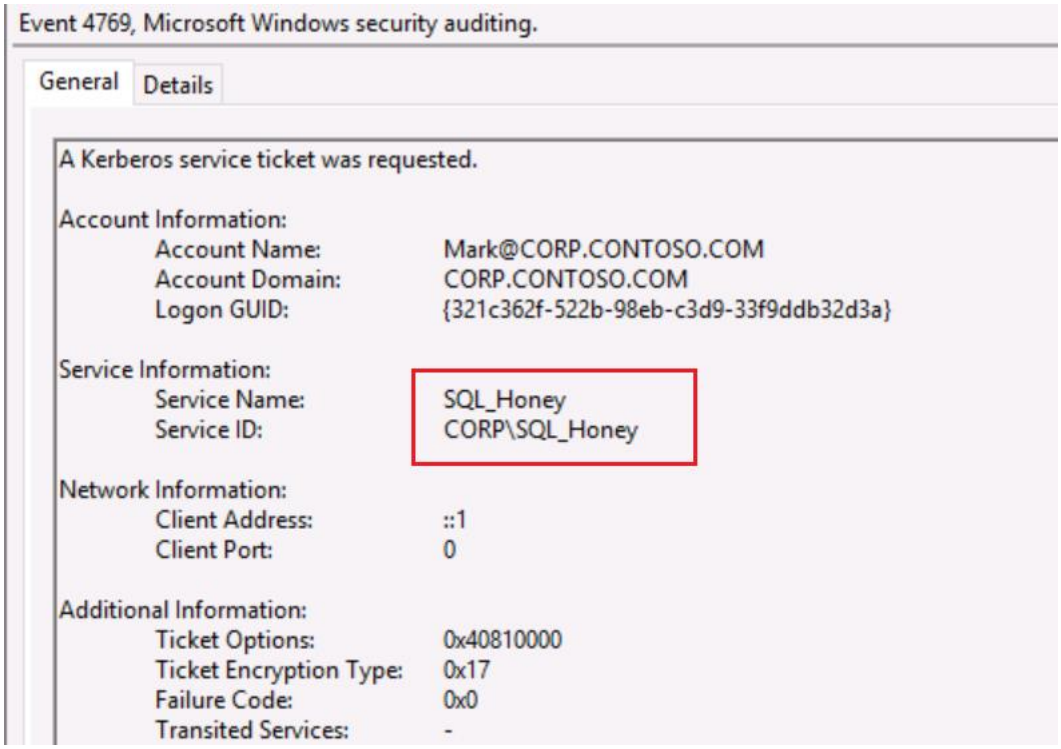


- Recommendations

Now when someone is requesting a service ticket from this SQL_Honey account. An event log will show up in the Security logs. Since this fake service account maps to nothing. An alert should go off.

```
PS C:\windows\system32> Add-Type -AssemblyName System.IdentityModel
PS C:\windows\system32> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/co
rp.contoso.com:1443"


Id                   : uuid-235881d6-d654-47c2-99e5-5969304c53ad-1
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 1/27/2020 8:28:11 AM
ValidTo              : 1/27/2020 6:16:49 PM
ServicePrincipalName : MSSQLSvc/corp.contoso.com:1443
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

Event 4769 on the Domain Controllers with all the additional information.



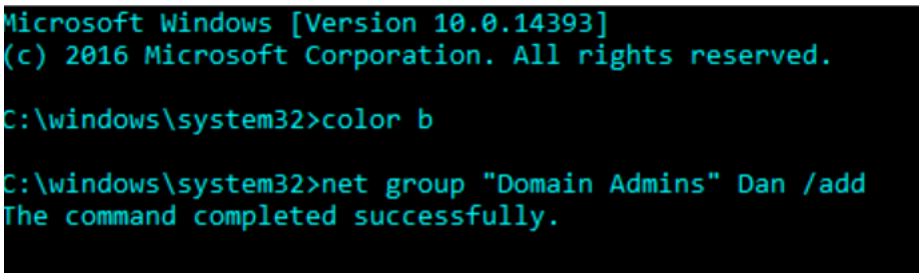
- 10.3 – Monitor high-privileged groups

Summary:

Monitoring high-privileged groups is necessary to keep an eye on privileged abuse. There are people who like to take the short road, which is adding random service accounts to groups like Domain Admins for example.

Since we know that adding service accounts to high-privileged groups is insecure. We need to ensure that we have alerts on this.

- User ''Dan'' has been added to the Domain Admins, group.



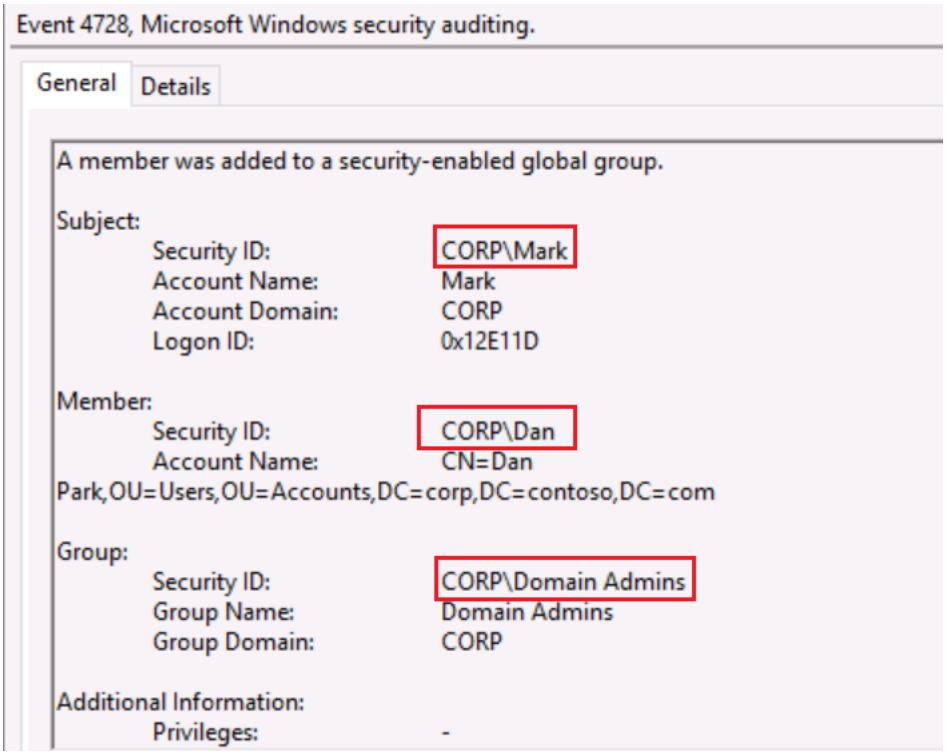
Is there an alert going off if this is happening?

- Recommendations

Monitor the following security event log and make sure bells are going to ring, when this occurs.

Event ID	Description
4728	A member was added to a security-enabled global group

- Mark added Dan to the Domain Admins, group.



- 10.4 – Event logs to monitor

Summary:

Relevant event logs from the Domain Controller that needs to be monitored. No need to filter anything, but just monitoring on the event ID, itself.

Event ID	Description
1100	The event log service has shutdown
1102	The audit log was cleared

Event ID	Description
4704	A user right was assigned
4705	A user right was removed

Event ID	Description
4715	The audit policy (SACL) on an object was changed
4719	System audit policy was changed

Event ID	Description
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group

Event ID	Description
4771	Kerberos pre-authentication failed
4772	A Kerberos authentication ticket request failed
4773	A Kerberos service ticket request failed

Event ID	Description
4780	The ACL was set on accounts which are members of administrators groups

- Recommendations

Start with collecting the above event logs and create priorities for them. If done, try to find a solution to forward all those event logs to a central point, like a SIEM.

The following security event logs might be value as well:

Event ID	Description
4742	A computer account was changed

Event ID	Description
4946	A change has been made to Windows Firewall exception list. A rule was added
4947	A change has been made to Windows Firewall exception list. A rule was modified

- 11.1 – Deploy Microsoft Administrative Tier Model

Summary:

Microsoft has developed a model with the name ''Administrative Tier Model'' and it is a great way to mitigate credential theft.

Domain Admins were usually login into multiple lower trusted servers and workstations, which means that they exposed their credentials in memory. Since then, a model has been introduced to mitigate these kind of attacks, which only allows Domain Admins or known as Tier 0 admins logon critical servers (Tier 0 servers), with the likes of Domain Controllers, Azure AD Connect, ADFS, PKI, NPS, etc. These are usually the Tier 0 servers

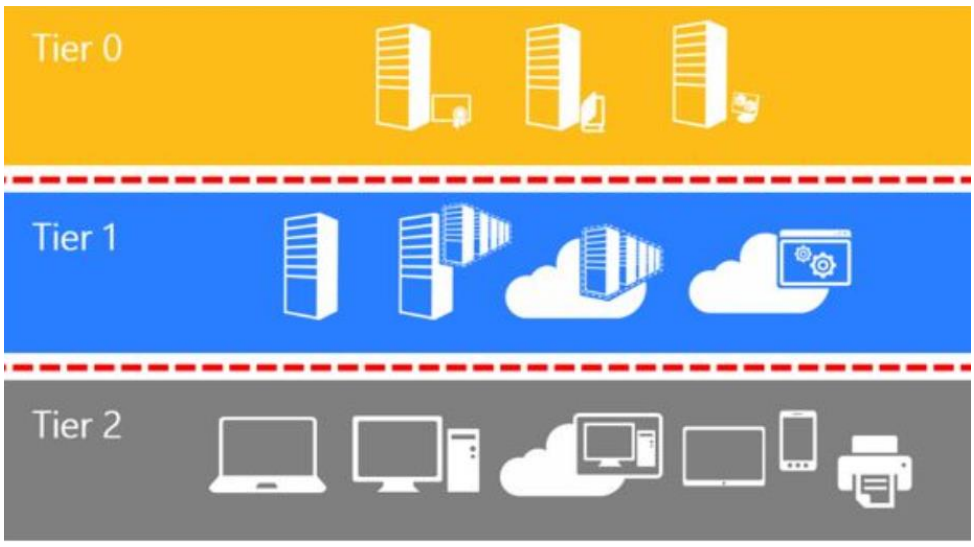
Administrative Tier Model exist with three layers, which are Tier 0, Tier 1, and Tier 2.

Tier 0 contains servers like Domain Controllers, Azure AD Connect, ADFS, PKI, etc. Domain Admins or equivalent are usually the one's, who are managing these servers.

Tier 1 contains important servers, but not critical. A few examples are SQL Servers, File servers, Print Servers, etc. Tier 1 are usually the server admins.

Tier 2 contains workstations. Tier 2 admins are usually the helpdesk / workstation admins that are taking care of workstations. They help to troubleshoot problems, when someone is calling the desk.

All of the Tier admins can only logon their own ''Tier zone'', so for example. Tier 0 admins cannot logon Tier 1 servers or Tier 2 workstations, and vice versa.



- Recommendation

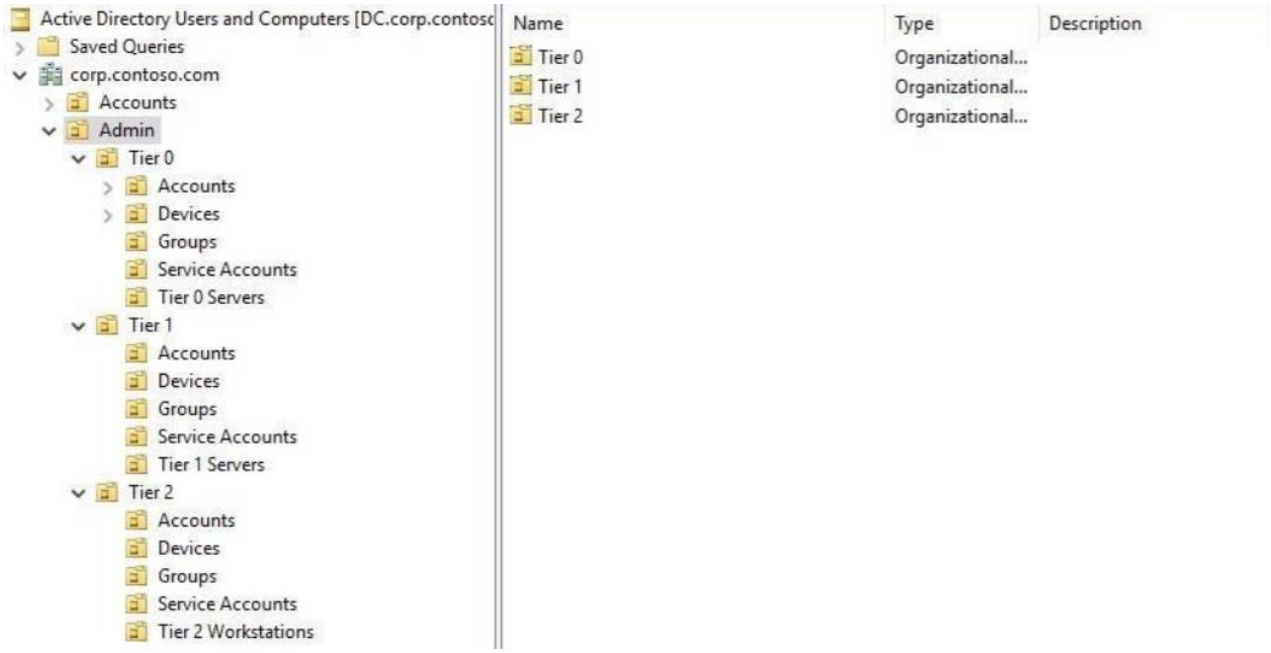
Deploying MS Administrative Tier Model can take some times, because it requires testing and planning, but this does not mean you shouldn't implement it.

- How does it looks like?

We created a bunch of OU's with all the right objects in it, and the second important part is to use Group Policy to deny logon access.

- <u>Example</u>

Tier 0 admins are not allowed to logon Tier 1 & Tier 2 their zone, so a Group Policy needs to be in place to deny logon access through User Right Assignment.



- 11.2 – Define which assets belong to Tier 0

Summary:

Define which assets belong to Tier 0 has always been misunderstanding. Usually people thought it would be just the Domain Controllers, but this is a misconception.

Tier 0 servers are the most critical servers in an organization. If one of those servers would be compromised. It would have immediately business impact.

Here are a few examples on servers that needs to be managed from a Tier 0

- Domain Controllers
- Azure AD Connect
- ADFS
- PKI

There is a huge chance that those servers are not only one, because you might have other critical servers as well, which means. A risk assessment needs to be done to define if there are other servers that needs to be managed from a Tier 0. A simple example is to ask yourself the following question: *''If server X goes down. Can business still go further?''*

- Risk Assessment

This is an example, but I recommend you to do this kind of risk assessment as well to have a better understanding of your Tier 0 assets.

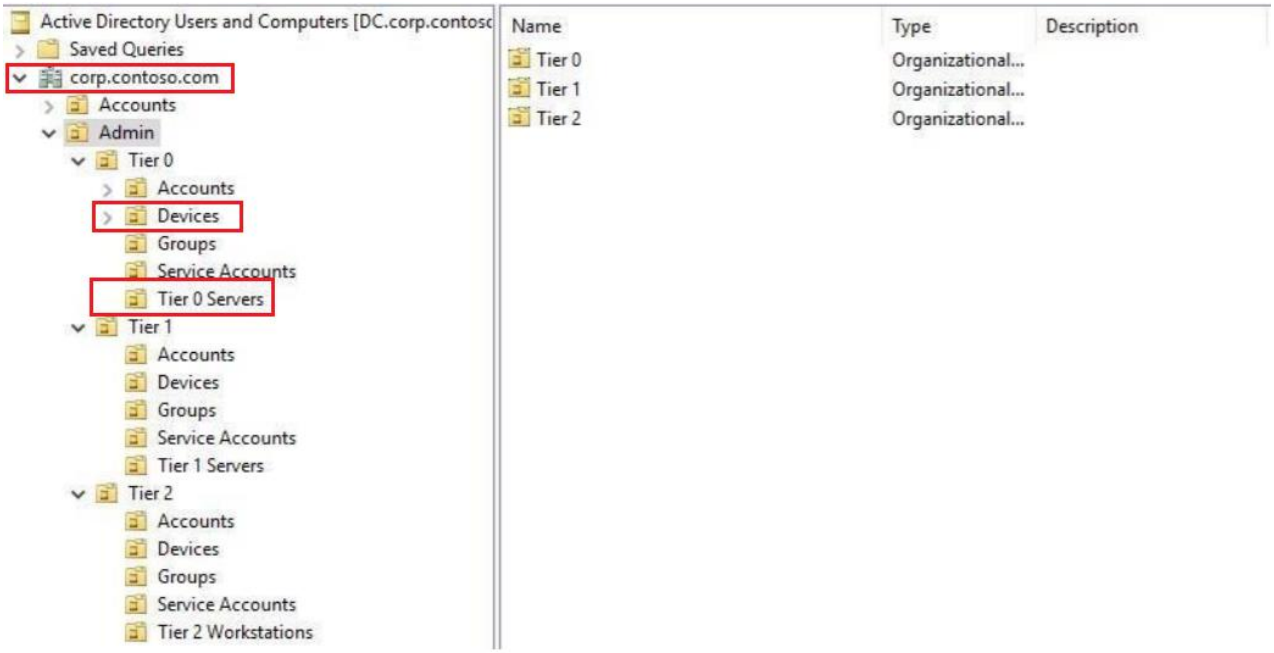
Server	**Description**	**Business Impact**
Domain Controller	Handles authentication for users in a Windows network	Management would probably run with their hair on fire if all the DC's were down or compromised.
Azure AD Connect	Responsible for synchronizing passwords to Azure	• Attacker can leverage to Azure AD Connect to obtain Domain Dominance • Escalate privileges to AAD permissions of the Sync account in Azure

- 11.2 – Manage GPOs in a Tier Model

Summary:

GPOs that are linked to Tier 0 assets needs to be managed by Tier 0 admins as well or otherwise potential privilege escalation might occur. It is very common to see that organizations have some sort of Tier Model in place, but there might be misconfigurations in place, which allows someone from Tier 1 escalating privileges to a Tier 0 asset.

- Here are all the Tier 0 assets that have been marked with red.



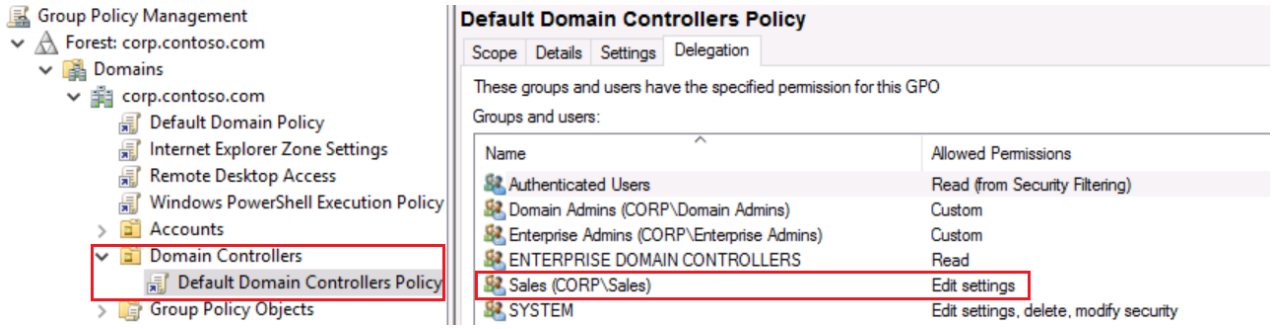
- GPOs of Tier 0 admins

All of this needs to be managed by Tier 0 admins.

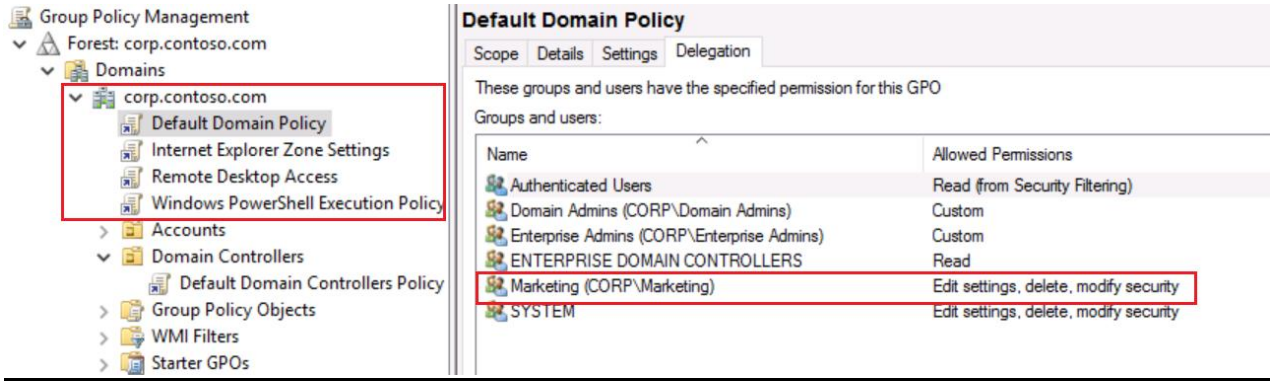
Domain Policy	Tier 0
OU=Domain Controllers	Tier 0
OU=Tier 0 servers	Tier 0
OU=Tier 0 devices	Tier 0

- Recommendation

- Example 1



- Example 2



All the Group Policy Objects that are linked to any Tier 0 asset, needs to be managed from a Tier 0 operations. Otherwise, escalation paths are possible if you do not manage your GPOs well.