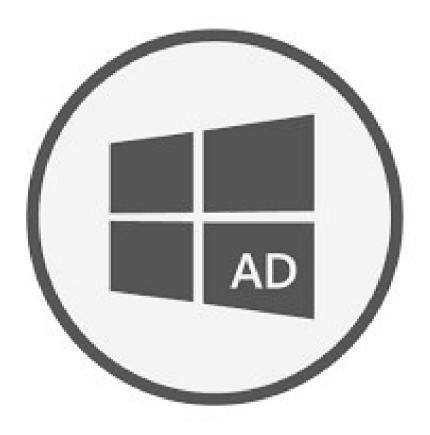
Active Directory Security Fundamentals



Author	Huy Kha
Contact	Huy_Kha@outlook.com

Summary

This document provides guidance to organizations on how they can secure their Active Directory. This includes making backups, delegating rights, designing MS Administrative Tier Model, etc.

Not everyone can afford expensive consultants, so I decided to work on a document that doesn't cost you any money, but it requires some effort on your side to work towards this document. Because this doc will guide you 'hands-on' through the different steps you need to take, to mitigate the risk of being compromised.

Foreword

Active Directory is often managed poorly and IT managers are often very incompetent, but that is not a surprise anymore.

A lot of targeted ransomware attacks are leveraging through Active Directory and most organizations aren't even looking how their own AD environment is set-up.

AD has always been placed at the IT Operations teams, and all of them often have the freedom to manage it the way, how they like it. Because nobody really cares about AD, until they end up the like the following:

given the to go wording story of your private and a consecution of your private and you consecution of your private and you will be the your private and the young of the your private and a consecution of the standard of your private and a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your private and you will be a consecution of the your pr

Hydro Hit by LockerGoga Ransomware via Active Directory
BankInfoSecurity.com - 20 mrt. 2019

Aluminum giant Norsk Hydro has been hit by an attack that appears to have ... by a supplementation of the first the first that the first that

Norsk Hydro cyber attack: What happened?

Help Net Security - 20 mrt. 2019

Alle bekijken

If you have an Active Directory, which most organizations do. Can your business still go further when AD is down for 5 days?

Like I said before. It is often managed very poorly, and yes. Also your managedservices might not do a great job.

Are you aware what kind of insecure changes are made in AD? Like for example adding service accounts with poor passwords to Domain Admin?

Who manages the high-privileged groups in AD with the likes of Domain & Enterprise Admins. Does your security or IAM teams manages it or is it someone from IT that makes all the decisions?

These are all questions that might be worth to ask yourself before you further. From what I have experienced in my career so far is the following:

- Everyone from IT is Domain Admin
- IT personnel makes all the decisions in AD, which includes managing groups.
- Companies with a managed-services are most of the time not in control of the changes that are made in AD.

Introduction

1 - Insecure configuration

- 1.1) Built-in\Administrator & Domain Admins accounts with a SPN
- 1.2) Accounts with "Do not require Kerberos pre authentication"
- 1.3) Exchange groups with WriteDacl on the DNC
- 1.4) Default Domain Password Policy

2 - DHCP

- 2.1) Delegate rights to authorize at a DHCP server
- 2.2) Delegate rights to create & delete subnets and sites
- 2.3) Ensure backups of DHCP are made and stored securely

• 3 - DNS

- 3.1) RBAC with DNS
- 3.2) Ensure that backups of DNS are made and stored securely
- 3.3) Ensure the DnsAdmins group is monitored

4 - PKI

- 4.1) RBAC with PKI
- 4.2) Ensure that auditing is enabled on PKI servers and AD CS related events are forwarded to a SIEM
- 4.3) Ensure that backups of PKI are made and stored securely

5 - Domain Controllers

- 5.1) Ensure that the Default Domain Controllers Policy is replaced with a more secure focused GPO.
- 5.2) DSRM as Break-Glass account
- 5.3) Ensure Windows Server Backup or equivalent is installed on the DC to make back-ups of Domain Controllers

6 - Group Policy

- 6.1) Replace "Authenticated Users" at the GPO's that are linked to the DC and add the "Domain Controllers" group to it at Security Filtering
- 6.2) GPO's that are linked to the Domain Controller or the Domain Root needs to be managed by Tier 0 admins.
- 6.3) Stop using Group Policy Creator Owners

7 - Active Directory

- 7.1) Do not use Account Operators
- 7.2) Do not use Print Operators
- 7.3) Do not use Server Operators, but there are exceptions
- 7.4) Turn on Active Directory Recycle Bin
- 7.5) Delegate rights for Tier 1 to restore AD objects
- 7.6) Tier 0 admins needs to be part of the "Protected Users" group
- 7.7) Tier 0 admins needs to have the "Account is sensitive and cannot be delegated" checkmark.
- 7.8) Reset the password of the KRBTGT account twice

8 - Monitoring

- 8.1) Monitoring high-privileged groups in AD
- 8.2) Deploy honey user for attacks such as Kerberoasting

9 - Administrative Tier Model

- 9.1) Understand the purpose of MS Administrative Tier Model
- 9.2) How to design the MS Administrative Tier Model?
- 9.3) Ensure Azure AD Connect is managed from a Tier 0
- 9.4) Ensure ADFS servers are managed from a Tier 0

10 - Others

- 10.1) Deploy Azure AD Password Protection for on-premise
- 10.2) Set a password for the Guest account in AD

11 - Access Controls

- 11.1) Discretionary Access Control List
- 11.2) Access Control Entities
- 11.3) BloodHoundAD

12 - AD Audit Tools

12.1) - PingCastle

13 - Acknowledgment

13.1) - Acknowledgment and References

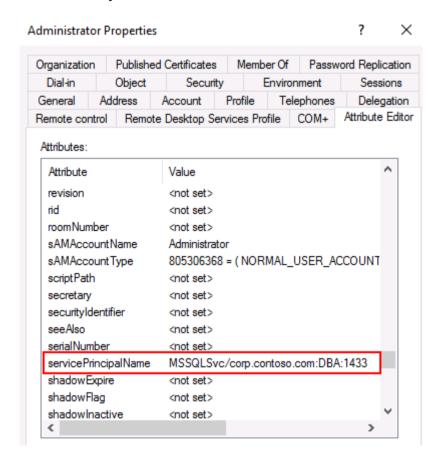
1.1 – Built-in\Administrator with a SPN

Built-in\Administrator is the default account that is created when Active Directory is installed on the first DC.

This account is stored in the **CN=Users** container and is considered as one of the most privileged account in Active Directory, because it is part of groups, such as Domain Admins and Enterprise Admins.

Unfortunately this account has been (mis)used for different tasks with the likes of setting up multiple SQL servers.

Here you can see that the Administrator account has an SPN



Why care?

Every authenticated user in the domain is able to request the service ticket from this Built-in\Administrator account.

Now they are able to export the service ticket locally and crack it offline without being detected.

If an attacker is able to crack the Built-in\Administrator account. He or she has all the keys to the kingdom. Because this account is part of the Domain Admins, group.

This is the SPN of the Administrator account

Attacker request the service ticket of the Administrator account

```
PS C:\Users\Mark> Add-Type -AssemblyName System.IdentityModel
PS C:\Users\Mark> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/corp.con
toso.com:DBA:1433"

Id : uuid-d6bf109e-02b6-4368-97c4-2f8d3e28c9ef-1
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 12/28/2019 1:35:44 PM
ValidTo : 12/28/2019 1:35:44 PM
ServicePrincipalName : MSSQLSvc/corp.contoso.com:DBA:1433
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

 Attacker exports the service ticket and can now crack it offline without any detection or account lockouts.

High-privileged accounts that contains a SPN are immediately at risk, because every authenticated user is able to request service tickets of those accounts and can crack it offline.

It is recommended to use a strong password of around 25 characters for service accounts with SPNs, but since we're talking about the Administrator account. It does not need to have a SPN, so remove the SPN of the Administrator account.

Run CMD with elevated rights (GenericWrite or equivalent is required)

- Setspn -L Administrator
- Setspn -D MSSQLsvc/corp.contoso.com:DBA:1443 Administrator

When can I use the Administrator account?

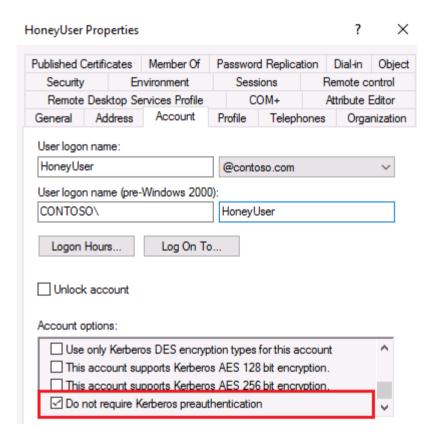
I would keep this account disabled, but only use it for the following tasks:

- Promote a Domain Controller
- Raise a Domain Functional Level
- Add a new Domain Trust

 1.2 – Accounts with "Do not require Kerberos pre authentication"

"Do not require Kerberos pre authentication" is another exposure for an attacker to perform a Kerberos related attack like I have mention above at 1.1

If pre authentication is disabled. An attacker is able to request authentication data from the Domain Controller and the DC will return an encrypted TGT that can be cracked offline.



Why care?

An attacker is able to request the TGT of every account that has pre authentication disabled and can later on, crack it offline without being detected.

Attacker performs recon to discover accounts with pre authentication disabled

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

PS C:\windows\system32> get-aduser -LDAP "(&(objectCategory=person)(userAccountControl:1.2.840.113556.1.4.803:=4194304))" -properties DoesNotRequirePreAuth

DistinguishedName : CN=HoneyUser,0U=Users,0U=Accounts,DC=corp,DC=contoso,DC=com
DoesNotRequirePreAuth : True
Enabled : True
GivenName : HoneyUser
Name : HoneyUser
ObjectClass : user
ObjectClass : user
ObjectGUID : 7222fc79-ba57-4b11-87db-e50247488e9e
SamAccountName : HoneyUser
SID : S-1-5-21-3566662483-2648771335-1709913503-20601
Surname :
UserPrincipalName : HoneyUser@corp.contoso.com
```

 Attacker request the TGT of the vulnerable account(s) and can crack it now offline.

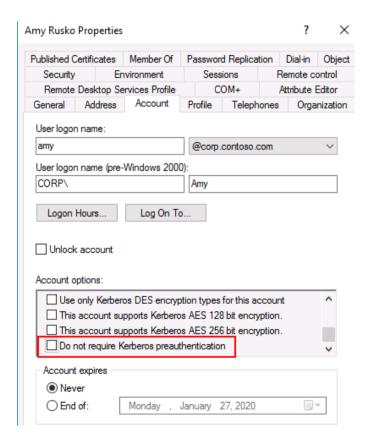


• Event 4768 "An Kerberos authentication ticket (TGT) was requested will show in the security event logs of the DC.

I would start with discovering accounts that have pre authentication disabled and take a look if those accounts are still in use. If not, enable pre authentication again.

 get-aduser -LDAP "(&(objectCategory=person) (userAccountControl:1.2.840.113556.1.4.803:=4194304))" -properties DoesNotRequirePreAuth

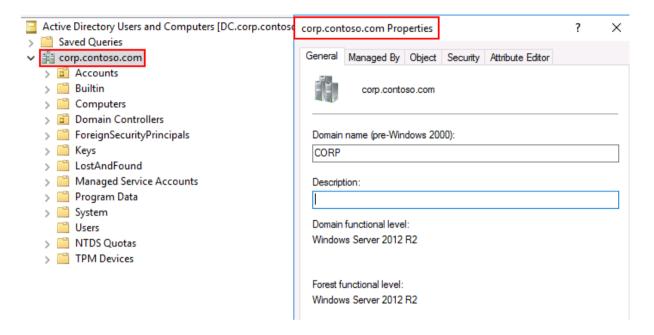
 You likely will find service accounts that have pre authentication disabled, because of compatibility reasons, but if you have managed to discover normal accounts that have pre authentication disabled. Enable it again!



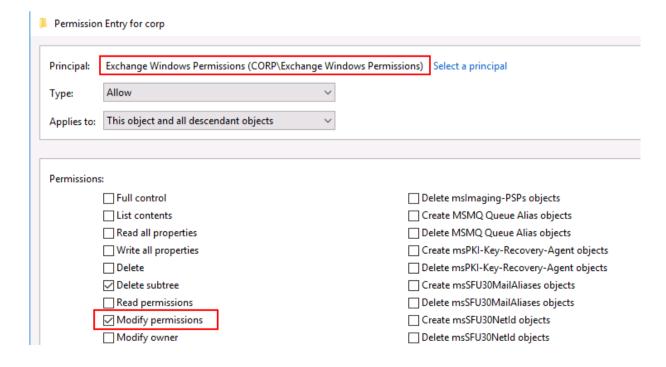
1.3 - Exchange groups with WriteDacl on the DNC

By default most organizations around the world have an Exchange that they used to install 10 years ago.

Exchange has by default a lot of rights in AD that is delegated in the environment. Even on the Domain Naming Context or known as the Domain Root.



Exchange Windows Permissions with WriteDacl on the DNC



Why care?

It is a common mistake that organizations are delegating groups on the DNC, which is not something that I would recommend you to do so.

Besides of Exchange Windows Permissions and Exchange Trusted Subsystem. I would recommend you to look for others group with permissions such as GenericAll, GenericWrite, WriteDacl and WriteOwner

- Get-Acl -Path "AD:\OU=Domain Controllers,DC=corp,DC=contoso,DC=com" | Select-Object -ExpandProperty Access
- Exchange Trusted Subsystem with WriteDacl on Descendant Group Objects

```
ActiveDirectoryRights : ReadProperty, WriteDacl
                       : Descendents
Inheritancelype
                        : 00000000-0000-0000-0000-00000000000
ObjectType
InheritedObjectType
                        : bf967a9c-0de6-11d0-a285-00aa003049e2
ObjectFlags
                         InheritedObjectAceTypePresent
AccessControlType
                        : Allow
IdentityReference
IsInherited
                        : CORP\Exchange Trusted Subsystem
                         True
InheritanceFlags
                         ContainerInherit
PropagationFlags
                        : InheritOnly
```

Exchange Windows Permissions with WriteDacl on the DNC

```
ActiveDirectoryRights : ReadProperty, DeleteTree, WriteDacl
InheritanceType
ObjectType
InheritedObjectType
                         0000000-0000-0000-0000-000000000000
                         0000000-0000-0000-0000-00000000000
ObjectFlags
                         None
AccessControlType
IdentityReference
                        CORP\Exchange Windows Permissions
IsInherited
                         True
InheritanceFlags
                         ContainerInherit
PropagationFlags
                         None
```

An attacker is able to modify the rights on the DNC to grant every ACE for example the **DS-Replication-Get-Changes** & **DS-Replication-Get-Changes-All** permissions to synchronize credentials from the Domain Controller and become a Domain Admin.

If you are running an Exchange of 2013-2019. There is a way to resolve this problem, which is by installing the latest cumulative update.

Fore more information:

https://support.microsoft.com/en-us/help/4490059/using-shared-permissions-model-to-run-exchange-server

The second way to resolve this problem is, when you have fully migrated your entire Exchange environment to Office365 and you don't use anything of onpremise anymore. Remove WriteDacl on the DNC from both Exchange groups.

What happens when you have Exchange 2010?

I have tested this from my own experience, and when you remove WriteDacl from Exchange Trusted Subsystem. It will break a small functionality in Exchange, which is granting "Send as" permissions to users through the Exchange Management Console.

This can be resolved by delegating WriteDacl on Descendant Users on the OU, that stores all the mailbox accounts. Which means that you have to do it through another way instead of using Exchange Management Console.

As far as I know. Removing WriteDacl of Exchange Windows Permissions in Exchange 2010 didn't cause any problems.

Don't allow Exchange groups with having WriteDacl on the DNC. This makes it much easier for an attacker to compromise your AD.

1.4 - Default Domain Password Policy

By default the domain password policy of AD is 7 or 8 characters, which can be considered "insecure" from all the breaches that has happened in the past.

Weak passwords are common in most environment and it is recommended to increase the password policy to something stronger like 12 or 14 characters.

This is the default password policy of most environments

Net accounts /domain

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

PS C:\Users\Mark> net accounts /domain
Force user logoff how long after time expires?: Never
Minimum password age (days): 1

Maximum password age (days): 42
Minimum password length: 7

Length of password history maintained: 24

Lockout threshold: Never
Lockout duration (minutes): 30

Lockout observation window (minutes): 30

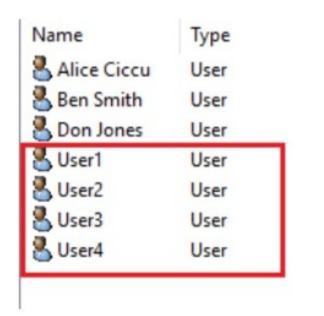
Computer role: PRIMARY

The command completed successfully.
```

• Why care?

Weak passwords are considered insecure, and attackers love weak passwords. There is an attack called "Password spraying", where someone loops one password across the entire domain to see if someone used a poor password, such as "Wachtwoord"

Here I have created four users in AD with "Wachtwoord" as password.



 Password spraying attack on 8 users and 4 of them have been cracked in this example.

```
Confirm Password Spray

Are you sure you want to perform a password spray against 8 accounts?

[Y] Yes [N] No [?] Help (default is "Y"): Y

[*] Password spraying has begun with 1 passwords

[*] This might take a while depending on the total number of users

[*] Now trying password Wachtwoord against 8 users. Current time is 1:49 AM

[*] Writing successes to

[*] SUCCESS! User:User1 Password:Wachtwoord

[*] SUCCESS! User:User2 Password:Wachtwoord

[*] SUCCESS! User:User3 Password:Wachtwoord

[*] SUCCESS! User:User4 Password:Wachtwoord

[*] Password spraying is complete
```

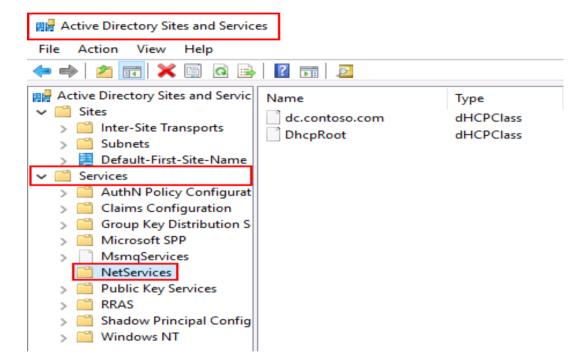
It can be a challenge, but if possible. Increase the password policy to something like 12 or 14 characters. It's a difficult task since lots of political reasons will be involved when doing this.

2.1 - Delegate rights to authorize to DHCP servers

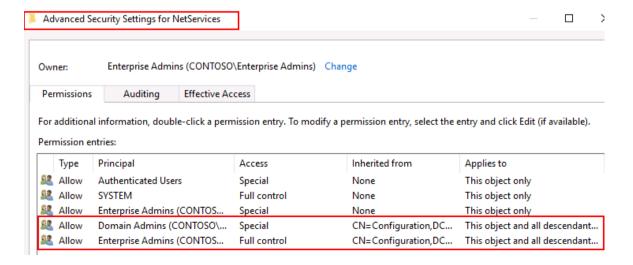
One of the common reason(s) that IT personnel require "DA" privileges is because they need to authorize to DHCP servers, but unfortunately. This is by default only allowed for Domain Admins or equivalent.

Which means that it needs to be delegated. Do most organizations have done this? No.

All the metadata of DHCP is stored in the **CN=NetServices** container. As you can see in the following screenshot.

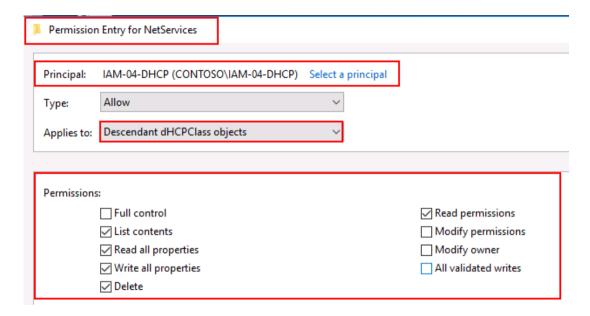


 Here you can see that the DACL of CN=NetServices only contains two ACE's with GenericAll or equivalent permissions. Which is in this case. Domain & Enterprise Admins.

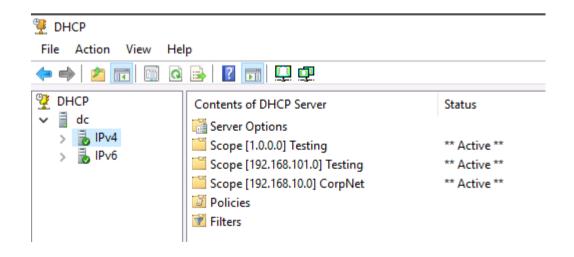


Create a new group that is allowed to authorize to DHCP servers.

- Open ADSI.Edit
- Go to the following: CN=Configuration → CN=Services → CN=NetServices
 → Properties → Security → Add the delegated group → Advanced → Edit →
 Descendant dHCPClass objects
- Select the following permissions down below:



 Now all the users in the delegated group are allowed to authorize to DHCP servers.

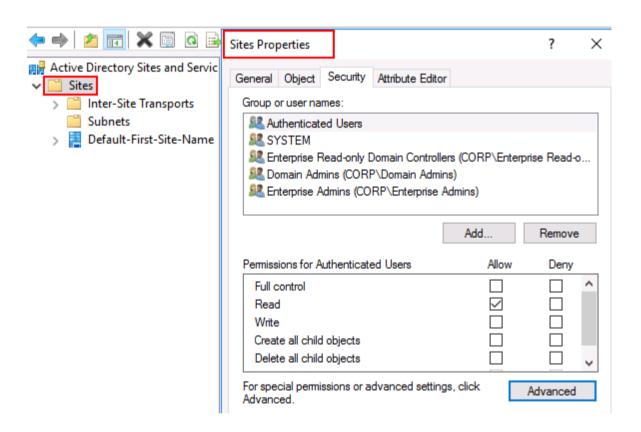


2.2 - Delegate rights to create/delete sites and subnets

We have created a group and delegated it to the CN=NetServices container so it is allowed to authorize to all DHCP servers without having Domain Admin privileges.

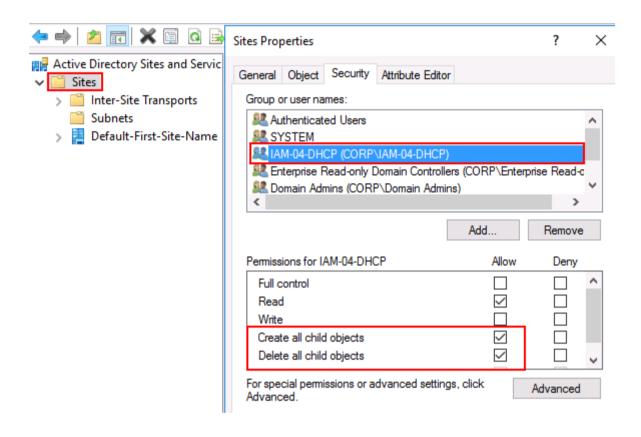
By default, creating new sites or subnets. Requires to have "DA" as well, but this can be delegated easily.

 Here we can see that when we expand the CN=Sites container. It contains two other containers with the likes of "Inter-Site Transport" and "Subnets"



Use the delegated group that you have created before and grant it the following permissions on the **CN=Sites** container:

- Create all child objects
- · Delete all child objects

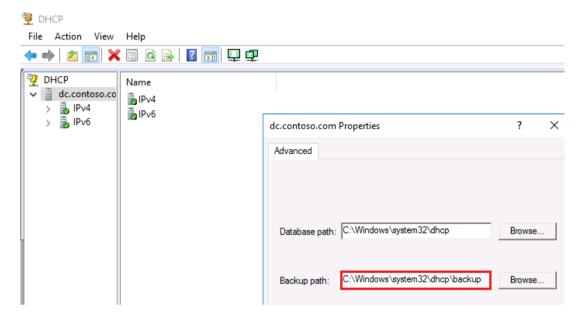


Now Domain Admin or equivalent is not required anymore to create or delete sites and subnets.

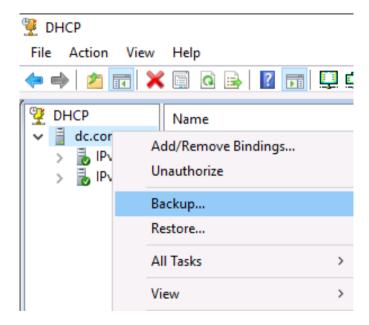
2.3 - Ensure backups of DHCP are made and stored securely

Back-ups are crucial and especially on AD & DHCP, because DHCP allows devices to participate in networks by allocating IP addresses and provide a directory lookup for valid addresses.

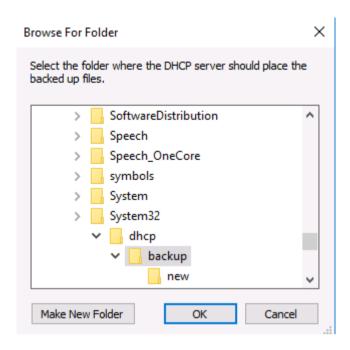
Back-up path of DHCP is: C:\Windows\System32\dhcp\backup



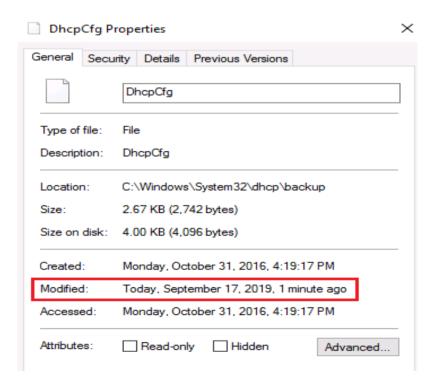
Authorize to the DHCP server and click on "Backup"



Now store the backup in the following location: C:\Windows\System32\
dhcp\backup



• When accessing the directory folder of the DHCP backup. You can see that the back-up of DHCP has been made.



- Start with developing a process for making back-ups of DHCP if you haven't done it yet. Like when are we going to make back-ups of DHCP?
- Start with practicing the restore of it. How quick would you be able to restore the DHCP back-up, when there is a disaster?

All the back-ups of DHCP are crucial and should be stored locally on a server that is **not** AD joined.

3.1 – RBAC with DNS

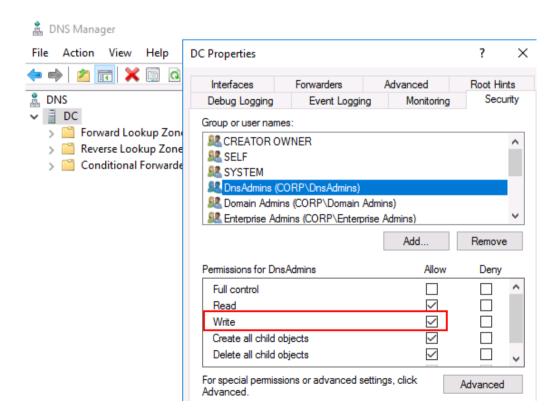
Start with creating two new groups in Active Directory:

- DnsManagers
- DnsCreators



DnsAdmins is often not needed to manage DNS, because most tasks can be delegated.

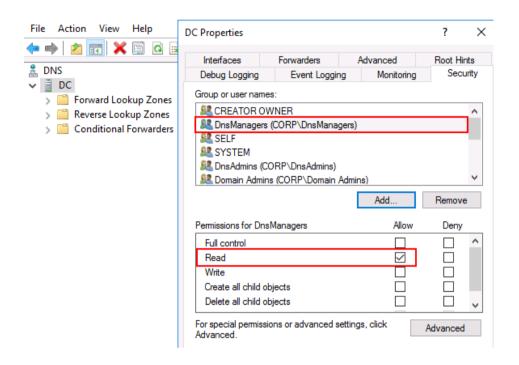
Since **DnsAdmins** has the rights to execute a DLL as SYSTEM on the DC. It becomes a valuable target for attackers to elevate from DnsAdmins to Domain Admin. All the users with GenericWrite or equivalent on the DC DNS Object can perform this attack.



DnsAdmins	DnsManagers	DnsCreators
 Configure Debug/Event logging 	 Create new records, such as MX, CNAME, A, AAA, etc. 	 Create new records, such as MX, CNAME, A, AAA, etc.
 Configure a DNS Server 	 Delete created records 	 Delete created records
 Create new Forward/Reverse Lookup Zone 	 Read DNS Event Logs 	
 Create new Conditional Forwarders 	 GenericAll on exisiting DNS records 	
Clear (DNS) Cache	 Start, stop and pause the Forward Lookup Zone 	
 Start, Stop, Pause and Restart the DNS Server 	 Change the Zone type (e.g. Primary, Stub and Secondary) 	
	 Give permission to users/groups to manage the Forward Lookup Zones 	
	 Allowing Zone Transfers 	
	Add/Remove Name Servers	
	 Change aging/scavenging properties 	
	 Change the TTL of a Forward lookup zone 	
	 Sign the zone with DNSSEC 	

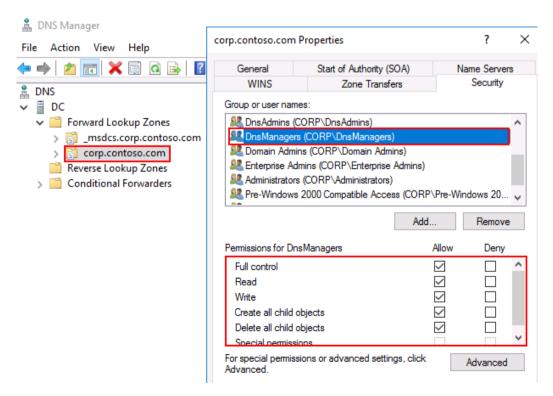
• **DnsManagers**

1. Start with adding the group to the DACL of the DC DNS Object and make sure it has "Read all properties" permission. That's it.



2. Expand the Forward Lookup Zones containers

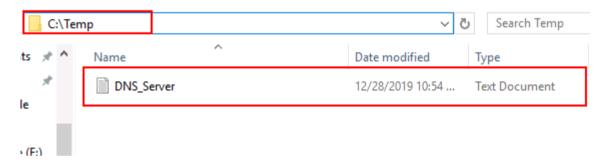
Give DnsManagers "GenericAll" on the Forward Lookup Zones



- Delegate rights to **DnsManagers** to read DNS Event Logs
 By default only Domain Admins or equivalent can read **DNS Server** logs.
- 3. Log in as Domain Admin and run CMD with elevated rights
- **3.1.** Type the following command in CMD: **wevtutil gl "DNS Server" > C:\ Temp\DNS_Server.txt**

```
C:\windows\system32>wevtutil gl "DNS Server" > C:\Temp\DNS_Server.txt
C:\windows\system32>_
```

3.2. Open the <u>C:\Temp</u> folder and click DNS_Server.txt



3.3. Copy the following part of the textfile: **channelAccess:** (A;;0x1;;;SID)

```
DNS_Server.txt - Notepad
File Edit Format View Help
name: DNS Server
enabled: true
type: Admin
owningPublisher:
isolation: Application
channelAccess: 0:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x5;;;S0)(A;;0x1;;;IU)(A;;0x1;;
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\DNS Server.evtx
  retention: false
  autoBackup: false
  maxSize: 104857600
publishing:
  fileMax: 1
```

3.4. Get the SID of the DnsManagers group

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

PS C:\Users\Mark> Get-ADGroup -Identity "DnsManagers"

DistinguishedName: CN=DnsManagers,OU=DNS Groups,OU=Accounts,DC=corp,DC=contoso,DC=com GroupCategory: Security
GroupScope: Global
Name: DnsManagers
ObjectClass: group
ObjectGUID: 7374a049-1786-47d1-85f8-98f174ef124b
SamAccountName: DnsManagers
SID: S-1-5-21-3566662483-2648771335-1709913503-20601
```

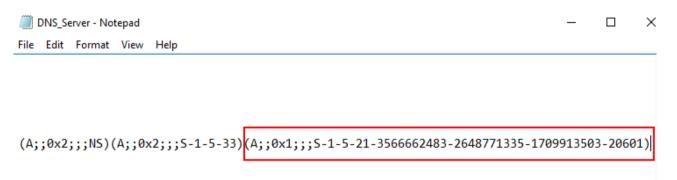
3.5. Copy the following (A;;0x1;;;SID) and replace "SID" with the actual SID of the DnsManagers group.

S-1-5-21-3566662483-2648771335-1709913503-20601

Which means that you should get something like this:

(A;;0x1;;;S-1-5-21-3566662483-2648771335-1709913503-20601)

3.6. Now copy **(A;;0x1;;;S-1-5-21-3566662483-2648771335-1709913503-20601)** and paste it at the end of **channelAccess** in the text file.



3.7. Now copy the entire text from O:BAG:SYD: till the end of the text.

O:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x5;;;SO)(A;;0x1;;;IU)(A;;0x1;;;SU)
(A;;0x1;;;S-1-5-3)(A;;0x2;;;LS)(A;;0x2;;;NS)(A;;0x2;;;S-1-5-33)(A;;0x1;;;S-1-5-21-3566662483-2648771335-1709913503-20601)

3.8. Open CMD with elevated rights and type the following command:

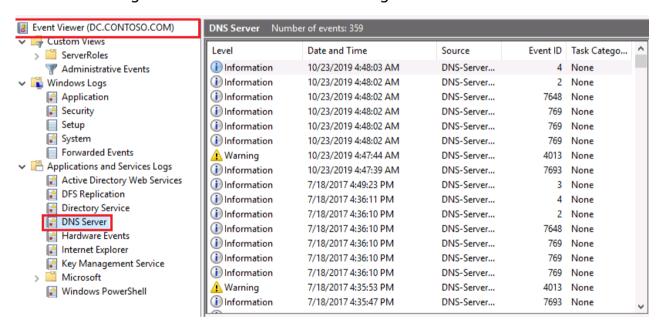
wevtutil sl "DNS Server" /ca: **O:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)** (A;;0x5;;;SO)(A;;0x1;;;IU)(A;;0x1;;;SU)(A;;0x1;;;S-1-5-3)(A;;0x2;;;LS) (A;;0x2;;;NS)(A;;0x2;;;S-1-5-33)(A;;0x1;;;S-1-5-21-3566662483-2648771335-1709913503-20601)

Administrator: Command Prompt

C:\windows\system32>wevtutil sl "DNS Server" /ca:0:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x5;;;SO)(A;;0x1;;;;U)(A;;0x1;;;SU)(A;;0x1;;;SU)(A;;0x1;;;S-1-5-3)(A;;0x1;;;S-1-5-3)(A;;0x2;;;LS)(A;;0x2;;;NS)(A;;0x2;;;S-1-5-33)(A;;0x1;;;S-1-5-21-3566662483-2648771335-1709913503-20601)

C:\windows\system32>

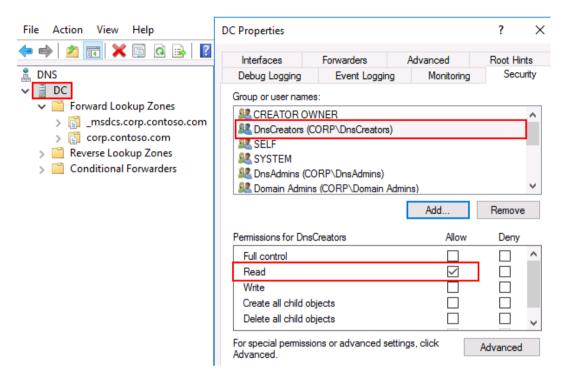
3.9. DnsManagers can now read the event logs of "DNS Server"



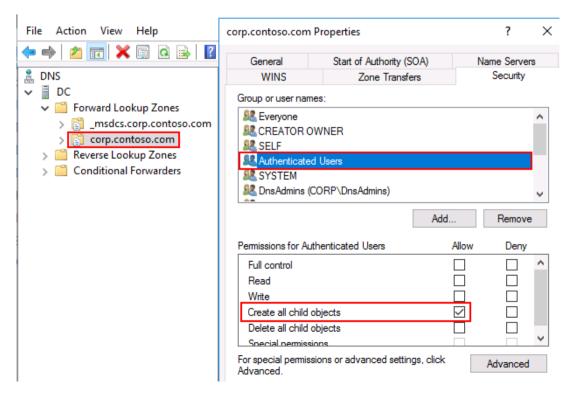
3.10. DnsManagers has now all the rights that we have managed in our RBAC model.

DnsCreators

Add the ''DnsCreators'' group to the DACL of the DNS Object and ensure only ''Read all properties'' is assigned. That's it.



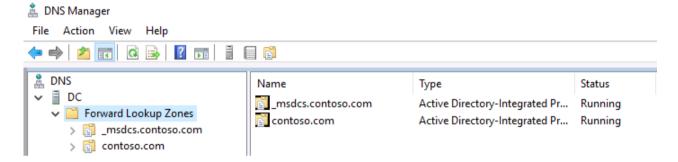
 By default "Authenticated Users" already have "Create all child objects" on the FWL zones, so that means that **DnsCreators** can create DNS records. If it has "Read" permission on the DNS Object itself.



 3.2 – Ensure that back-ups of DNS are made and stored securely

All the information related to DNS records etc are stored in the following location: **C:\Windows\System32\dns**

- Open DNS Manager
- Expand the Forward Lookup Zone, container.



- Open PowerShell or CMD with elevated rights
- Type the following commands:
- 1. Dnscmd /zoneexport msdcs.contoso.com msdcs.contoso.com.txt

```
PS C:\Users\Administrator> dnscmd /zoneexport _msdcs.contoso.com _msdcs.contoso.com.txt

DNS Server . exported zone
   _msdcs.contoso.com to file C:\Windows\system32\dns\_msdcs.contoso.com.txt

Command completed successfully.

PS C:\Users\Administrator>
```

Dnscmd /zoneexport contoso.com contoso.com.txt

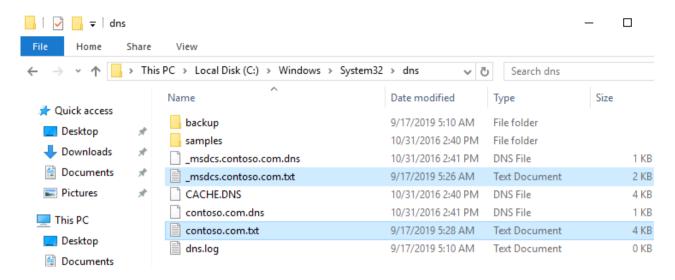
```
PS C:\Users\Administrator> dnscmd /zoneexport contoso.com contoso.com.txt

DNS Server . exported zone
    contoso.com to file C:\Windows\system32\dns\contoso.com.txt

Command completed successfully.

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

3. Open C:\Windows\System32\dns and you can see our back-ups



- Store the DNS back-ups locally on a server that is not AD joined.
- Start a procedure for making back-ups of DNS if you haven't done it yet.
 Like for example. When are we going to make back-ups? Every month, week, days?
- Start preparing for a disaster. What happens when someone accidentally deleted your entire Forward Lookup Zone? How would you restore it quickly as possible to reduce downtime? Do you know how to restore it? These are questions that you might ask your team about.
- Try to avoid or limit DnsAdmins since it is barely needed.
- Deploying a RBAC model for managing DNS reduces the risk for assigning users the DnsAdmins privileges.

• 4.1 - RBAC with PKI

ion
gle
n CA manage nage of the nould
· · ·

Tasks

CA Administrator	CA Manager
	Approve certificate enrollment and revocation requests.

• Who can do what?

CA Administrator

- Create Certificate Templates
- Enroll users and computers to the created certificate template
- Start and stop Active Directory Certificate Services
- Configure extensions
- Configure roles
- Define key recovery agents
- Restrict certificate managers
- Delete a single row in CA
- Mass deletion of CA rows
- Enable, publish, or configure certificate revocation list (CRL) schedules
- Read the CA database
- Read the CA configuration
- Configure policy and exist module

CA Manager

- Issue and approve certificates
- Deny certificates
- Revoke certificates
- Reactivate certificates that are placed on hold
- Renew certificate template
- Recover archived keys
- Read the CA database
- Read the CA configuration

Start with creating two new groups in AD

- CA Administrators
- CA Managers

Name	Туре	Description
🎎 CA Administrators	Security Group	Configure and maintain the CA
a CA Managers	Security Group	Approve certificate enrollment and revocation reque

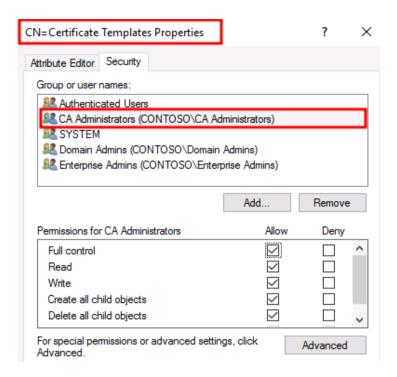
Open ADSI Edit → Configuration → CN=Services → CN=Public Key Services

The following containers that have been marked in **RED** are the containers that we need to use to delegate the administrative tasks.

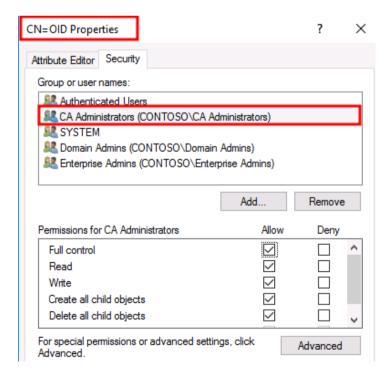
- CN=Certificate Templates
- · CN=OID

Name	Class	Distinguished Name
CN=AIA	container	CN=AIA,CN=Public Key Services,CN
CN=CDP	container	CN=CDP,CN=Public Key Services,C1
CN=Certificate Templates	container	CN=Certificate Templates,CN=Publ
CN=Certification Authorities	container	CN=Certification Authorities, CN=Pu
CN=Enrollment Services	container	CN=Enrollment Services, CN=Public
CN=KRA	container	CN=KRA,CN=Public Key Services,CN
CN=OID	msPKI-Enter	CN=OID,CN=Public Key Services,CN
CN=NTAuthCertificates	certification	CN=NTAuthCertificates,CN=Public

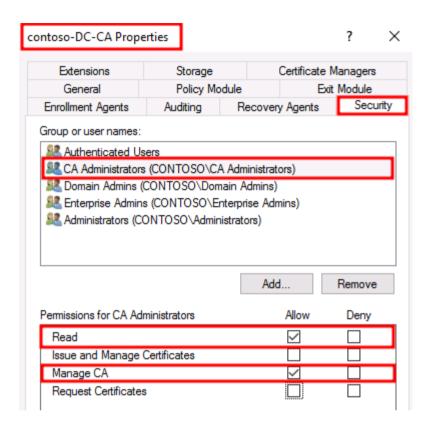
Right click on CN=Certificate Templates → Security → Add → CA
 Administrators → Full control



Right click on CN=OID → Security → Add → CA Administrators → Full control

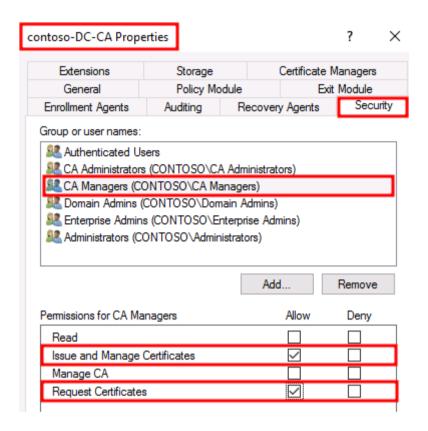


Open Certificate Authority → Right click on CA server object → Security → Add → CA Administrators → Read → Manage CA → Uncheck "Request Certificates"



Delegation has been finished for **CA Administrators**.

Open Certificate Authority → Right click on CA server object → Security → Add → CA Managers → Issue and Manage Certificates → Request Certificates



Now we have finished the delegation for ${\bf CA\ Managers}.$

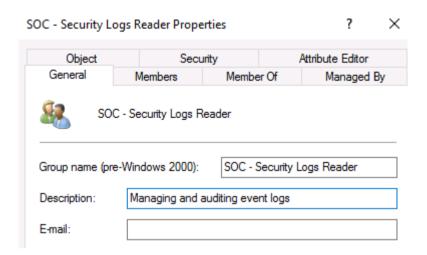
4.2 - Ensure auditing is enabled on PKI servers and event logs are forwarded to a SIEM

Requirement	Turn on CA Auditing	
Description	By default all the related events regarding CA are not logged. These auditing rules needs to be enabled and manage by the security team with the likes of an SOC/SIEM for example.	
Supplement	Since PKI is a critical asset. It should be monitored strictly in an environment. Logging is one of the most important tasks to ensure the security of an Certificate Authority.	
ID	AD-CS-003	
Exception	PKI is often a critical assets, but that doesn't mean it is for all the companies around the world.	

Tasks

•	SOC/SIEM
•	Configure auditing rules
•	Managing auditing logs in Event Viewer
•	Import & Export event logs in Event Viewer
•	Clear event logs

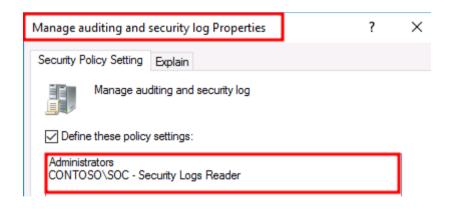
First a new group should be created that is responsible for managing CA auditing logs.



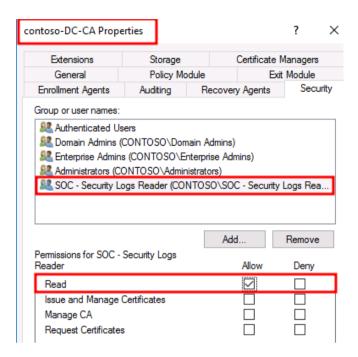
After the group has been created. Add everyone that will be responsible for keeping an eye on CA. Which is usually the SOC.

Log on the CA server and open Local Security Policy → Policies → Windows Settings → Security Settings → Local Policies → User Right Assignment → Manage auditing and security logs

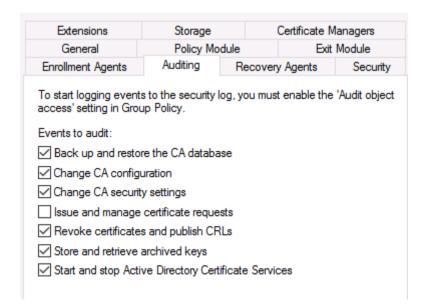
Add SOC - Security Logs Reader



Now give "SOC - Security Logs Reader" the "Read" permission on the CA servers.



 Now everyone from the SOC - Security Logs Reader can turn on the auditing rules and collect AD CS related event logs.



To get a better visibility it is recommended to turn on the "Certification Services" subcategory as well.

auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable

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

PS C:\windows\system32> auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
The command was successfully executed.

PS C:\windows\system32> _
```

auditpol /get /category:*

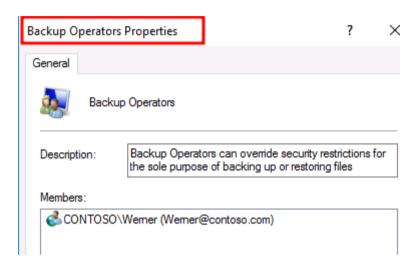
```
PS C:\windows\system32><sup>'</sup>auditpol /get /category:*
System audit policy
Category/Subcategory
                                                             Setting
System
  Security System Extension
System Integrity
IPsec Driver
                                                             No Auditing
                                                             Success and Failure
No Auditing
Other System Events
Security State Change
Logon/Logoff
                                                             Success and Failure
                                                             Success
                                                            Success and Failure
  Logon
  Logoff
                                                            Success
  Account Lockout
                                                             Success
  IPsec Main Mode
                                                            No Auditing
  IPsec Quick Mode
IPsec Extended Mode
Special Logon
                                                            No Auditing
                                                            No Auditing
                                                            Success
                                                            No Auditing
Success and Failure
No Auditing
  Other Logon/Logoff Events
Network Policy Server
User / Device Claims
Group Membership
                                                             No Auditing
Object Access
File System
                                                             No Auditing
  Registry
Kernel Object
                                                             No Auditing
                                                             No Auditing
                                                             No Auditing
                                                             Success and Failure
  Certification Services
                                                             No Auditing
No Auditing
  Application Generated
  Handle Manipulation
  File Share
                                                             No Auditing
```

• All AD CS related events ID's can be found here:

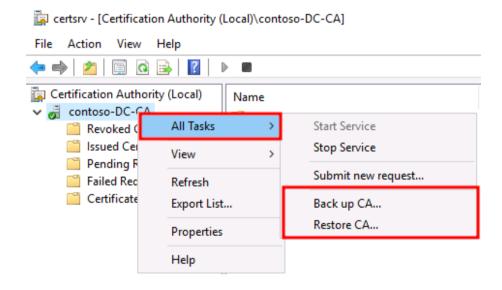
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786423(v=ws.11)

4.3 - Ensure that backups of PKI are made and stored securely

Log on the CA server(s) \rightarrow Open Computer Management \rightarrow Local Users and Groups \rightarrow Groups \rightarrow **Backup Operators** \rightarrow Add the appropriate member(s) that are responsible for making back-ups.



- Backup Operators has the rights to log on locally on the CA servers, but it cannot log on via RDP.
- All Tasks → Back up CA...



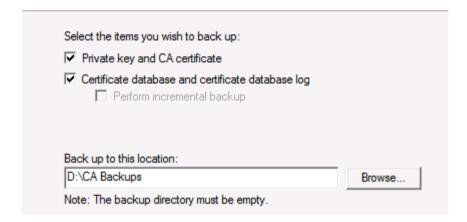
- When performing CA back-ups. Ensure the following things are covered.
- CA certificate(s) and private key(s)
- CA database backup
- CA registry information

Tip: Consider back-up the CA to another secure location that interfaces with backup systems rather than having backup systems connect directly to the CA.

Certification Authority Backup Wizard

Items to Back Up

You can back up individual components of the certification authority data.



Ensure that you select both options

Completing the Certification Authority Backup Wizard

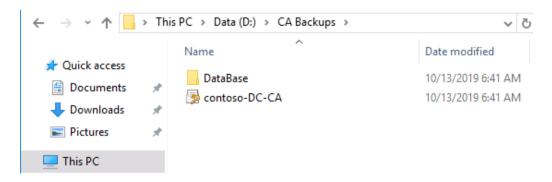
You have successfully completed the Certification Authority Backup wizard.

You have selected the following settings:

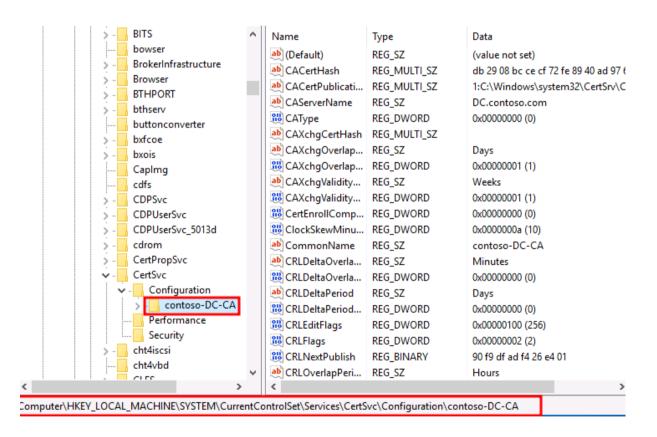


To close this wizard and begin backup, click Finish.

 Here we can see that the back-up has been made. Ensure that the private key has a strong password.



- Ensure that you cover the CA Registry key as well on the PKI server. This
 can be found here: HKLM\System\CurrentControlSet\Services\
 CertSVc\Configuration\CAname
- · Make an **export** of the exact registry path



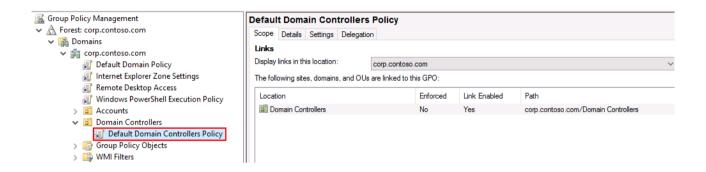
Recommendations

- Do not forget to make back-ups of CA servers.
- Enable auditing on CA servers
- Forward PKI security events to a SIEM
- Back-up the registry key of CA as well
- Store back-ups locally on a server that is not AD joined.
- Deploying an RBAC model on AD CS helps you to manage PKI without having unnecessary users in Domain Admins or equivalent.

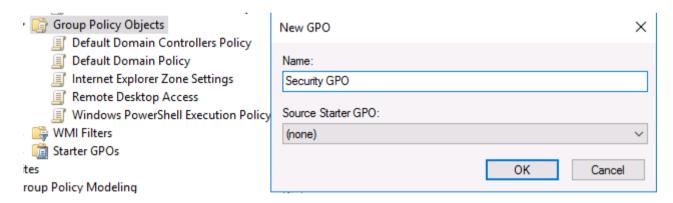
 5.1 - Ensure that the Default Domain Controllers Policy is replaced with a more secure focused GPO

By default, there is the known "Default Domain Controllers Policy" that is linked to the Domain Controllers.

The settings that are deployed by default in the "Default Domain Controllers Policy" are not secure, and no. I'm not going to explain "why"



 Create a new GPO and replace it with the more "secure" minded settings.



 Edit the created GPO with the following settings that can be found at User Right Assignments

• User Right Assignment

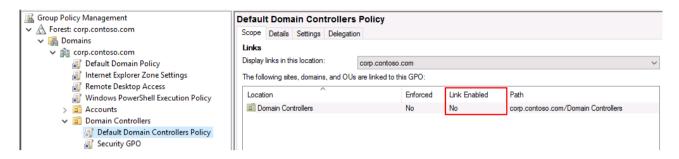
Access this computer from the network	Administrators, Authenticated Users, Enterprise Domain Controllers
Add workstation to a domain	Administrators
Allow log on locally	Administrators, Backup Operators
Allow log on through Remote Desktop Services	Administrators
Backup files and directories	Administrators, Backup Operators
Restore files and directories	Administrators, Backup Operators
Change the system time	Administrators
Debug Programs	Administrators
Deny access to this computer from the network	Guests, DC
Deny log on through Remote Desktop Services	Guests, DC
Shutdown the system	Administrators
Log on as a service	Service accounts that need to run as a service
Log on as a batch job	Service accounts for scheduled tasks

• Security Options

Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Domain controller: Allow server operators 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 (Test this first)

Recommendation

- Link the new security GPO to the Domain Controllers
- Unlink the "Default Domain Controllers Policy" from the Domain Controllers.



5.2 - DSRM as Break-Glass account.

Directory Services Restore Mode (**DSRM**) is a safe mode boot option for Windows Server domain controllers. DSRM allows an administrator to repair or recover to repair or restore an Active Directory database.

This is like the break-glass account of Active Directory for disaster recovery.

Source: https://searchwindowsserver.techtarget.com/definition/Directory-Services-Restore-Mode-DSRM

- Are you aware who has the password of this account?
- When was the last time that the password has been reset?
- Reset the password of DSRM with ntdsutil
- **1.** Open CMD with elevated rights (DA or equivalent is required)
- 2. Type: ntdsutil
- 3. Type: set DSRM password

Administrator: Command Prompt - ntdsutil

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:

4. Type: **reset password on server DC**Our Domain Controller name is called "DC"

```
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:
```

5. Now pick a password for the **DSRM** account

```
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: q
ntdsutil:
```

6. Type: quit

7. Type: quit

8. Type: exit

9. Now when you want to sign in with the DSRM account:



Recommendations

DSRM is like the break-glass account for Domain Controllers Ensure the password is not shared across all your AD Admins.

- If you have never changed the password of this account. It's the right time to do so.
- Are you aware who has the password of the DSRM account?

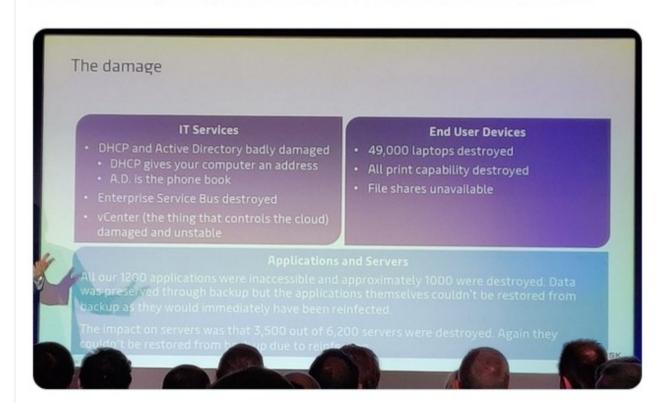
 5.3 - Ensure Windows Server Backup or equivalent is installed on the DC to make back-ups of Domain Controllers

Making back-ups is a very important task in Active Directory, and the ransomware attack on Maersk is a great example on why you should make back-ups and secure them very well.

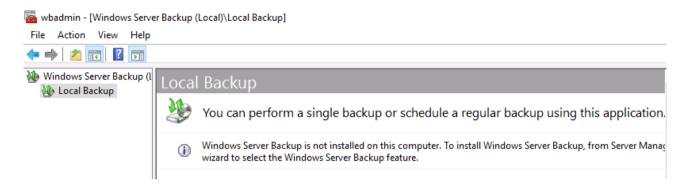
Like the CISO of Maersk mention as well. "Offline backups are critical, even in very large networks"



"Active Directory is king. Offline backups are critical, even in very large networks." Maersk CISO #BHEU



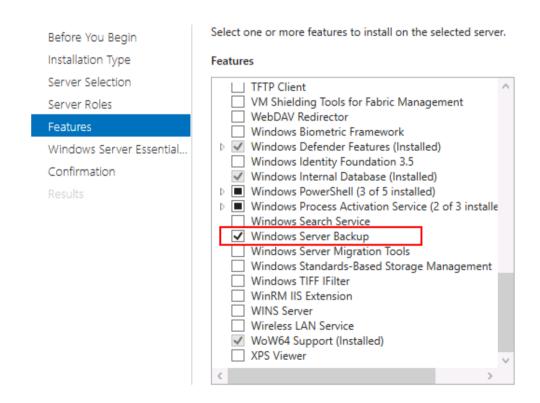
• **Windows Server Backup** can be installed from the "Add roles and features" in Server Manager. It is **not** installed by default.



Ensure that Windows Server Backup is installed the Domain Controllers.



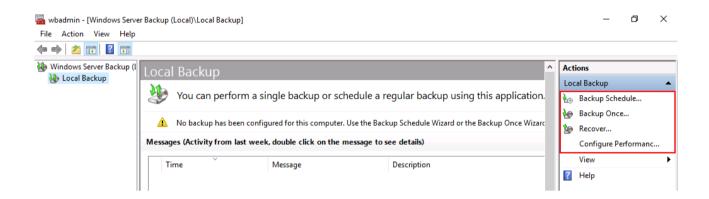
Select features



Since making back-ups is crucial in Active Directory. I will take the time to walk you through different steps.

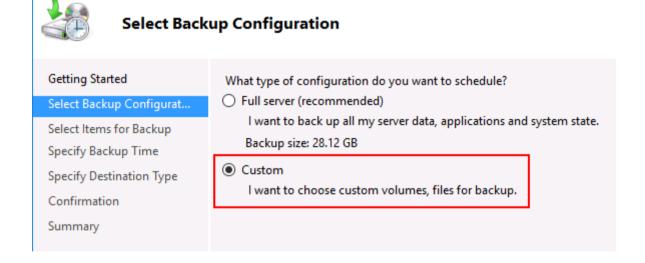
There are two options to create back-ups, which is the following:

- Backup schedule → Task scheduler for automatically back-ups
- Backup once → Manual backup AD/DC

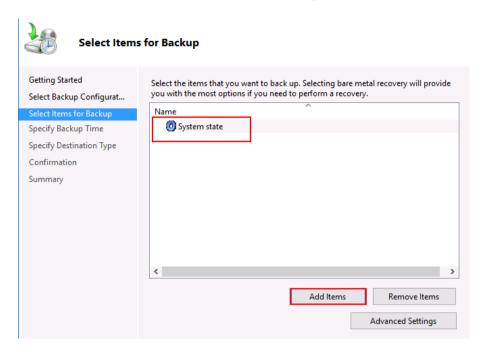


I will pick "Backup Schedule" in this example.

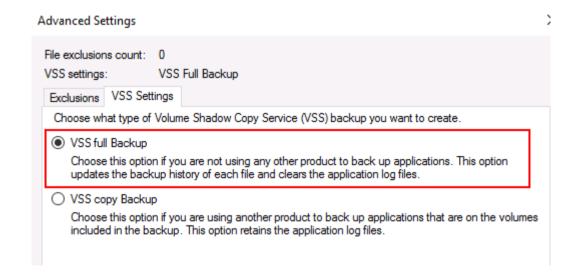
- Click on Backup Schedule
- Click next
- Click Custom



Click Add Items and select System state



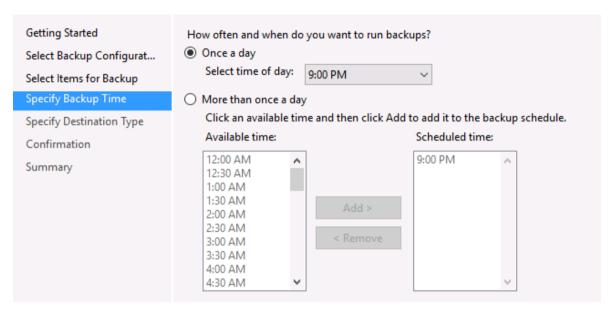
- Click on "Advanced Settings" and "VSS Settings"
- Select VSS full backup if you don't have any back-up software or equivalent to back-up AD/DC



- Click next
- Now select what kind of backup time you prefer.



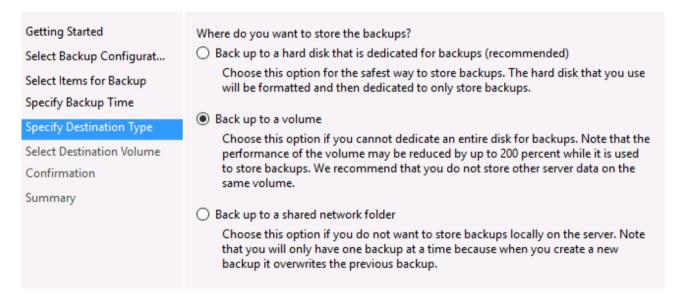
Specify Backup Time



- Click next
- At the destination type. Select the one that you prefer.



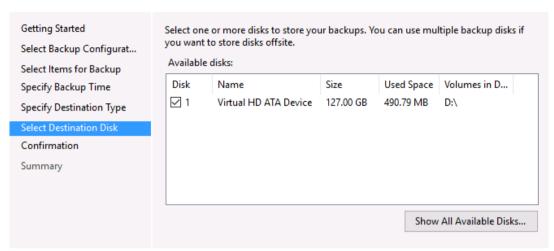
Specify Destination Type



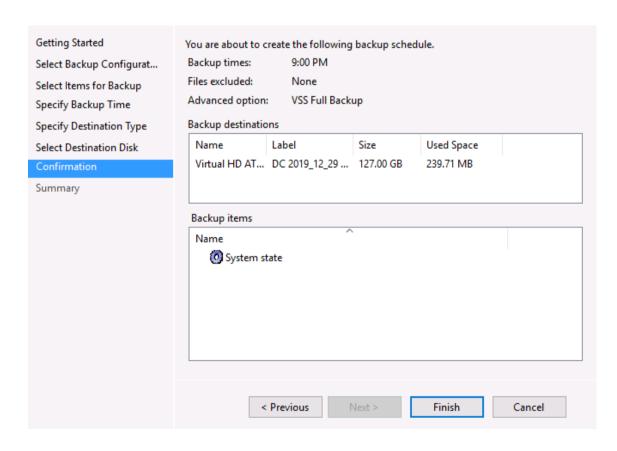
Now click next and you get something like this



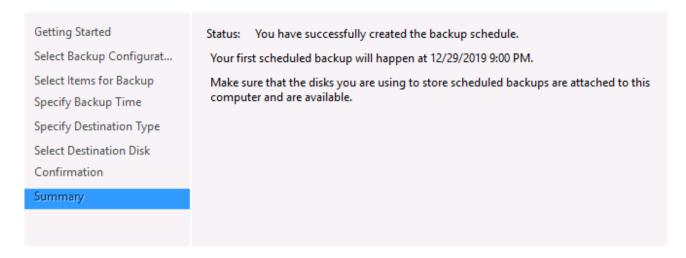
Select Destination Disk



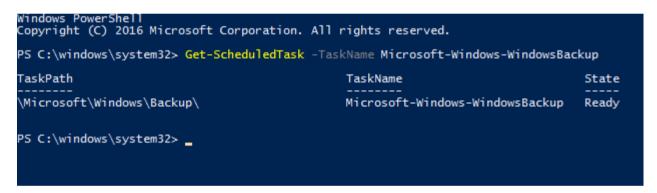
- Click next
- Click Finish

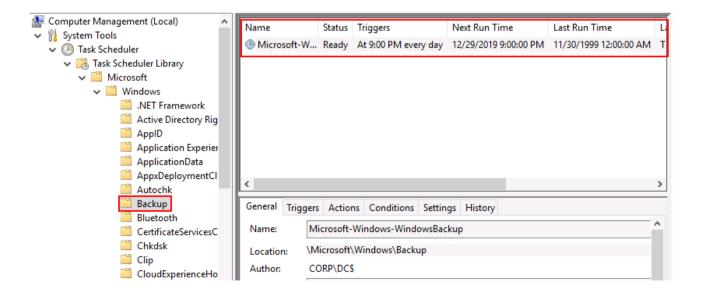


Backup Schedule has been finished!

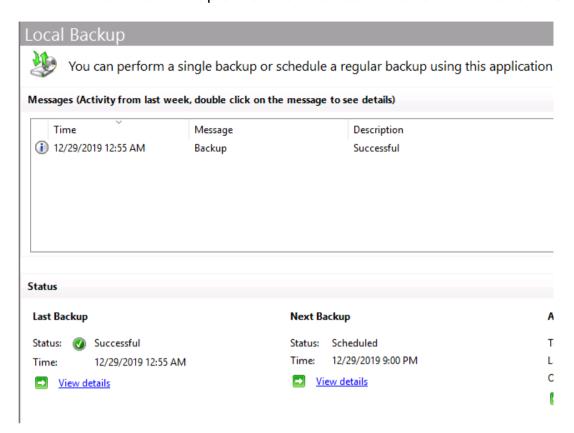


- Now a Scheduled Task will be created with the name "Microsoft-Windows-WindowsBackup"
- Location: \Microsoft\Windows\Backup

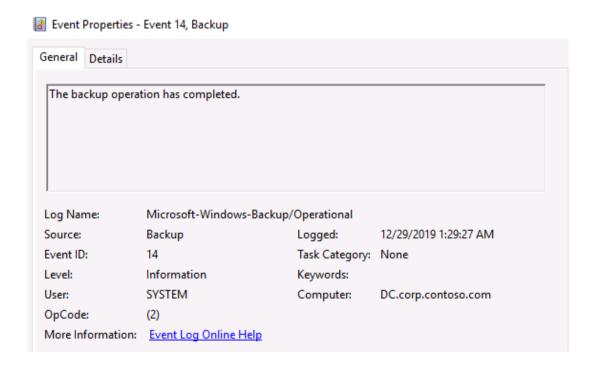




When the Backup schedule has been finished. It will show "successful"



 Everything is logged and when event 14 shows up. You know that the backup has been completed.



Recommendation

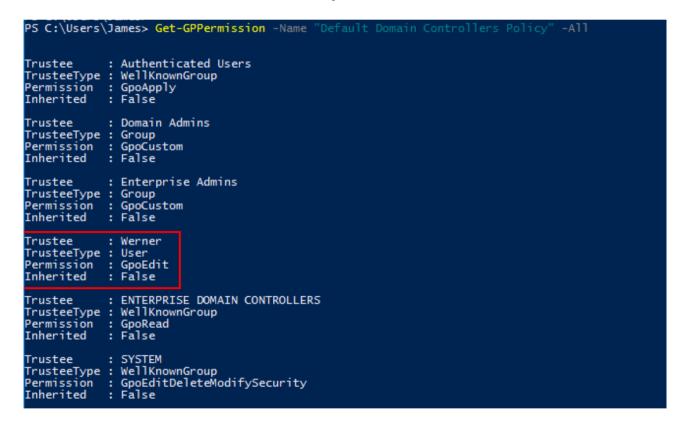
- Make back-ups of AD/DC.
- Store the back-up locally on a server that is not joined through AD.
- A common mistake is that companies store back-ups on Member servers that are joined in AD. An attacker is often aware of this and will also go after your backup servers.
- Making back-ups of AD/DC is usually from a Tier 0 operations. Because if someone wants to recover something. Logon access are required to the DC. Which doesn't immediately means that Domain Admins is required, because Backup Operators is enough as well.
- Audit periodically to see if back-ups are also completed "successfully"

 6.1 - Replace "Authenticated Users" at the GPO's that are linked to Domain Controllers

Every **authenticated user** has read permissions on GPO's in AD. Tools with the likes of BloodHound are able to discover wrong delegated permissions on GPO's, that are linked to the DC for example.

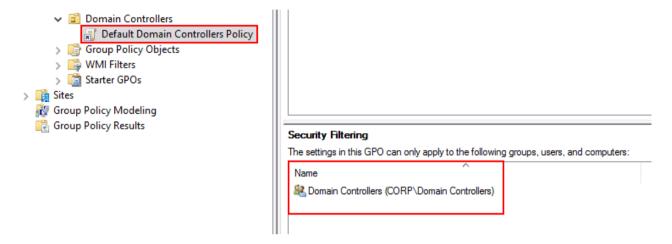
If an attacker is able to modify the GPO of a DC. All bets are off the Domain Controller, because an attacker would be able to run code on the DC or grant himself "Take ownership of files and objects" to elevate further to Domain Admin.

 Here we can see that the user Werner has GpoEdit permissions on the Default Domain Controllers Policy.



Recommendation

To slow down tools like BloodHound for reconnaissance. It is an option to target the ''Domain Controllers'' group at Security Filtering of the GPO's that are applied on all DC's.



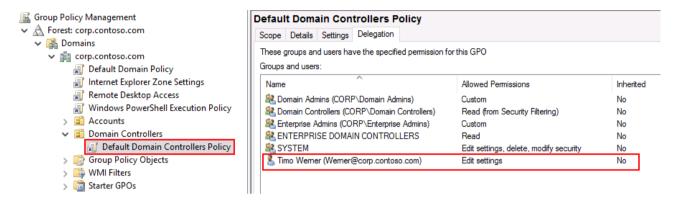
Result

```
PS C:\Users\James> Import-Module ActiveDirectory
PS C:\Users\James> Get-GPPermission -Name "Default Domain Controllers Policy" -All
Get-GPPermission: The "Default Domain Controllers Policy" GPO was not found in the corp.contoso.com domain.
Parameter name: gpoDisplayName
At line:1 char:1
+ Get-GPPermission -Name "Default Domain Controllers Policy" -All
+ CategoryInfo : ObjectNotFound: (Microsoft.GroupPolicy.GPDomain:GPDomain) [Get-GPPermission], ArgumentEx ception + FullyQualifiedErrorId: GpoWithNameNotFound,Microsoft.GroupPolicy.Commands.GetGPPermissionsCommand
PS C:\Users\James> __
```

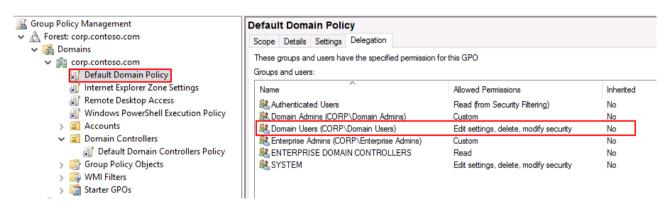
• 6.2 - GPO's that are linked to Tier 0 resources needs to be managed by Tier 0 admins.

In large organizations. It is common to see that permissions have been delegated on a wrong way at a GPO level.

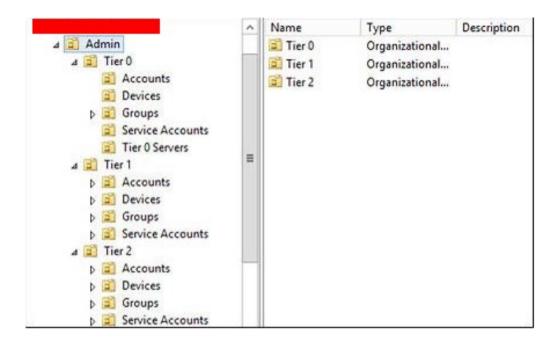
 Here is an example where you can see that a random user has GpoEdit permissions on the Default Domain Controllers Policy, GPO.



 Here someone decided to add Domain Users with Full permissions on the Default Domain Policy.



As you can see in the following screenshot. There is an administrative tier model that is in place to mitigate credential theft. Tier 0 admins cannot log on Tier 1 resources, and Tier 1 admins cannot log on Tier 2 resources.



- All the GPO's that are applied on the Tier 0 servers should be managed by Tier 0 admins.
- Tier 0 servers are usually the critical servers, such as ADFS, Azure AD Connect, PKI, Domain Controllers, etc.



• Recommendation

- GPO's that are applied to the Domain level and Domain Controllers needs to be managed by Tier 0 admins.
- GPO's that are applied to Tier 0 servers needs to be managed by Tier 0 admins.

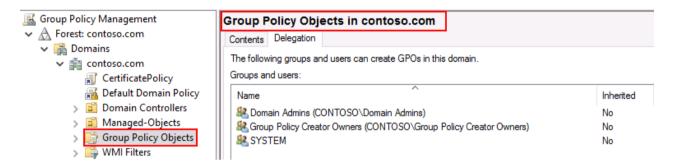
6.3 – Stop using Group Policy Creator Owners

Group Policy Creator Owners is a Built-in group in AD that comes out of the box with more rights than needed.

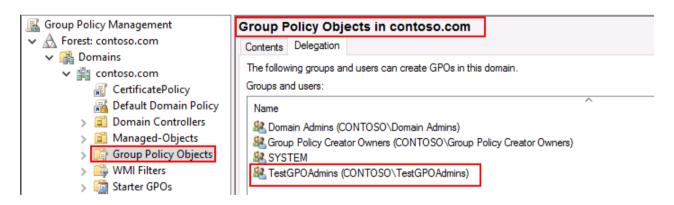
We all know that Group Policy Creator Onwers can only create GPO's, but cannot link it to something, which already makes it a bit useless to use it.

Another reason that this group is a bit useless is, because it is very difficult to delegate rights on the defaultSecurityDescriptor in the CN=Group-Policy-Container schema attribute. This schema attribute represents Group Policy.

 Here you can see that Domain Admins & Group Policy Creator Owners can create GPO's



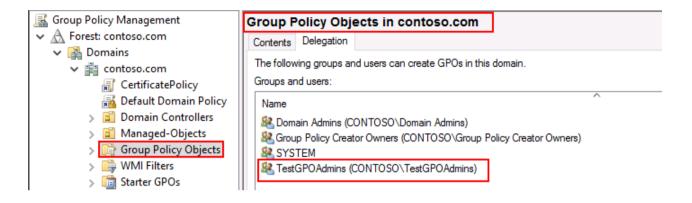
 Now I have added a delegated group to it. This group can now also create GPO's



Recommendations

To manage Group Policy on a much efficient way without having unnecessary privileges requires the following:

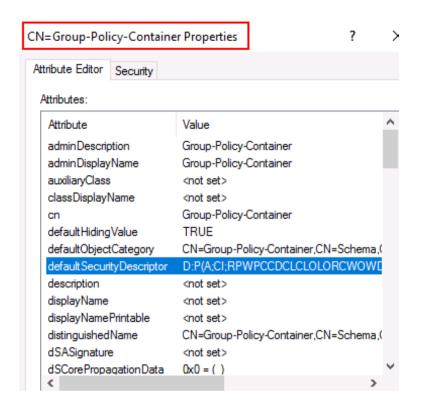
 Create a group and delegate it to Group Policy Objects. Allow this group to create GPO's



Get the SID of the delegated group

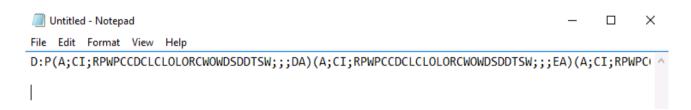
```
PS C:\Users\LabAdmin> Get-ADGroup -Identity "TestGPOAdmins"
DistinguishedName : CN=TestGPOAdmins,OU=Groups,OU=Managed-Objects,DC=contoso,DC=com
                  : Security
GroupCategory
                  : Global
GroupScope
                  : TestGPOAdmins
Name
ObjectClass
                  : group
ObjectGUID
                  : 5e17cbb5-4039-4a99-86c1-906214b4809f
                    TestGP0Admins
SamAccountName
SID
                  : 5-1-5-21-2367645265-33317674-1292933090-12603
```

Open ADSI.Edit and search for CN=Group-Policy-Container



Copy the defaultSecurityDescriptor and paste it in notepad:

D:P(A;CI;RPWPCCDCLCLOLORCWOWDSDDTSW;;;DA)
(A;CI;RPWPCCDCLCLOLORCWOWDSDDTSW;;;EA)
(A;CI;RPWPCCDCLCLOLORCWOWDSDDTSW;;;CO)
(A;CI;RPWPCCDCLCLORCWOWDSDDTSW;;;SY)(A;CI;RPLCLORC;;;AU)
(OA;CI;CR;edacfd8f-ffb3-11d1-b41d-00a0c968f939;;AU)



Now copy the following part:
 D:P(A;CI;RPWPCCDCLCLOLORCWOWDSDDTSW;;;

Copy the SID of the delegated group

```
PS C:\Users\LabAdmin> Get-ADGroup -Identity "TestGPOAdmins"

DistinguishedName : CN=TestGPOAdmins,OU=Groups,OU=Managed-Objects,DC=contoso,DC=com GroupCategory : Security
GroupScope : Global
Name : TestGPOAdmins
ObjectClass : group
ObjectGUID : 5e17cbb5-4039-4a99-86c1-906214b4809f
SamAccountName : TestGPOAdmins
SID : S-1-5-21-2367645265-33317674-1292933090-12603
```

 Place the SID of the group at the end of the copied part above. Which means that you will get something like this.

D:P(A;CI;RPWPCCDCLCLOLORCWOWDSDDTSW;;;S-1-5-21-2367645265-333317674-1292933090-12602)

Now copy the entire defaultSecurityDescriptor:

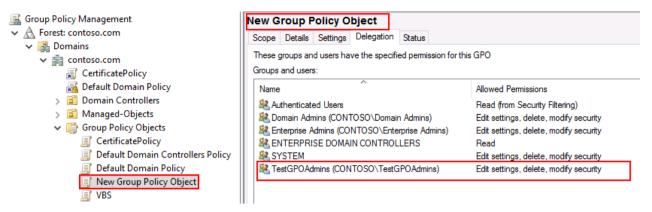
D:P(A;CI;RPWPCCDCLCLOLORCWOWDSDDTSW;;;S-1-5-21-2367645265-333317674-1292933090-12602)

 Paste it at the end of the defaultSecurityDescriptor at CN=Group-Policy-Container. It will look similar like this:

D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)
(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;ED)
(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)
(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;CO)

(A;;RPLCLORC;;;WD)D:P(A;CI;RPWPCCDCLCLOLORCWOWDSDDTS W;;;S-1-5-21-2367645265-333317674-1292933090-12602)

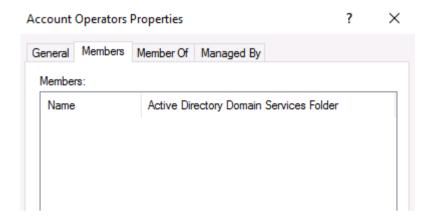
 Now when a user creates a GPO. The delegated group will be automatically added to it with Full permissions.



- If you want to allow the delegated group link GPO's as well. Give the following permissions on a OU:
- Write gpLink → Permission to link GPO's
- Write gpOptions → Permission to block inheritance

• 7.1 - Do not use Account Operators

Do not use Account Operators, because it has lots of rights out of the box. Users in Account Operators can potentially elevate to Domain Admin.



Attack path:

- Account Operators → GenericAll → Exchange Trusted Subsystem →
 Member of → Exchange Windows Permissions → WriteDacl on DNC =
 DCSync
- Account Operators → GenericAll → DnsAdmins → Executing a DLL as SYSTEM on the DC = Domain Admin

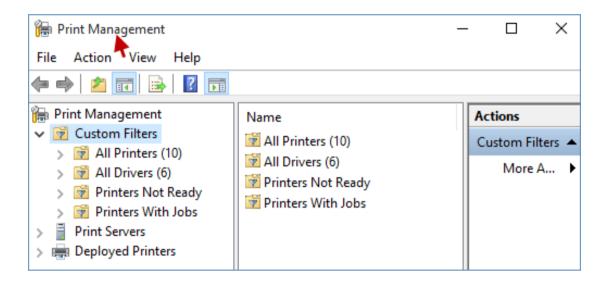
Reference: https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/from-dnsadmins-to-system-to-domain-compromise

Reference: https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/

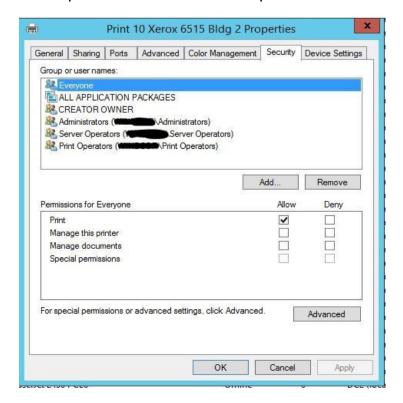
7.2 - Do not use Print Operators

Print Operators has by default logon rights to Domain Controllers and that is absolutely not needed for this group.

If you do use Print Operators. All the rights can be delegated as well through the Print Management, GUI.

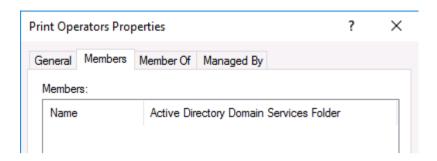


• Like this. You can add a new group to the DACL and assign the permissions that are required.



Recommendation

• Ensure that the Print Operators group is empty.



• 7.3 - Do not use Server Operators

Server Operators is a group that has lots of rights by default as well, which includes DC logon access. This group is often described as "DC Admins"

I would avoid using this group.

For more information: http://www.thenetworkencyclopedia.com/entry/server-operators-built-in-group/

7.4 – Turn on Active Directory Recycle Bin

Imagine that you accidentally deleted an object in Active Directory like the account of your CEO.

How great would it be if you could restore it again?

Active Directory Recycle Bin is by default **not** enabled. Enabling Recycle Bin would help you to recover a lot of scenarios, where someone accidentally ran a script and deleted tons of computer objects for example.

How to check if AD Recycle Bin is enabled?

Get-ADOptionalFeature -Filter 'name -like "Recycle Bin Feature"

As you can see. It is not enabled in my domain

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

```
PS C:\Users\Werner> Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target corp.contoso com WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=corp,DC=contoso,DC=com' is an irreversible action! You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=corp,DC=contoso,DC=com' if you proceed.

Confirm Are you sure you want to perform this action? Performing the operation "Enable" on target "Recycle Bin Feature".

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

- Recommendation
- · Turn on Active Directory Recycle Bin

```
PS C:\Users\Mark> Get-ADOptionalFeature -Filter 'name -like "Recycle Bin Feature"'

DistinguishedName : CN=Recycle Bin Feature;CN=Ontional Features;CN=Directory Service;CN=Windows NT,CN=Services;CN=Configuration,DC=corp,DC=contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Configuration,DC=corp,DC=contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Configuration;DC=corp,DC=contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Configuration;DC=corp,DC=contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Configuration;DC=corp,DC=contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Site-Name;CN=Sites;CN=Contoso,DC=com (CN=NTDS Settings;CN=DC,CN=Servers;CN=De fault-First-Sites;CN=DC,CN=Servers;CN=De fault-First-Sites;CN=DC,CN=Servers;CN=DC,CN=Servers;C
```

 7.5 - Delegate rights to Tier 1 admins to restore deleted objects

Tier 1 or 2 admins are creating objects, but sometimes. There might be cases where someone accidentally deleted an object.

By default Domain Admins or equivalent can restore deleted objects. Good news is that we can delegate this.

- First we have to take ownership of the CN=Deleted Objects container.
- Run PowerShell with DA privileges
- dsacls "CN=Deleted Objects,DC=corp,DC=contoso,DC=com" /takeownership

```
PS C:\windows\system32> dsacls "CN=Deleted Objects,DC=corp,DC=contoso,DC=com" /takeownership
Owner: CORP\Domain Admins
Group: NT AUTHORITY\SYSTEM

Access list:
{This object is protected from inheriting permissions from the parent}
Allow BUILTIN\Administrators SPECIAL ACCESS
LIST CONTENTS
READ PROPERTY
SPECIAL ACCESS
DELETE
READ PERMISSIONS
WRITE PERMISSIONS
CHANGE OWNERSHIP
CREATE CHILD
DELETE CHILD
LIST CONTENTS
WRITE SELF
WRITE SELF
WRITE PROPERTY
READ PROPERTY

The command completed successfully
PS C:\windows\system32>
```

• Now we are going to delegate the rights on the "Tier1" group to be able to restore objects.

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

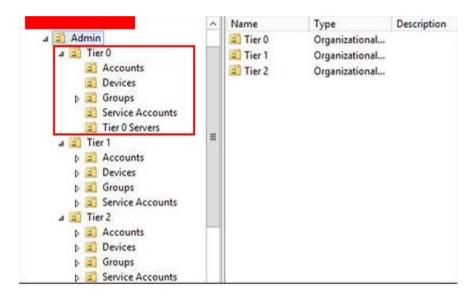
• Everyone that is now part of the Tier1 group can restore deleted objects.

7.6 - Tier 0 admins needs to be part of the "Protected Users" group

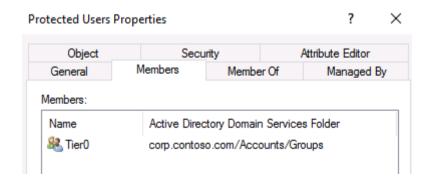
Protected Users is a global security group and its primary function is to prevent users' credentials being abused on the devices where they log in. Protected Users group features are supported on devices running Windows 8.1 and Windows Server 2012 (or higher).

Source: https://www.petri.com/windows-server-protected-privileged-accounts

• Tier 0 admins are usually the folks with access to the most critical resources, such as Domain Controllers, etc.



Add Tier 0 admins to the Protected Users, group.



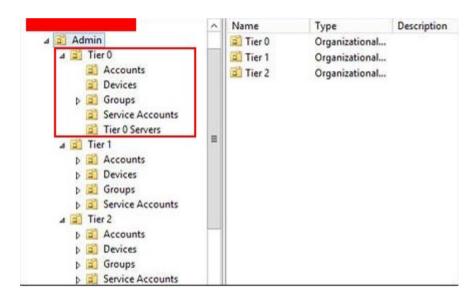
 7.7 - Tier 0 admins needs to have the "Account is sensitive and cannot be delegated" check mark

Account is sensitive and cannot be delegated ensures that an account's credentials cannot be forwarded to other computers or services on the network by a trusted application.

The feature that allows an application to act on behalf of a user is known as Kerberos Delegation.

Source: https://blogs.technet.microsoft.com/poshchap/2015/05/01/security-focus-analysing-account-is-sensitive-and-cannot-be-delegated-for-privileged-accounts/

Because Tier 0 admins are the folks with the highest privileges. It is recommended to enable this check mark for all Tier 0 admins.



Account is sensitive and cannot be delegated, check mark.

Account options.		
	Account is disabled	^
ı	☐ Smart card is required for interactive logon	
ı	Account is sensitive and cannot be delegated	
	Use only Kerberos DES encryption types for this account	v

7.8 - Reset the password of the KRBTGT twice

Every Active Directory environment has the "KRBTGT" account in Active Directory.

KRBTGT is service principal for the KDC that is responsible for encrypting and signing all the Kerberos tickets in a domain.

If an attacker has managed to get the NTLM hash of the KRBTGT account. Golden Tickets can be created to impersonate every user in the domain and remain persistence.

This often requires DA or equivalent privileges, so that means that an attacker already has domain dominance in your environment.

- Reset the password of the KRBTGT twice to make the Golden Ticket invalid for an attacker.
- When was the last time that you reset the password twice?

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

PS C:\windows\system32> Get-ADUser krbtgt -properties passwordlastset

DistinguishedName: CN=krbtgt,CN=Users,DC=corp,DC=contoso,DC=com
Enabled: False
GivenName: Name: krbtgt
ObjectClass: user
ObjectClass: user
ObjectGUID: de2a1c70-e8f1-4fb0-a720-32627866a213
PasswordLastSet: 1/18/2017 11:57:58 AM
SamAccountName: krbtgt
SID: S-1-5-21-3566662483-2648771335-1709913503-502
Surname: UserPrincipalName:
```

Recommendation

- Reset the KRBTGT account twice every half year. This has been discussed many of times, but a common industry best practice. Like STIG advises it. Reset it every 180 days.
- Make sure that there is a 10-24 hours delay before doing the second reset. In other words. Reset the password of the KRBTGT first and wait 10-24 hours before doing the second password reset. MS recommends this.
- What happens when you reset the password only once?

An attacker would still be able to use his Golden Ticket.

```
.#####. mimikatz 2.2.0 (x64) #18362 Dec 22 2019 21:45:22
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
 '## v ##'
                    Vincent LE TOUX
                                                      ( vincent.letoux@gmail.com )
                    > http://pingcastle.com / http://mysmartlogon.com ***/
  '#####'
mimikatz # kerberos::ptt ticket.kirbi
 File: 'ticket.kirbi': OK
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7C0A920A8
               Administrator: C:\WINDOWS\SYSTEM32\cmd.exe
mimikatz #
              Microsoft Windows [Version 10.0.17134.48]
              (c) 2018 Microsoft Corporation. All rights reserved.
              C:\x64>pushd \\DC\c$
              Y:\>cd Windows
              Y:\Windows>cd NTDS
               Y:\Windows\NTDS>dir
               Volume in drive Y is Boot Disk
               Volume Serial Number is E094-5822
               Directory of Y:\Windows\NTDS
```

What happens when you reset the password twice?

Golden Ticket becomes invalid.

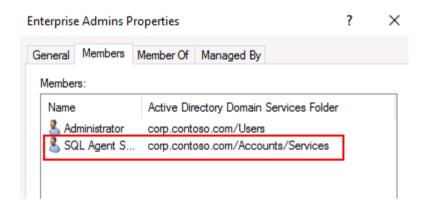
```
( vincent.letoux@gmail.com )
'## v ##'
              Vincent LE TOUX
              > http://pingcastle.com / http://mysmartlogon.com ***/
 "####"
mimikatz # kerberos::ptt ticket.kirbi
 File: 'ticket.kirbi': OK
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF6F89020A8
mimikatz #
            Administrator: C:\WINDOWS\SYSTEM32\cmd.exe
           Microsoft Windows [Version 10.0.17134.48]
           (c) 2018 Microsoft Corporation. All rights reserved.
           C:\x64>dir \\DC\c$
           Access is denied.
           C:\x64>pushd \\DC\c$
           Access is denied.
           C:\x64>
```

 8.1 – Monitoring High-privileged groups in Active Directory

High-privileged groups with the likes of Domain & Enterprise Admins are crucial to monitor, because attackers are likely going after this groups

Keep in mind that there are more high-privileged groups, which are often forgotten, such as Built-in\Administrators, Schema Admins, Account Operators, Backup Operators, Server Operators, Print Operators, DnsAdmins, Organization Management, Exchange Trusted Subsystems, Exchange Windows Permissions.

- Do you monitor when someone is added to the Enterprise Admins group for example?
- Here is a SQL service account added to the Enterprise Admins, group.



Recommendation

- Start monitoring high-privileged groups, but not just limited to Domain or Enterprise Admin group
- Event 4728 "A member was added to a security-enabled group" Monitor this event, because it could be sign of privileges abuse. Like
 adding service accounts to Domain Admin, etc.
- Event Properties Event 4728, Microsoft Windows security auditing.



8.2 - Deploy a honey user for Kerberoasting

We all might have heard of Kerberoasting. An attack that allows every authenticated user request service tickets of accounts with a servicePrincipalName.

With these service tickets they are able to export it and crack it offline. If you are curious about how to perform this attack.

Please take a look at: https://attack.stealthbits.com/cracking-kerberos-tgs-tickets-using-kerberoasting

This is the step of an attacker.

- Scanning accounts with a SPN
- Request service ticket(s)
- Export service tickets
- Crack service tickets

[Example]

• Attacker enumerates the Domain Admins group and discovers a service account with a SPN, which is in this case. "SQLAgent"

Attacker request the service tickets of the "SQLAgent" account.

- Event 4769 will show up in the Security logs. "A Kerberos service ticket was requested"
- As you can see. Mark has requested a service ticket from SQLAgent. This service account is our honey user.
- We Event Properties Event 4769, Microsoft Windows security auditing.

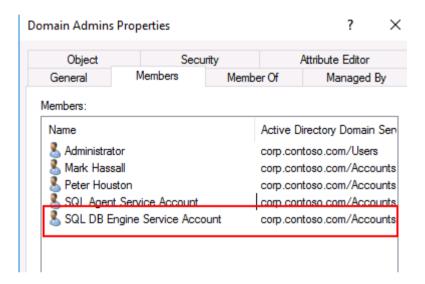


Recommendation

- Create a fake service account, but make it look real as possible.
- Assign a fake SPN to the account.
- Add the honey user to Domain Admin or something similar.
- Monitor when someone request a service ticket from your honey user account, 4769

[EXAMPLE]

I have added a honey user account into the Domain Admins, group.



Register a fake SPN on the honey user.

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

PS C:\windows\system32> setspn -s MSSQLSvc/corp.contoso.com:DBA:1334 SQLDBEngine
Checking domain DC=corp,DC=contoso,DC=com

Registering ServicePrincipalNames for CN=SQL DB Engine Service Account,OU=Services,OU=Accounts,DC=corp,DC=contoso,DC=cor
MSSQLSvc/corp.contoso.com:DBA:1334

Updated object
PS C:\windows\system32> _____
```

Here we can see that SQLDBEngine has now a fake SPN

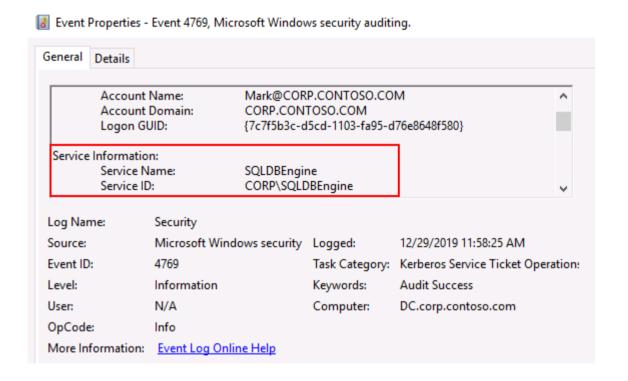
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> setspn -L SQLDBEngine
Registered ServicePrincipalNames for CN=SQL DB Engine Service Account,OU=Services,OU=Accounts,DC=corp,DC=contoso,DC=com:
MSSQLSvc/corp.contoso.com:DBA:1334

PS C:\windows\system32> _
```

Now when the attacker requests the SPN of our honey user.

- We can catch him or her.
- Here we can see that Mark has requested a service ticket from an account that is not mapped to anything in AD.



9.1 – Understand the concept of MS Administrative Tier Model

The purpose of MS Administrative Tier model is to reduce down credential by using different levels. Tier 1, 2 and 3.

Tier 0 = Domain Admins or equivalent that have access to the most critical servers like Domain Controllers, Azure AD, ADFS and PKI.

Tier 1 = Usually the server admins that can access different servers, such as file servers, print servers, exchange, etc.

Tier 2 = Workstation / Helpdesk admins that have access to the workstations of the clients.

Tier 0 admins can only access Tier 0 resources. Tier 1 admins can only access Tier 1 resources and Tier 2 admins can only access Tier 2 resources.

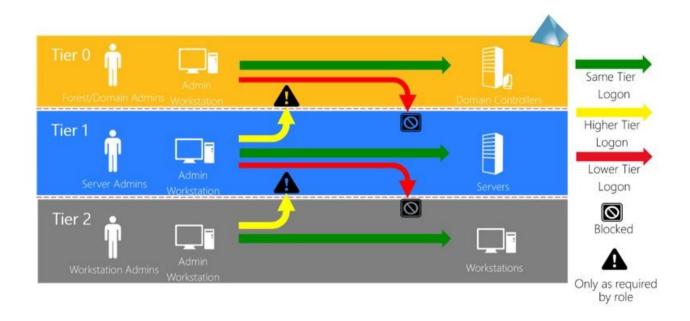
[Example]

An Tier 0 admin can't log on to a Tier 1 server or workstation, because he is not allowed to do so.

Tier 2 admins can't log on Tier 1 servers, because they are not allowed to.

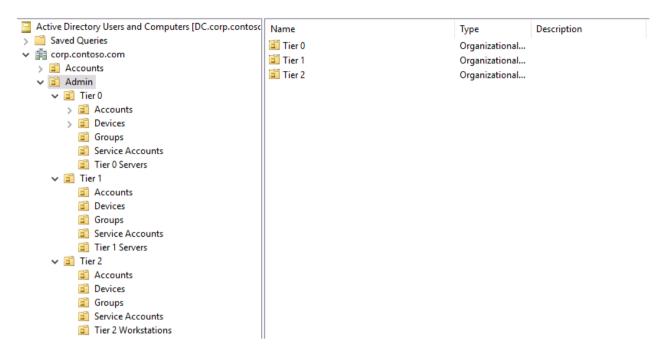
Tier 1 admins can't log on Tier 0 or Tier 2, etc.

Makes sense?



9.2 – How to design MS Administrative Tier Model?

First you need to create an OU structure that looks similar like this:



Tier 0

- Accounts = Accounts of all Tier 0 admins in Active Directory
- **Devices** = Computer Objects of all the Tier 0 admins.
- Groups = AD group for Tier 0 admins
- Service Accounts = Service accounts that run as a service on Tier 0 server(s)
- Tier 0 Servers = Computer Objects of Azure AD Connect, ADFS, PKI, NPS. etc.

Domain Controllers as well, but I suggest to leave them in the Domain Controllers OU.

Tier 1

- Accounts = Accounts of all Tier 1 admins in Active Directory
- **Devices** = Computer Objects of all Tier 1 admins.
- Groups = AD group for Tier 1 admins
- Service Accounts = Service accounts that runs as a service on Tier 1 server(s)
- **Tier 1 Servers** = Computer objects of File servers, print servers, SQL servers, etc. The rest of the servers in your environment.

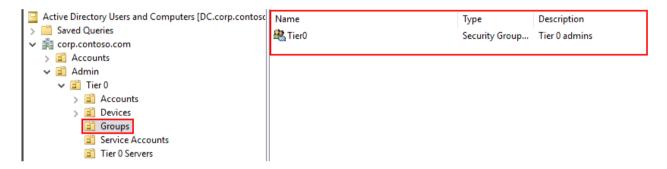
Tier 2

- **Accounts** = Accounts of all Tier 2 admins in Active Directory
- **Devices** = Computer Objects of all Tier 2 admins
- **Groups** = AD group for Tier 2 admins
- Service accounts = Service accounts that runs as a service on workstations of clients
- **Tier 2 Workstations** = Workstations of all the clients

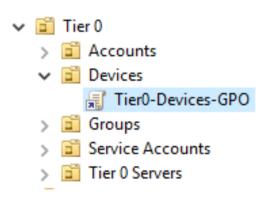
This is how it kinda looks like. It is a design, so you have a feeling how this model can be implemented. I will only guide it from a Tier 0 perspective. There are more different ways to approach this model.

[EXAMPLE]

- Create a group in the "Groups" OU of Tier 0.
- Add all the users that belongs to Tier 0 to this group.

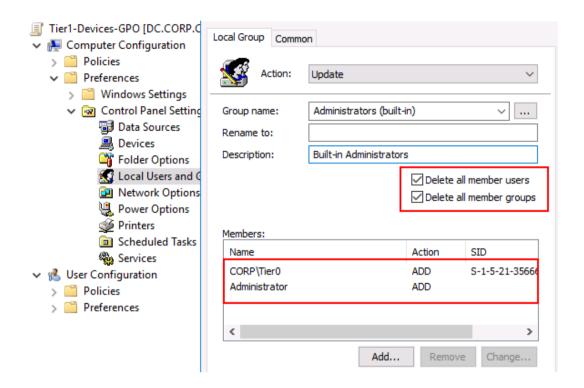


- Now we are going to create a GPO and link it to the "Devices" OU in Tier
- As you can see in the image. I have created a GPO and have linked it to the OU "Devices"



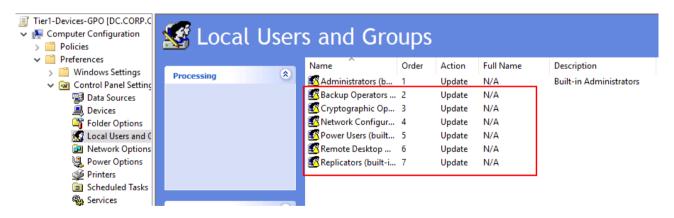
Now I am going to edit that GPO with the following settings:

On the devices of Tier 0 admins. Only the **local Administrator** account and the **Tier0** group should be **member of the local Administrators** group.

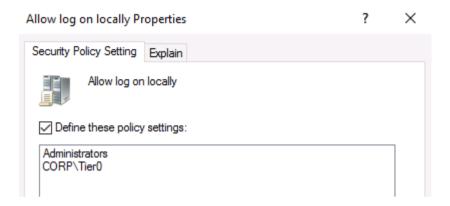


The following groups should be empty on the Tier 0 devices.

Backup Operators, Cryptographic Operators, Network Configuration Operations, Power Users, Remote Desktop Users, Replicators

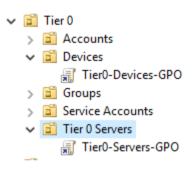


• At User Right Assignment – I have allowed Administrators and Tier0 users to be able to log on locally to the devices.



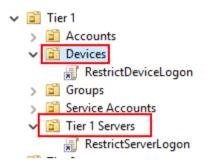
Now I am done this with this GPO.

Now I have to create a new GPO and link it to the "**Tier 0 Servers**" OU in Tier 0. This GPO is called "**Tier0-Servers-GPO**"



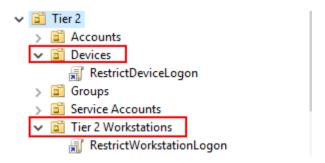
- This GPO should contains the same settings as the Tier0-Devices-GPO. Ensure that only the **local Administrator** and **Tier0 admins** are member of the **local Administrators** group **on the Tier 0 servers**.
- Ensure that the following groups are empty on the Tier 0 servers:
 Backup Operators, Cryptographic Operators, Network
 Configuration Operations, Power Users, Remote Desktop Users,
 Replicators

- Since we all know that Tier 0 admins are usually the Domain Admins or equivalent. We have to deny logon access to lower Tiers, which is in this case. Tier 1 & Tier 2.
- I have created two GPO's and linked it to the "Devices" and "Tier 1
 Servers" OU at Tier 1



Both GPO contains the following settings: <u>User Right Assignments</u>

- Deny access to this computer from the network: Domain Admins, Enterprise Admins, Schema Admins, Tier0
- Deny log on locally: Domain Admins, Enterprise Admins, Schema Admins, Tier0
- Deny log on through Remote Desktop Services: Domain Admins, Enterprise Admins, Schema Admins, Tier0
- Now I have linked the exact same GPO that is called "RestrictDeviceLogon" to the OU "Devices" in Tier 2
- I have created a new GPO with the exact same settings, but only with a different name, which is "RestrictWorkstationLogon" and I have linked this one to the "Tier 2 Workstations" OU



Recommendation

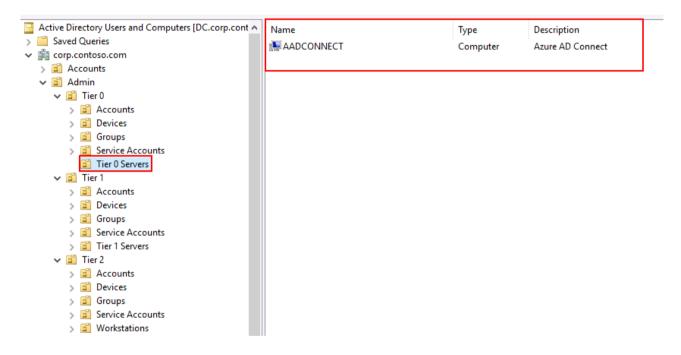
- In my example. I have only demonstrated it from Tier 0. You still need to ensure that Tier 1 their devices is in clean state, and that only the local Administrator and the Tier 1 group is part of the local Administrators group on the Tier 1 devices and Tier 1 servers.
- Besides of that, you need to ensure that Tier 1 admins cannot log on Tier 2 assets. Like for example, the devices of Tier 2 admins or the workstations from the clients.
- At the Tier 2 zone. Only the local Administrator & Tier 2 group should be part of the local Administrators group on the devices of Tier 2 admins and the workstations of the clients.
- I have created at every Tier an OU called "Service accounts" A nice example is that there are plenty of vendors claiming "DA" privileges or otherwise they won't support. Tier model helps to reduce down service accounts login into lower tiers.
- For more information: <u>https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material</u>

• 9.3 - Manage Azure AD Connect from a Tier 0 level

The Azure AD Connect server contains critical identity data and should be treated as a Tier 0 component as documented in the Active Directory administrative tier model.

Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites#azure-ad-connect-server

Here you can see that Azure AD Connect is managed from a Tier 0 operations.



Recommendations

- Manage Azure AD Connect from a Tier 0 operations. Attackers with local admin access to AAD servers are able to compromise an entire Active Directory domain.
- Azure AD Connect needs to be threaten as a second Domain Controller.

Source: https://blog.xpnsec.com/azuread-connect-for-redteam/

• All GPO's that are applied on Azure AD Connect needs to be managed from a Tier 0 operations or otherwise unauthorized users would be able to add themselves to the local Administrators group.

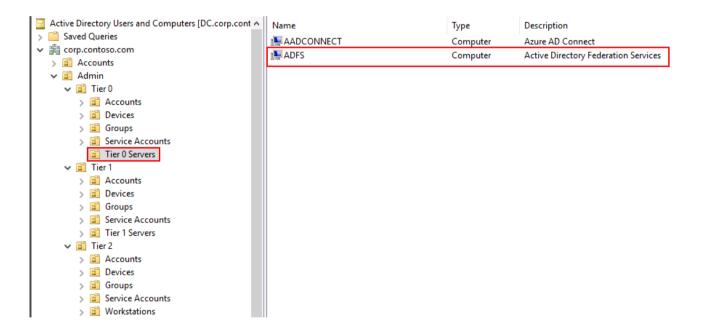
9.4 – Manage ADFS from a Tier 0 level

AD FS is, fundamentally, an authentication system. Thus, it should be treated as a "Tier 0" system like other identity system on your network.

Source:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/best-practices-for-secure-planning-and-deployment-of-ad-fs

Here you can see that ADFS is managed from a Tier 0 operations.



• Recommendations

- Start managing ADFS from a Tier 0 level
- Ensure that all the GPO's that are applied on the ADFS server(s) are managed from a Tier 0 level.

10.1 - Deploy Azure AD Password Protection

Azure AD Password Protection helps you to have a better overview of users, that use or pick poor passwords.

One of the cool things about Azure AD Password Protection is, that it's also available for on-premise, and not just for the Cloud.

We always had that problem where attackers were using different techniques, such as Password Spraying. Because users were picking poor passwords, and attackers love to after them.

Here in the image down below. You can see that the attacker had a few success by using "Password123456"

Password Spraying

```
PS C:\temp> Invoke-DomainPasswordSpray -UserList .\users.txt -Password 123456 -Verbose

[*] Using .\users.txt as userlist to spray with

[*] Warning: Users will not be checked for lockout threshold.

[*] The domain password policy observation window is set to 30 minutes.

[*] Setting a 30 minute wait in between sprays.

Confirm Password Spray

Are you sure you want to perform a password spray against 7 accounts?

[Y] Yes [N] No [?] Help (default is "Y"): y

[*] Password spraying has begun with 1 passwords

[*] This might take a while depending on the total number of users

[*] Now trying password 123456 against 7 users. Current time is 9:28 PM

[*] Writing successes to

[*] SUCCESS! User:Administrator Password:123456

[*] SUCCESS! User:spot Password:123456

[*] SUCCESS! User:spotless Password:123456

[*] Password spraying is complete
```

• **Credits:** https://ired.team/offensive-security-experiments/active-directory-password-spraying

NOTE: If you have plans to use Azure AD Password Protection for on-premise. It is only supported in public Cloud. Since there is no on-premise version for Azure AD Password Protection

Requirements

- Azure AD Premium P1 or P2
- All the Domain Controllers must run at least Windows Server 2012 or later to have the DC Agent Software installed
- All the Domain Controllers need to have Microsoft .NET 4.5 installed
- All the Member servers where Azure AD Password Protection Proxy service will be installed. Must run on a Windows Server 2012 R2 or later.
- All the Member servers with Azure AD Password Protection Proxy service must have Microsoft .NET 4.7 installed.
- Network connectivity must exist between at least one domain controller in each domain and at least one server that hosts the proxy service for password protection. This connectivity must allow the domain controller to access RPC endpoint mapper port 135 and the RPC server port on the proxy service
- All the Member servers where Azure AD Password Protection is installed must have network access to the following:

Endpoint	Purpose
https://login.microsoftonline.com	Authentication requests
https://enterpriseregistration.windows.net	Azure AD password protection functionality

 The list goes on, so please read here further: https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/authentication/howto-password-ban-bad-on-premises-deploy.md

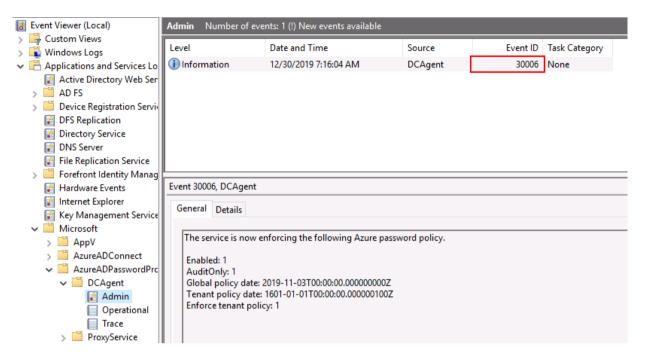
I'm going to assume that you have read the link and that you fully understand what you have to do first before deploying Azure AD Password Protection. It gives you an entire walkthrough.

https://techcommunity.microsoft.com/t5/ITOps-Talk-Blog/Step-By-Step-Implementing-Azure-AD-Password-Protection-On/ba-p/563342

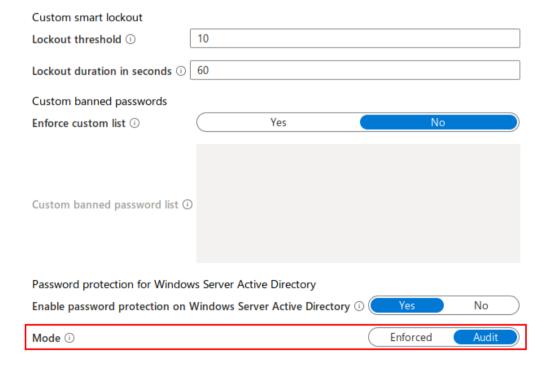
Please test this in a test environment, because there is a chance, that you will do something stupid.

NOTE: This is tested on a test environment.

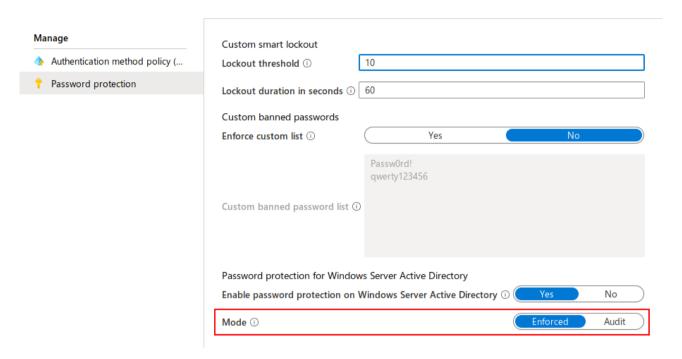
- If everything went well. You will now receive the following event at Microsoft-AzureADPasswordProtection-DCAgent/Admin
- **Event:** 3006 "The service is now enforcing the following Azure password policy"



· This is how my current setting looks like.



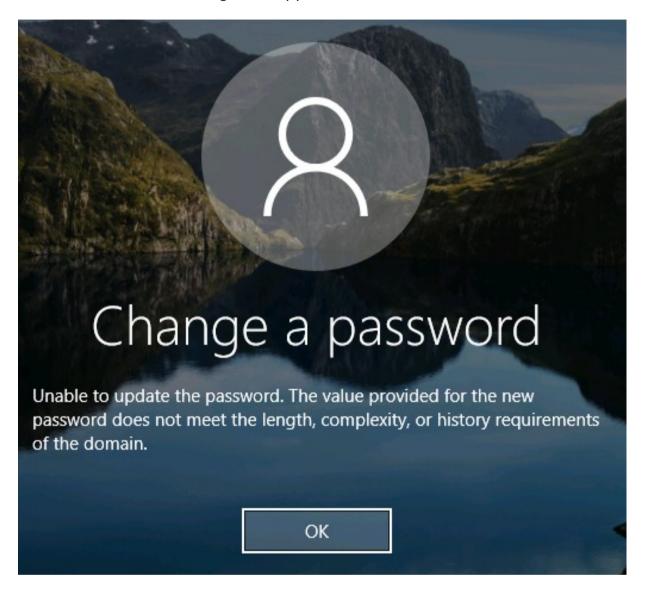
 Now I am going to change it to "Enforced" so instead of auditing. I will block banned passwords.



 Here is an example that the password of Amy has expired, so she needs to change her password.

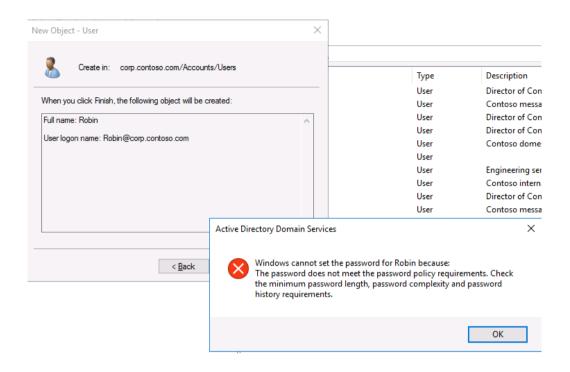


• When she decides to change her password to "Passw0rd!" or something similar. The following will happen.

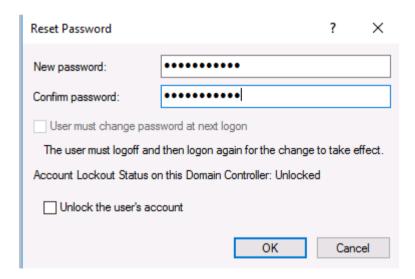


- The global banned password list is based of the following information that can be found here:
 - $\frac{https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/authentication/concept-password-ban-bad.md$

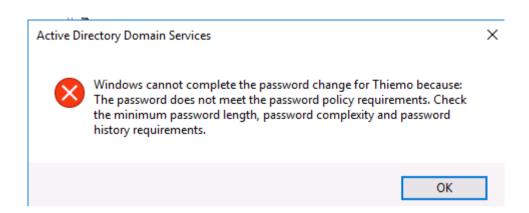
• When someone is creating a new user and decides to choose a poor password. The following message will be shown



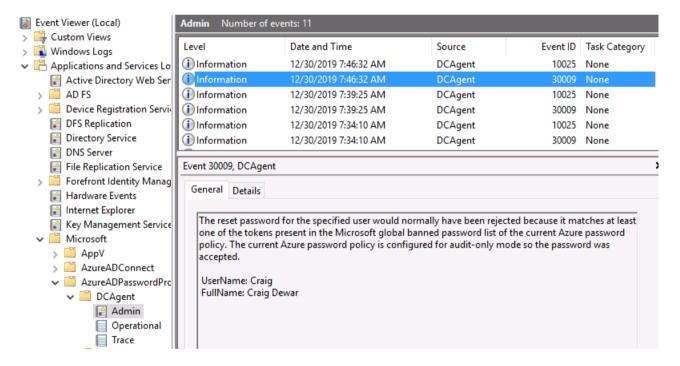
 When someone wants to reset a user his/her password and decides to choose a weak password...



The following message will show up

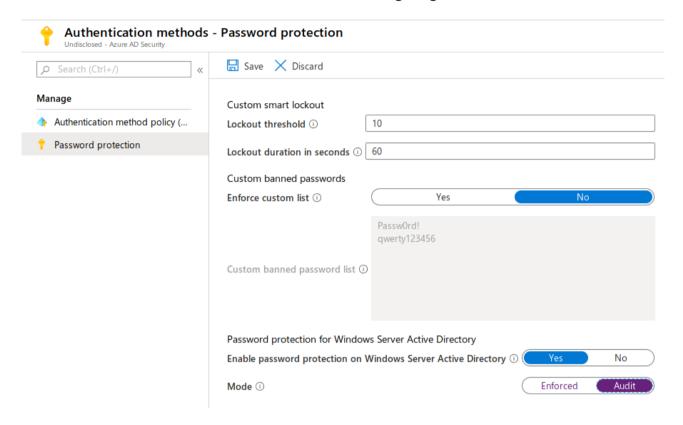


When you have it on audit mode. You will see event 3009 that it says
the password was accepted, but that the password was discovered in the
banned password list.



Recommendation

- · Start deploying Azure AD Password Protection if you haven't done it yet.
- Start with the "audit" mode first before going to "Enforce"



 Make sure that you first have deployed Azure AD Password Protection in a test environment to see if you fully understand the implementation. It is not that difficult, but it is always common that mistakes will be made, which is fine. We're all can learn from mistakes! 10.2 - Set a password for the Guest & DefaultAccount account

By default, **Guest** & **DefaultAccount** have no password in AD. Good news is that both accounts are disabled, but if someone enables them. They can log on those accounts.

Recommendation

Set a password for both accounts.

11.1 - Discretionary Access Control List

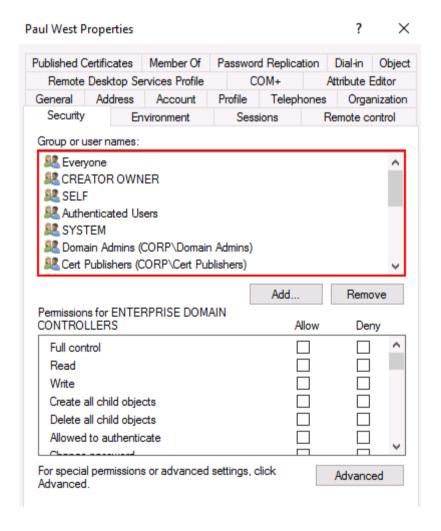
(DACL) An **access control list** that is controlled by the **owner** of an object and that specifies the **access** particular users or groups can have to the object.

Source: https://docs.microsoft.com/en-us/windows/win32/secgloss/d-gly

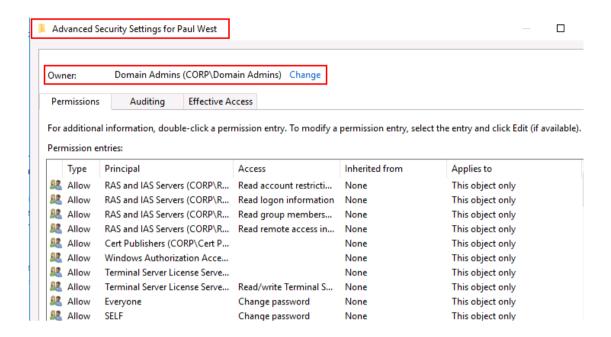
Example

Here we have a user that is called Paul West. The side that is marked as red defines the **ACL**, which identifies, which users or groups are assigned or denied permission to an object.

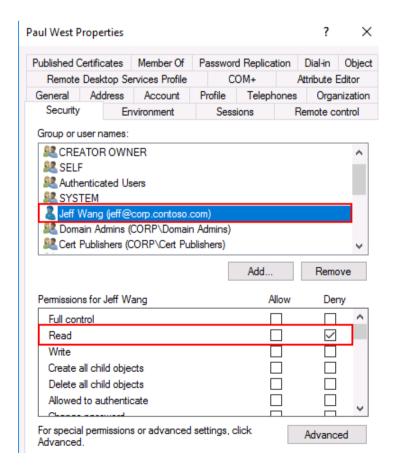
As you can see in the image. There are different groups that are assigned to the object, such as Authenticated Users, Cert Publishers and Domain Admins.



An **ACL** is controlled by the owner of an object. Which is in this example. Domain Admins.



Domain Admins has the rights to control the access of particular users and groups. Like for example denying read access to an object.



Example

Here I am logged in as the user **Mark** and I am going to do a query on the user **Paul**.

All the results will be displayed for Mark.

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

PS C:\Users\Mark> Get-ADUser Paul

DistinguishedName : CN=Paul West,OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com
GivenName : Paul
Name : Paul West
ObjectClass : user
ObjectGUID : bf048ac8-e67a-4dc1-8562-4edc0263aa38
SamAccountName : Paul
SID : S-1-5-21-3566662483-2648771335-1709913503-1107
Surname : West
UserPrincipalName : paul@corp.contoso.com
```

Here I am logged in as the user **Jeff** and I am going to do a query as well on the user **Paul**, but this time. I won't get any results. Because "Read" permission has been denied.

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

PS C:\Users\Jeff> Get-ADUser Paul
Get-ADUser : Cannot find an object with identity: 'Paul' under: 'DC=corp,DC=contoso,DC=com'.
At line:1 char:1
+ Get-ADUser Paul
+ CategoryInfo : ObjectNotFound: (Paul:ADUser) [Get-ADUser], ADIdentityNotFoundException
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,Microsoft.ActiveDirectory.Management.Commands.GetADUser

PS C:\Users\Jeff> ____
```

11.2 - Access Control Entries

Access control entries (**ACE**) are entries in an access control list containing information describing the **access rights** related to a particular security identifier or user.

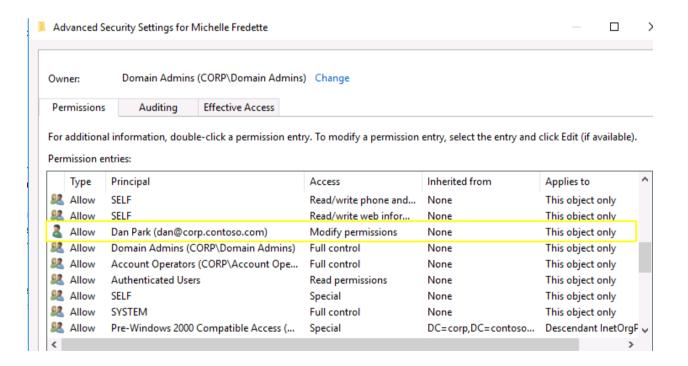
Source: https://www.techopedia.com/definition/24/access-control-list-acl-microsoft

Example

We have read at 11.1 that an **ACL** specifies the particular access, a user or group has on an object.

An **ACE** is an entry in the access control list that describes which access rights is assigned.

Here we can see that **Dan Park** has the rights to modify the permission (WriteDacl) of **Michelle** and is able to take her account over.



List of exploitable ACEs: https://wald0.com/?p=112

11.3 – Example of ACL based attack

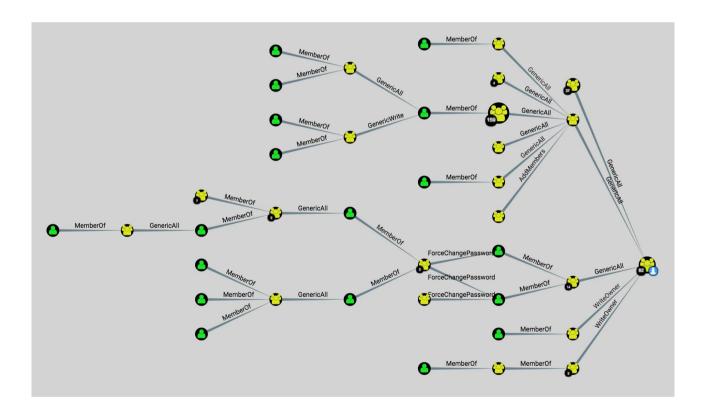
BloodHoundAD is a tool that maps out different attack paths in Active Directory based on exploitable ACL & ACEs.

The great thing about this tool is mainly the automation that it does for you. Instead of looking manually. It will show you all the different attack paths to Domain Admin for example.

I would highly encourage everyone to run this tool in their environment to see how "secure" their configuration is in Active Directory.

In most environments there is a lot of legacy from 5 or 10 years ago, which might shock you, when you run this tool. Perhaps Domain Users could become Domain Admin?

Find the tool here: https://github.com/BloodHoundAD/Bloodhound/wiki



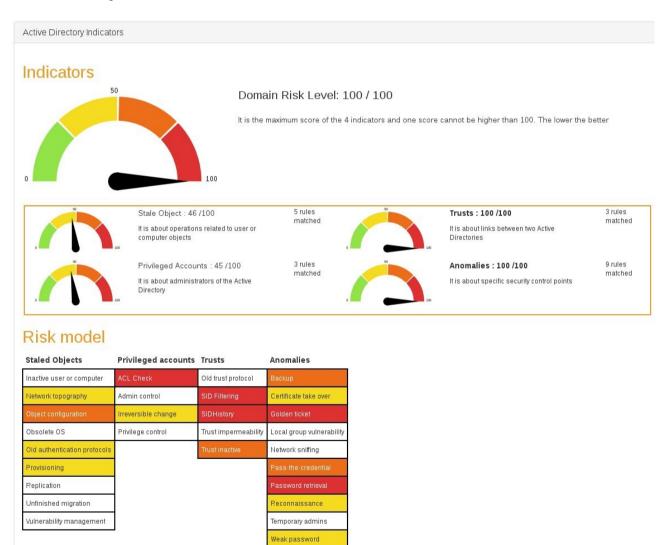
• 12.1 - PingCastle

PingCastle is a free, Windows-based utility to audit the risk level of your AD infrastructure and check for vulnerable practices.

This tool has been developed by Vincent Le Toux and it gives you a quick overview with nice dashboards to see your risk score in AD.

Download PingCastle: https://www.pingcastle.com/download/

Example



• 13 – Acknowledgment and References

- https://blog.fox-it.com/2018/04/26/escalating-privileges-with-acls-in-active-directory/
- https://wald0.com/?p=112
- https://adsecurity.org
- https://github.com/dafthack/DomainPasswordSpray
- https://github.com/nidem/kerberoast
- https://github.com/HarmJ0y/ASREPRoast
- https://github.com/gentilkiwi/mimikatz
- https://twitter.com/DirectoryRanger

I would like to thank all the authors for their write-ups or releases. It has increases the awareness of Active Directory and organizations are starting to pay attention to it.