

Author	Huy Kha
Contact	Huy_Kha@outlook.com

总结

本文档为组织提供了如何确保安全的指导
他们的活动目录。这包括备份、授权，
设计微软管理层模型等。
不是每个人都能负担得起昂贵的顾问费用，所以我决定在一个
不花你任何钱的文件，但是它需要一些努力
你方为这份文件而努力。因为这个医生会指导你
通过您需要采取的不同步骤来“亲身体验”，以降低风险
妥协。

• Foreword

无能，但这不再是一个惊喜。

许多有针对性的 ransomware 攻击都是通过活动目录来利用的

大多数组织甚至没有考虑他们自己的广告环境

设置。

广告一直被放在信息技术运营团队中，而且他们都经常

有自由以他们喜欢的方式管理它。因为没有人

真的很关心广告，直到他们最终像下面这样：

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 using the company's own Active Directory services against it.

Norsk Hydro cyber attack: What happened?

[Help Net Security](#) - 20 mrt. 2019

[Alle bekijken](#)

如果您有活动目录，大多数组织都有。你能

广告下跌 5 天后，生意还会进一步发展吗？

就像我之前说的。它通常管理得很差，是的。还有你管理的-

服务可能不会做得很好。

你知道广告中发生了什么不安全的变化吗？比如说

向域管理员添加密码不正确的服务帐户？

谁管理像域&这样的广告中的高特权群体

企业管理员。您的安全团队或 IAM 团队管理它吗

做所有决定的信息技术人员？

这些都是在你进一步之前值得问自己的问题。

从我迄今为止的职业经历来看：

...)

...)

...)

信息技术部门的每个人都是域管理员

信息技术人员在广告中做出所有决策，包括管理
团体。

拥有托管服务的公司大部分时间不受控制
广告中的变化。

• Introduction

1 -不安全的配置

- 1.1) -内置\具有 SPN 的管理员和域管理员帐户
- 1.2) -具有“不需要 Kerberos 预身份验证”的帐户
- 1.3) -与 DNC 上的写数据交换组
- 1.4) -默认域密码策略

2 - DHCP

- 2.1) -委派在 DHCP 服务器上授权的权限
- 2.2) -授权创建和删除子网和站点
- 2.3) -确保对 DHCP 进行备份并安全存储

3 -域名系统

- 3.1) - RBAC 与域名系统
- 3.2) -确保安全地备份和存储域名系统
- 3.3) -确保 DnsAdmins 组受到监控

4 -公钥基础设施

- 4.1) - RBAC 与公钥基础设施
- 4.2) -确保在公钥基础设施服务器和与广告客户服务相关的事件上启用审计
被转发到 SIEM

4.3) -确保对公钥基础设施进行备份并安全存储

5 域控制器

5.1) -确保将默认域控制器策略替换为更多

安全集中的 GPO。

5.2) -DSRM 作为碎玻璃账户

5.3) -确保在 DC 安装了视窗服务器备份或同等产品，以便

对域控制器进行备份

6 -集团政策

6.1) -在链接到 DC 的 GPO 中替换“已认证用户”

并在安全筛选中将“域控制器”组添加到其中

6.2) -链接到域控制器或域根需求的 GPO

由 0 级管理员管理。

6.3) -停止使用组策略创建者所有者

7 -活动目录

7.1) -不要使用账户操作员

7.2) -不要使用打印操作员

7.3) -不要使用服务器操作员，但也有例外

7.4) -打开活动目录回收站

7.5) -委托第 1 层恢复广告对象的权限

7.6) -第 0 层管理员需要属于“受保护用户”组

7.7) -第 0 层管理员需要拥有敏感且不能敏感的“”帐户

委派"勾号。

7.8) -重置 KRBTGT 帐户的密码两次

8 -监控

8.1) -监控广告中的高特权群体

8.2) -针对诸如 Kerberoasting 攻击之类的攻击部署蜂蜜用户

9 层管理模式

9.1) -了解微软管理层模型的目的

9.2) -如何设计微软管理层模型?

9.3) -确保从第 0 层管理 Azure 广告连接

9.4) -确保从第 0 层管理 ADFS 服务器

10 -其他

10.1) -为内部部署 Azure 广告密码保护

10.2) -在广告中为来宾帐户设置密码

11 -访问控制

11.1) -自由访问控制列表

11.2) -访问控制实体

11.3) -血迹斑斑

12 -广告审计工具

12.1) - PingCastle

13 -确认

13.1) -确认和参考

1.1 -内置\带 SPN 的管理员

内置\管理员是激活时创建的默认帐户

目录安装在第一个 DC。

该帐户存储在用户容器中，被视为

活动目录中权限最高的帐户，因为它是组的一部分，

例如域管理员和企业管理员。

不幸的是，这个帐户已经被(错误地)用于类似的不同任务

设置多个 SQL 服务器。

在这里，您可以看到管理员帐户有一个 SPN

The screenshot shows the 'Administrator Properties' dialog box with the 'Attributes' tab selected. The table lists various attributes and their values. The 'servicePrincipalName' attribute is highlighted with a red box.

Attribute	Value
revision	<not set>
rid	<not set>
roomNumber	<not set>
sAMAccountName	Administrator
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT)
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	MSSQLSvc/corp.contoso.com:DBA:1433
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>

- Why care?

域中每个经过身份验证的用户都能够请求服务票证

从这个内置的\管理员帐户。

现在，他们能够在本地导出服务票并离线破解

却没有被发现。

如果攻击者能够破解内置的管理员帐户。他或她有

王国的所有钥匙。因为该帐户是域的一部分

管理员，小组。

这是管理员帐户的 SPN

...)

Windows PowerShell

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

PS C:\Users\Mark> setspn -L Administrator
Registered ServicePrincipalNames for CN=Administrator,CN=Users,DC=corp,DC=contoso,DC=com:
MSSQLSvc/corp.contoso.com:DBA:1433
PS C:\Users\Mark> _
```

攻击者请求管理员帐户的服务票证

```
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 11:35:44 PM
ServicePrincipalName : MSSQLSvc/corp.contoso.com:DBA:1433
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

...)

攻击者导出服务票证，现在可以离线破解它，而无需

任何检测或账户锁定。

```
.#####. 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::list /export

[00000000] - 0x000000012 - aes256_hmac
Start/End/MaxRenew: 12/28/2019 5:12:22 AM ; 12/28/2019 3:12:22 PM ; 1/4/2020 5:12:22 AM
Server Name : krbtgt/CORP.CONTOSO.COM @ CORP.CONTOSO.COM
Client Name : Mark @ CORP.CONTOSO.COM
Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
* Saved to file : 0-40e10000-Mark@krbtgt~CORP.CONTOSO.COM-CORP.CONTOSO.COM.kirbi

[00000001] - 0x000000017 - rc4_hmac_nt
Start/End/MaxRenew: 12/28/2019 5:39:04 AM ; 12/28/2019 3:12:22 PM ; 1/4/2020 5:12:22 AM
Server Name : MSSQLSvc/corp.contoso.com:DBA:1433 @ CORP.CONTOSO.COM
Client Name : Mark @ CORP.CONTOSO.COM
Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardable ;
* Saved to file : 1-40a10000-Mark@MSSQLSvc~corp.contoso.com~DBA~1433-CORP.CONTOSO.COM.kirbi
```

• Recommendation

包含 SPN 的高特权帐户立即面临风险，因为

每个经过身份验证的用户都能够请求这些帐户的服务票据

并且可以离线破解。

建议使用大约 25 个字符的强密码

使用 SPNs 的服务帐户，但是既然我们谈论的是管理员

账户。它不需要有一个 SPN，因此请移除

管理员帐户。

以提升的权限运行 CMD(需要泛型写或等效的)

...)

...)

setspn -1 管理员

setspn -D MSSqlSvc/corp . contoso . com:DBA:1443 Administrator

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

PS C:\windows\system32> setspn -L Administrator
Registered ServicePrincipalNames for CN=Administrator,CN=Users,DC=corp,DC=contoso,DC=com:
    MSSQLSvc/corp.contoso.com:DBA:1433
PS C:\windows\system32> setspn -D MSSQLSvc/corp.contoso.com:DBA:1433 Administrator
Unregistering ServicePrincipalNames for CN=Administrator,CN=Users,DC=corp,DC=contoso,DC=com
    MSSQLSvc/corp.contoso.com:DBA:1433
Updated object
PS C:\windows\system32> _
```

我什么时候可以使用管理员帐户？

我会禁用此帐户，但仅将其用于以下任务：

...)

...)

...)

提升域控制器

提升域功能级别

添加新的域信任

1.2 - 带有 “” 的帐户不需要 Kerberos pre
身份验证 “”

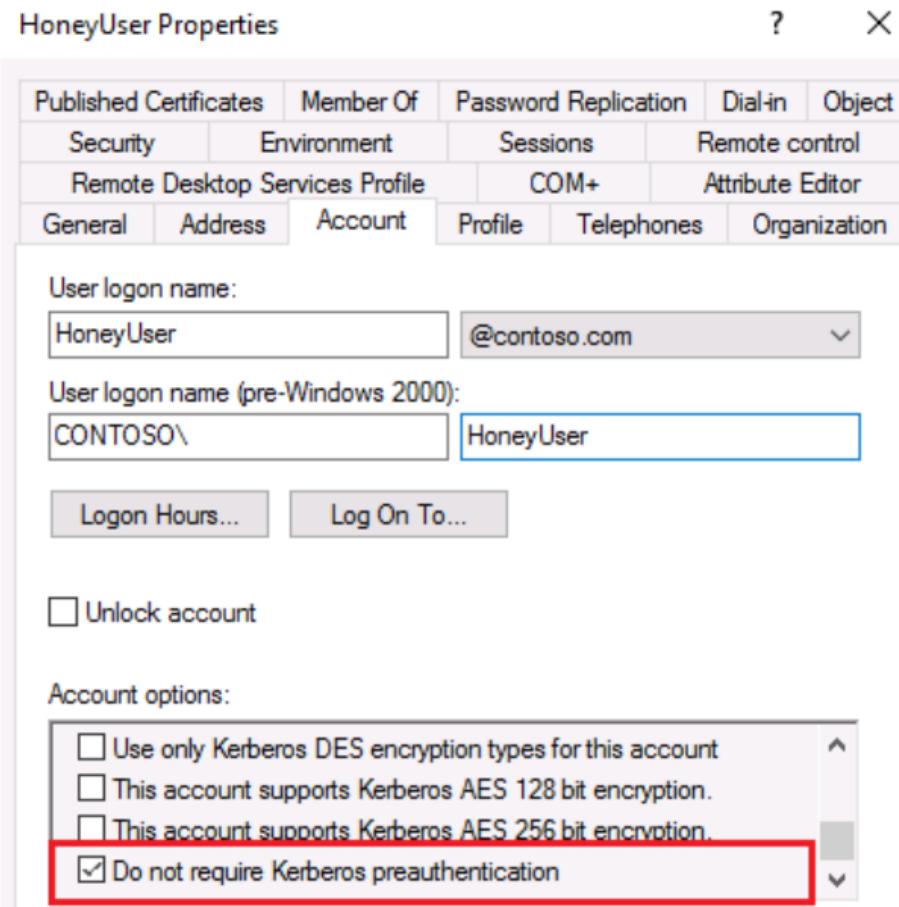
“不需要 Kerberos 预身份验证” 是

攻击者执行与 Kerberos 相关攻击，就像我上面在 1.1 中提到的

如果预认证被禁用。攻击者能够请求身份验证

来自域控制器和 DC 的数据将返回加密的 TGT

可以离线破解。



• Why care?

攻击者能够请求每个帐户的 TGT

身份验证已禁用，稍后可以在不被

检测到。

...)

攻击者执行侦察以发现具有预身份验证的帐户

有缺陷的

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

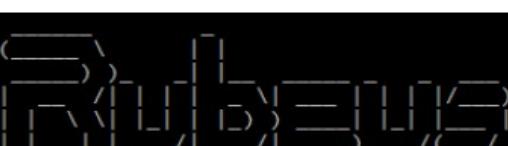
PS C:\windows\system32> get-aduser -LDAP "(&(objectCategory=person)(userAccountControl:1.2.840.113556.1.4.803:=4194304))" -properties DoesNotRequirePreAuth

DistinguishedName      : CN=HoneyUser,OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com
DoesNotRequirePreAuth  : True
Enabled                : True
GivenName               : HoneyUser
Name                   : HoneyUser
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
```

...)

攻击者请求易受攻击帐户的 TGT，并可以破解它

现在离线。



v1.4.2

```
[*] Action: AS-REP roasting
[*] Target Domain      : contoso.com
[*] SamAccountName    : HoneyUser
[*] DistinguishedName : CN=HoneyUser,OU=Employees,DC=contoso,DC=com
[*] Using domain controller: contoso.com (192.168.1.100)
[*] Building AS-REQ (w/o preauth) for: 'contoso.com\HoneyUser'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:
$krb5asrep$HoneyUser@contoso.com:469066FFA3CFEE49A254D642CB8C3393$D63D3233603A99
777B5D2F3ECF463B221B36526C651B77B9D8CBB7997927B838BB7540D3C2FB04BDA0473F9C33446E
3393A3BD79C6C120C22CB3F6F2CAAA6FA571B2BADA7EBFB717B2DBD6DC7CF88CC00BAEAF8EB76AF
6544A39E17BC531B4BC89A1313CEC7CDE1151420694E62BF3A535AACF278B3AB0111F7EA34B226FC
5A81479EC3E9580E2E7696D250459915D2AC6487FA08646762AA34731C875550D3B1535987B91EF6
0D4E77B38D714FDD98D37EF7FA4E68148ED6E0EB43DF3C0C290B7795B4243E5F86757AF6445CD57C
81663EC4645641EADD10CA22EB7B4C79FD25315104E83CAB8318BE
```

...)

事件 4768“请求 Kerberos 身份验证票证(TGT)”将

显示在 DC 的安全事件日志中。

• Recommendation

我将从发现禁用预认证的帐户开始

看看那些账户是否还在使用。如果没有，请启用 pre

再次验证。

...)

get-aduser-LDAP”(&(对象类别=人)

(用户帐户控制:1 . 2 . 840 . 113556 . 1 . 4 . 803:= 4194304))-属性

不需要验证

```
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

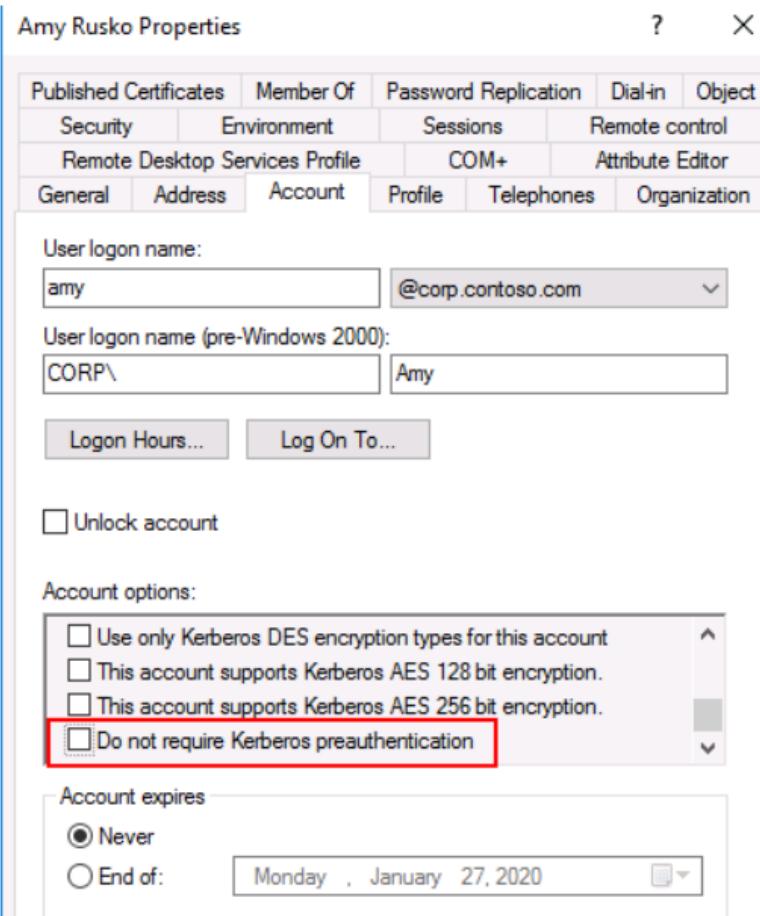
DistinguishedName      : CN=HoneyUser,OU=Users,OU=Accounts,DC=corp,DC=contoso,DC=com
DoesNotRequirePreAuth  : True
Enabled                : True
GivenName               : HoneyUser
Name                   : HoneyUser
ObjectClass             : user
ObjectGUID              : 7222fc79-ba57-4b11-87db-e50247488e9e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

...
```

您可能会发现已禁用预身份验证的服务帐户，

因为兼容性的原因，但是如果你发现

禁用预身份验证的普通帐户。再次启用它！



1.3 -在 DNC 上使用 WriteDacl 交换组

默认情况下，世界上大多数组织都有一个交易所

十年前安装的。

默认情况下，Exchange 在广告中拥有许多权限，这些权限在

环境。即使在域名上下文中或被称为域

根。

corp.contoso.com Properties

General Managed By Object Security Attribute Editor

corp.contoso.com

Domain name (pre-Windows 2000): CORP

Description:

Domain functional level: Windows Server 2012 R2

Forest functional level: Windows Server 2012 R2

在 DNC 上与 WriteDacl 交换窗口权限

Permission Entry for corp

Principal: Exchange Windows Permissions (CORP\Exchange Windows Permissions) Select a principal

Type: Allow

Applies to: This object and all descendant objects

Permissions:

- Full control
- List contents
- Read all properties
- Write all properties
- Delete
- Delete subtree
- Read permissions
- Modify permissions
- Modify owner
- Delete msImaging-PSPs objects
- Create MSMQ Queue Alias objects
- Delete MSMQ Queue Alias objects
- Create msPKI-Key-Recovery-Agent objects
- Delete msPKI-Key-Recovery-Agent objects
- Create msSFU30MailAliases objects
- Delete msSFU30MailAliases objects
- Create msSFU30NetId objects
- Delete msSFU30NetId objects

• Why care?

组织在 DNC 上委派组是一个常见的错误，

我不建议你这么做。

除了交换窗口权限和交换信任

子系统。我建议您寻找其他有权限的组

例如泛型、泛型写、WriteDacl 和 WriteOwner

...)

get-Acl-Path " AD:\ OU =域

控制器， DC =公司， DC=contoso， DC = com“|选择-对象-

扩展属性访问

...)

将受信任子系统与后代组上的写数据交换

目标

ActiveDirectoryRights	:	ReadProperty, WriteDacl
InheritanceType	:	Descendents
ObjectType	:	00000000-0000-0000-0000-000000000000
InheritedObjectType	:	bf967a9c-0de6-11d0-a285-00aa003049e2
ObjectFlags	:	InheritedObjectTypePresent
AccessControlType	:	Allow
IdentityReference	:	CORP\Exchange Trusted Subsystem
IsInherited	:	True
InheritanceFlags	:	ContainerInherit
PropagationFlags	:	InheritOnly

在 DNC 上与 WriteDacl 交换窗口权限

ActiveDirectoryRights	:	ReadProperty, DeleteTree, WriteDacl
InheritanceType	:	All
ObjectType	:	00000000-0000-0000-0000-000000000000
InheritedObjectType	:	00000000-0000-0000-0000-000000000000
ObjectFlags	:	None
AccessControlType	:	Allow
IdentityReference	:	CORP\Exchange Windows Permissions
IsInherited	:	True
InheritanceFlags	:	ContainerInherit
PropagationFlags	:	None

攻击者能够修改域名控制器上的权限，以授予每个

DS-复制-获取-更改& DS-复制-获取-示例

更改-同步域凭据的所有权限

控制器并成为域管理员。

• Recommendation

如果您运行的是 2013-2019 年的交易所。有办法解决这个问题

问题在于安装了最新的累积更新。

更多信息：

<http://support.Microsoft.com/en-us/help/4490059/using-shared-permissions-model-to-run-exchange-servers>

模型到运行交换服务器

解决这个问题的第二种方法是，当您完全迁移完

整个交换环境连接到办公室 365，并且您不使用任何打开的

前提。从两个交换组中删除 DNC 上的写数据。

当您拥有 2010 年交易所时会发生什么？

我已经根据自己的经验测试过了，当你删除 WriteDacl 时

来自交换信任子系统。它将在中打破一个小功能

Exchange，它通过

Exchange 管理控制台。

这可以通过在 OU 的后代用户上委派 WriteDacl 来解决，

存储所有邮箱账户的。这意味着你必须这么做

而不是使用交换管理控制台。

据我所知。正在删除中的 Exchange 窗口权限的写操作

Exchange 2010 没有造成任何问题。

不允许在 DNC 上有写数据的交换组。这就成功了

攻击者更容易泄露您的广告。

1.4 -默认域密码策略

默认情况下，广告的域密码策略是 7 或 8 个字符，可以是

在过去发生的所有违规事件中被认为是“不安全的”。

弱密码在大多数环境中很常见，建议

将密码策略增加到 12 或 14 个字符。

这是大多数环境的默认密码策略

网络帐户/域

```
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?

弱密码被认为是不安全的，攻击者喜欢弱密码。

有一种被称为“密码喷洒”的攻击，有人循环使用

整个域中的密码来查看是否有人使用了错误的密码，

例如“瓦奇伍德”

在这里，我在广告中创建了四个用户，密码是“沃希伍德”。

Name	Type
Alice Ciccu	User
Ben Smith	User
Don Jones	User
User1	User
User2	User
User3	User
User4	User

...)

对 8 名用户的密码喷雾攻击，其中 4 人已被破解

这个例子。

```
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
```

• Recommendation

这可能是一个挑战，但如果可能的话。将密码策略增加到

大约 12 或 14 个字符。这是一项艰巨的任务，因为许多政治

这样做时会涉及原因。

2.1 -授权给 DHCP 服务器

信息技术人员需要“数据助理”权限的一个常见原因是

因为他们需要授权给 DHCP 服务器，但不幸的是。这是

默认仅允许域管理员或等效人员使用。

这意味着它需要授权。大多数组织都做过吗

这个。没有。

DHCP 的所有元数据都存储在网络服务容器中。像你一样

可以在下面的截图中看到。

The screenshot shows the 'Active Directory Sites and Services' snap-in window. The left pane displays a tree view of network services under 'Active Directory Sites and Services'. The 'Services' node is expanded, and its child node 'NetServices' is highlighted with a red box. The right pane is a table listing network services with their names and types:

Name	Type
dc.contoso.com	dHCPClass
DhcpRoot	dHCPClass

...)

在这里，您可以看到网络服务的 DACL 只包含两个

ACE 具有通用或同等权限。在这种情况下。

域和企业管理员。

Advanced Security Settings for NetServices

Owner: Enterprise Admins (CONTOSO\Enterprise Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Enterprise Admins (CONTOSO\Enterprise Admins)	Special	None	This object only
Allow	Domain Admins (CONTOSO\...)	Special	CN=Configuration,DC...	This object and all descendant...
Allow	Enterprise Admins (CONTOSO\...)	Full control	CN=Configuration,DC...	This object and all descendant...

• Recommendation

创建允许授权给 DHCP 服务器的新组。

...)

...)

...)

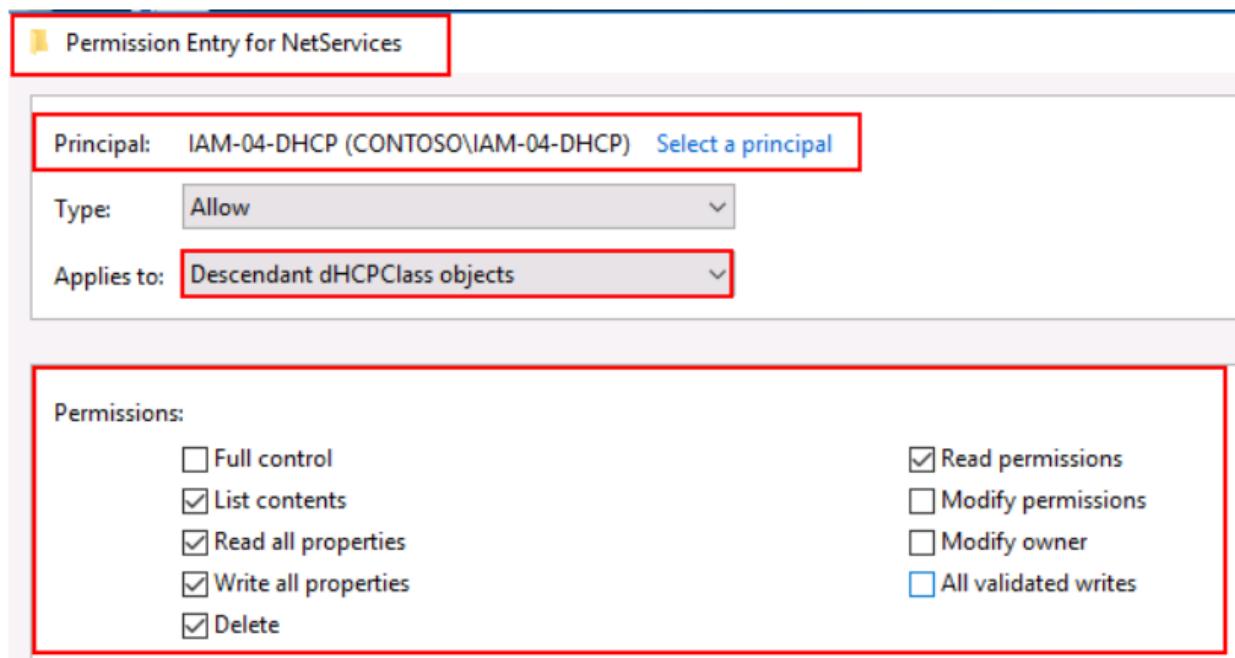
打开 ADSI。编辑

转到以下位置:CN =配置→CN =服务→CN =网络服务

→属性→安全性→添加委派组→高级→编辑→

后代 dHCPClass 对象

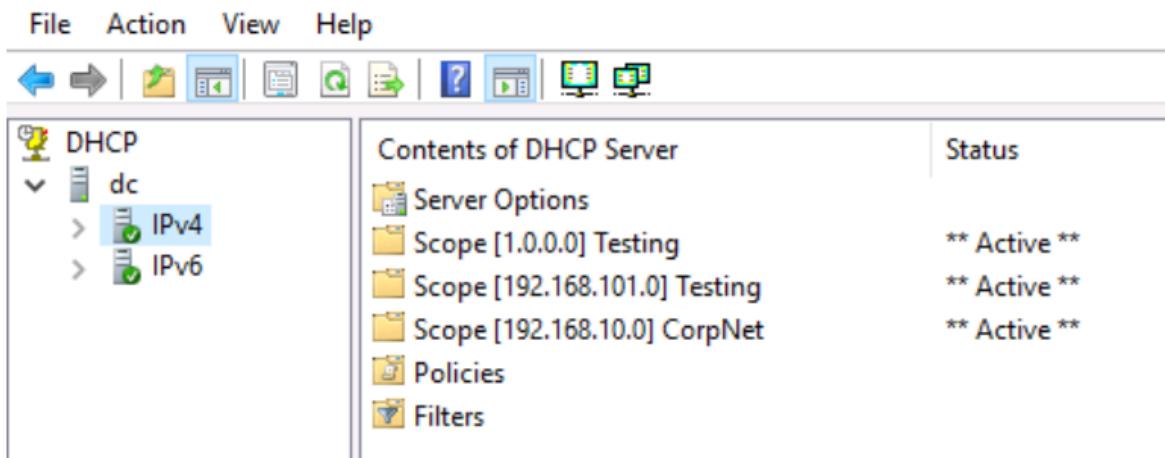
选择下面的以下权限:



...)

现在，授权组中的所有用户都可以授权

DHCP 服务器。



2.2 -授权创建/删除网站和子网

我们已经创建了一个组，并将它委托给了网络服务容器

允许在没有域管理员的情况下授权给所有的 DHCP 服务器

特权。

默认情况下，创建新站点或子网。也需要有“DA”，但是

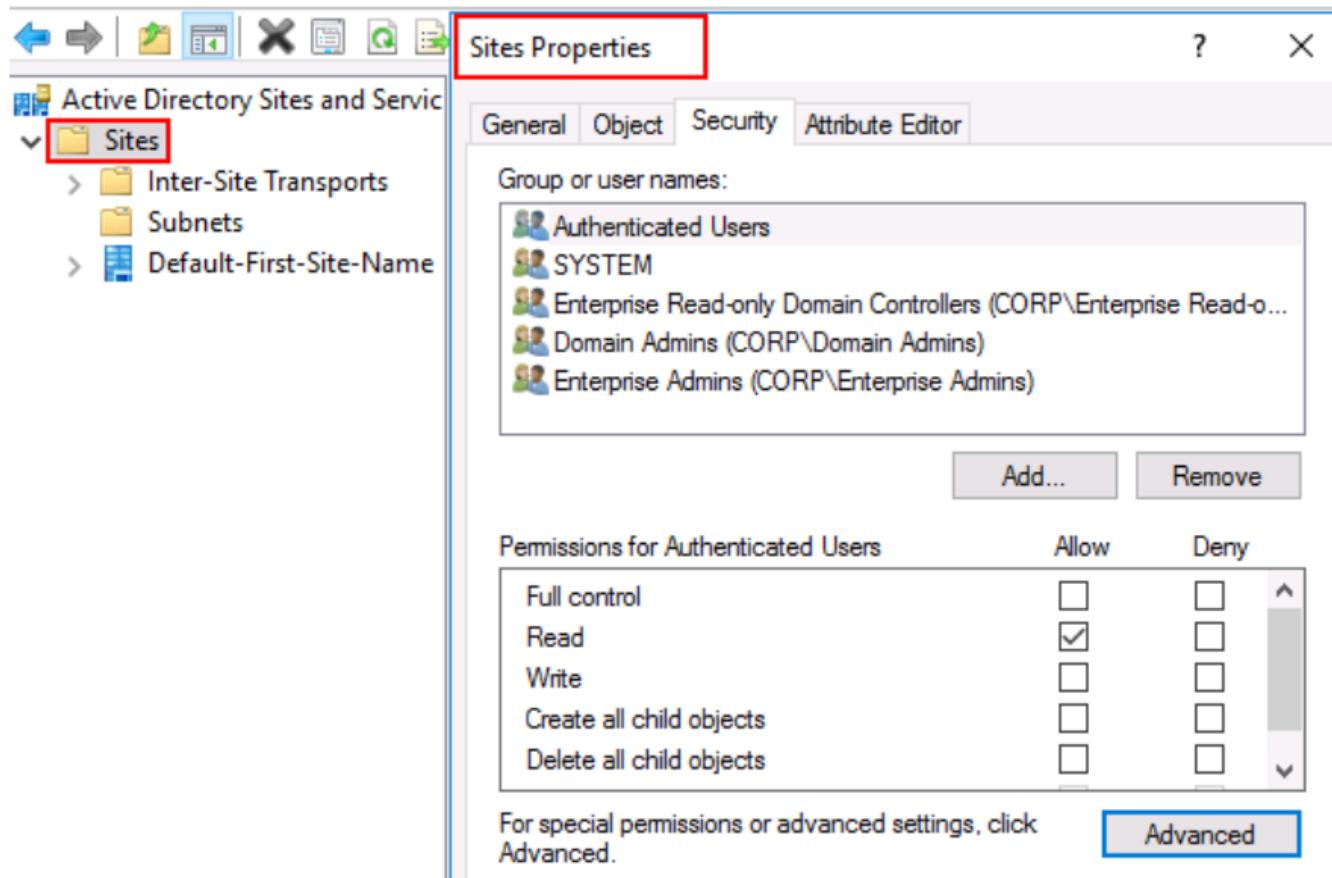
这很容易委派。

...)

在这里，我们可以看到当我们扩展网站容器时。它

包含另外两个类似“站点间传输”的容器

“子网”



• Recommendation

使用您之前创建的委派组，并授予它

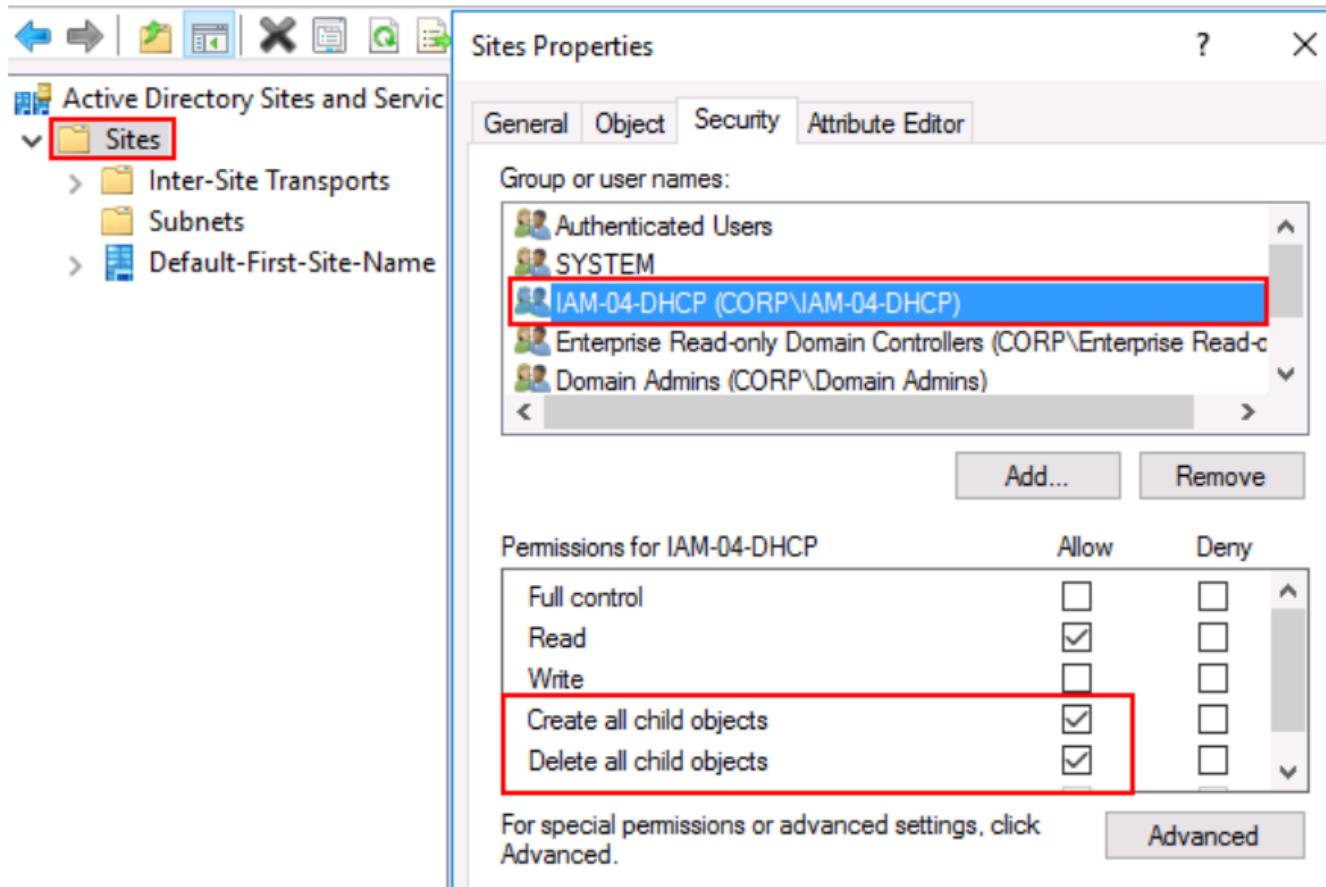
CN = 站点容器上的以下权限:

...)

...)

创建所有子对象

删除所有子对象



现在不再需要域管理员或等效人员来创建或删除

站点和子网。

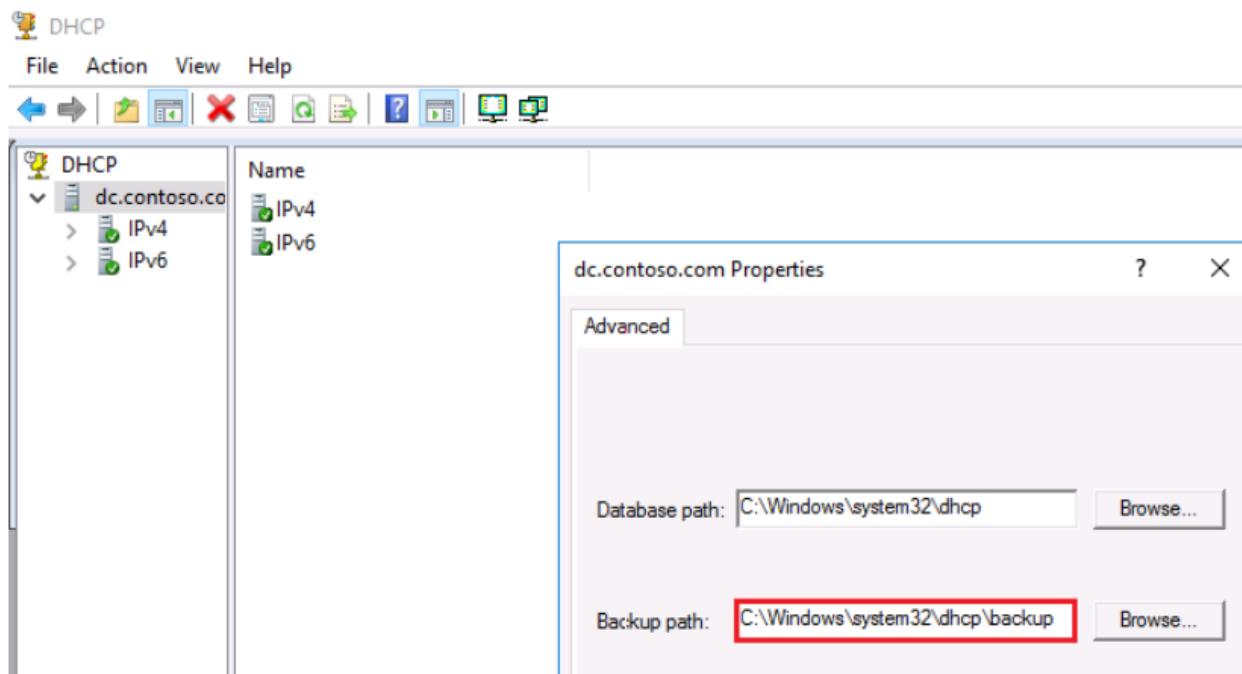
2.3 -确保对 DHCP 进行备份和存储 安全地

备份是至关重要的，尤其是在分布式哈希表和分布式哈希表上，因为分布式哈希表允许

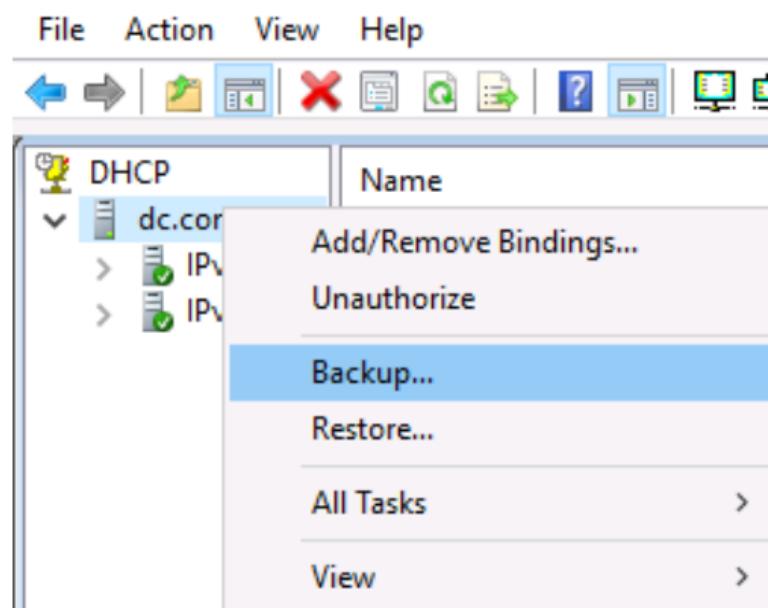
通过分配 IP 地址参与网络的设备，并提供

有效地址的目录查找。

DHCP 的备份路径是:C:\窗口\System32\dhcp\backup

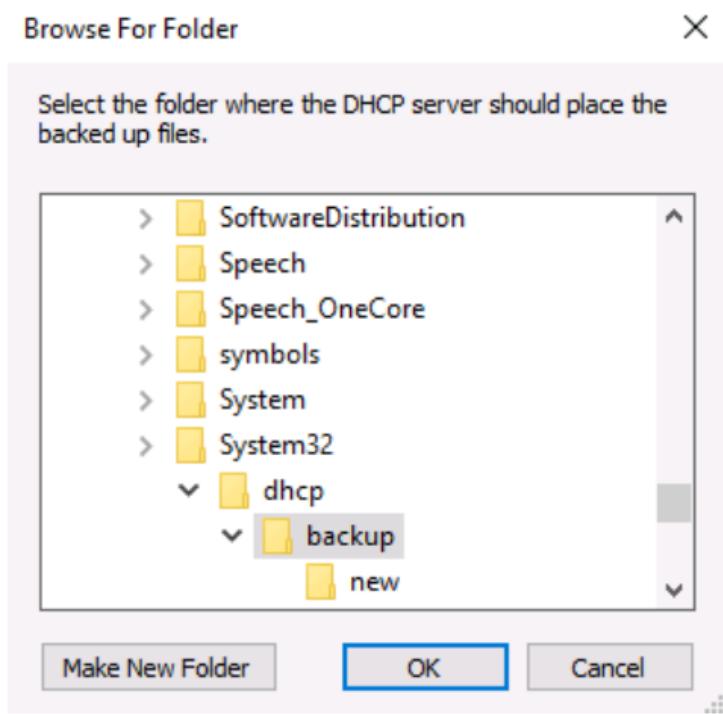


授权到 DHCP 服务器，然后单击“备份”



...)

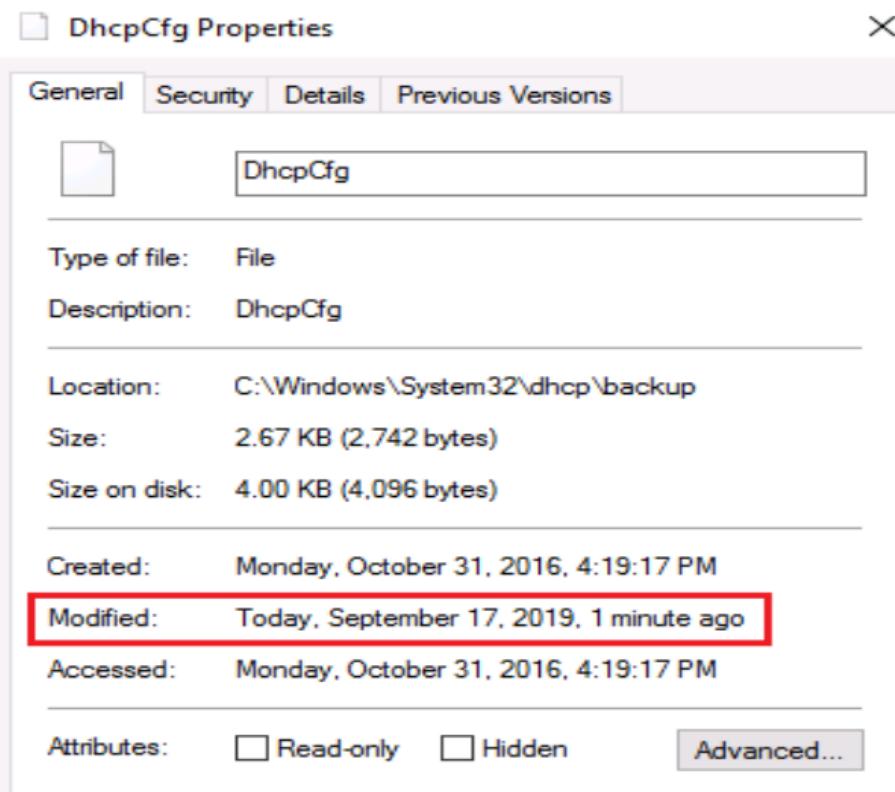
现在将备份存储在以下位置:C:\窗口\System32\
dhcp\backup



...)

当访问 DHCP 备份的目录文件夹时。你可以看到

DHCP 的备份已经完成。



• Recommendation

...)

...)

从开发一个对 DHCP 进行备份的过程开始，如果您

还没做过。比如我们什么时候备份 DHCP?

从练习恢复开始。你能多快

发生灾难时，是否恢复 DHCP 备份?

所有的 DHCP 备份都至关重要，应该存储在本地服务器上

没有加入广告。

3.1 -带有域名系统的 RBAC

从在活动目录中创建两个新组开始:

...)

...)

DnsManagers

DnsCreators

Name	Type	Description
DnsCreators	Security Group - Global	
DnsManagers	Security Group - Global	

The screenshot shows the Active Directory Users and Computers console. On the left, the navigation pane shows 'Active Directory Users and Computers [DC.corp.contoso.com]'. Under 'corp.contoso.com > Accounts', there is a red box around 'DNS Groups'. In the main pane, a table lists two security groups: 'DnsCreators' and 'DnsManagers', both of which are 'Security Group - Global'.

管理域名系统通常不需要域名解析器，因为大多数任务都可以

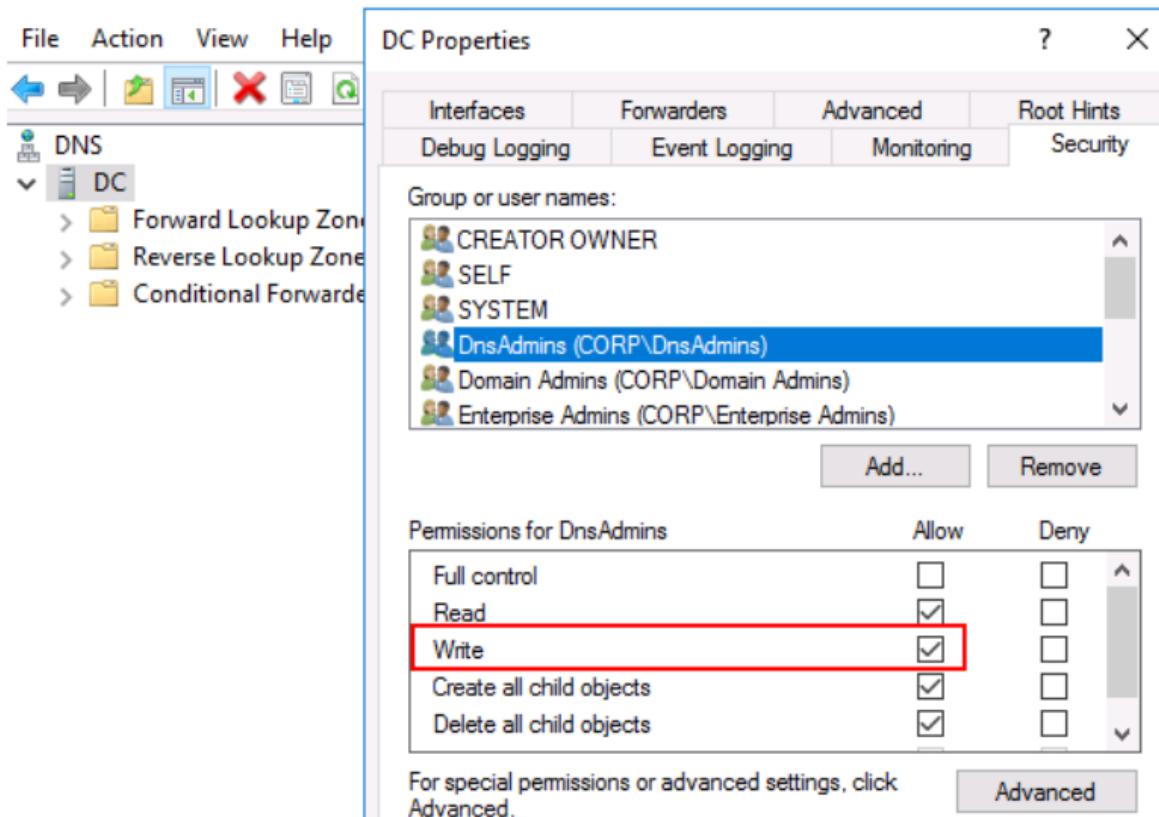
委托。

因为 DnsAdmins 有权在 DC 以系统的形式执行动态链接库。它

成为攻击者从域名升级到域名的重要目标

管理员。所有在 DC 域名系统对象上具有通用写或等效功能的用户都可以

执行这次攻击。



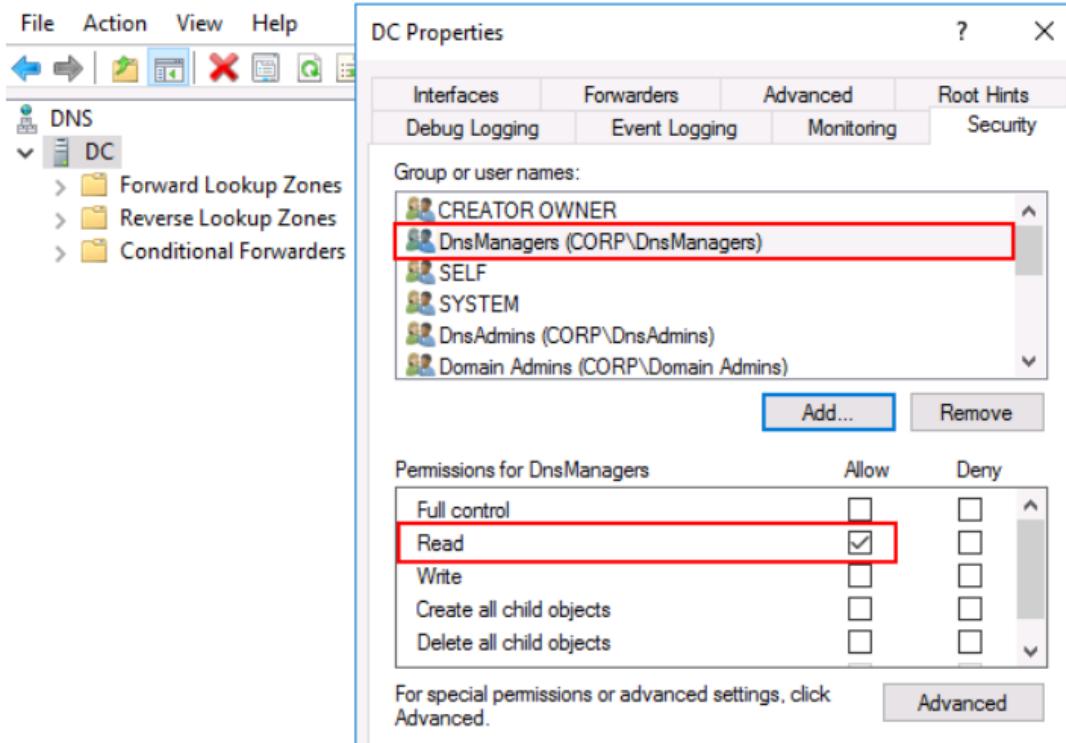
DnsAdmins	DnsManagers	DnsCreators
配置 调试/事件 记录	创建新的 记录，例如 MX、CNAME、美国、美国汽 车协会等。	创建新的 记录，例如 MX、CNAME、美国、美国汽 车协会等。
配置域名系统 服务器	删除已创建的 记录	删除已创建的 记录
创建新的 向前/向后 查找区域	读取域名系统事件 日志	
创建新的 有条件的 短材集运机	通用全部开启 现有域名系统 记录	
清除(域名系统)缓存	启动、停止和 暂停前进	

	查找区域	
开始、停止、暂停 并重新启动 DNS 服务器	更改区域 类型(例如初级、 存根和 次要)	
	允许 用户/组到 管理 正向查找 区域	
	允许区域 转移	
	添加/删除名称 服务器	
	变化 老化/清除 性能	
	更改的 TTL 正向查找 地区	
	在区域上签名 DNSSEC	

DnsManagers

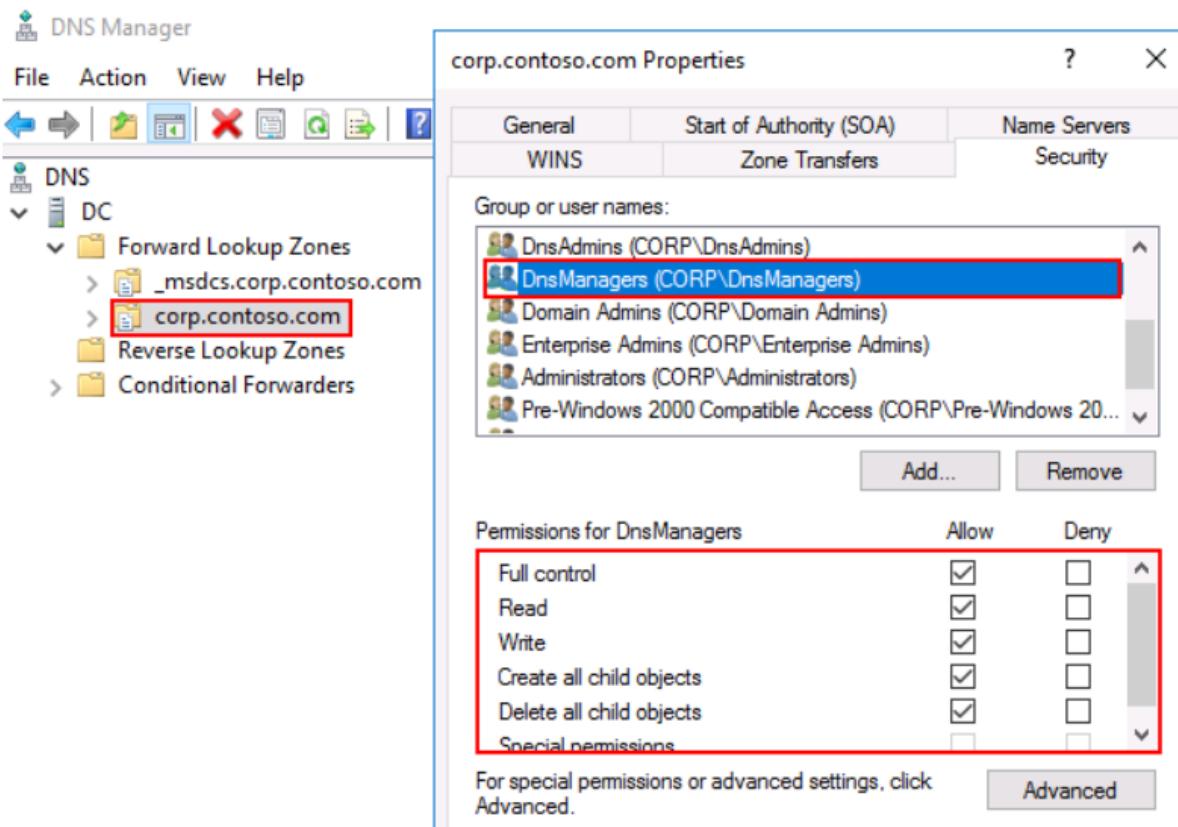
1.首先将该组添加到 DC 域名系统对象的 DACL 中，然后

确保它具有“读取所有属性”权限。就这样。



2. 展开正向查找区域容器

在前向查找区域中给域名管理器“通用代码”



将读取 DNS 事件日志的权限委托给 DNS 管理器

默认情况下，只有域管理员或同等人员可以读取 DNS 服务器日志。

3.以域管理员身份登录，并以提升的权限运行 CMD

3.1 .在 CMD 中键入以下命令:命令行 “域名系统服务器” > C:\

临时\ DNS _服务器. txt

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

3.2 .打开临时文件夹，然后单击域名服务器



3.3 .复制文本文件的以下部分:通道访问:; 0x1; ; SID)



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。复制以下内容(一；；0x1；；样本号)，并用的实际样本号替换“样本号”

DnsManagers 组。

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

这意味着你应该得到这样的东西:

(一)；；0x1；；s-1-5-21-3566662483-2648771335-1709913503-20601)

3.6 .现在复制(一；；0x1；；s-1-5-21-3566662483-2648771335-1709913503-20601)并将其粘贴到文本文件中通道访问的末尾。

File Edit Format View Help

(A; ; 0x2; ; ; NS)(A; ; 0x2; ; ; S-1-5-33)(A; ; 0x1; ; ; S-1-5-21-3566662483-2648771335-1709913503-20601)|

3.7 .现在，把 SYD:奥:包:的整篇课文抄下来，直到课文结束。

SYD:(甲；；0xf0007；；西)(一；；0x7；；文学士)(甲；；0x5；；(一)；；0x1；；国际单位)(一；；0x1；；苏)(一；；0x1；；s-1-5-3)(A；；0x2；；一次总付(甲)；；0x2；；NS)(A；；0x2；；s-1-5-33)(A；；0x1；；s-1-5-21-3566662483-2648771335-1709913503-20601)

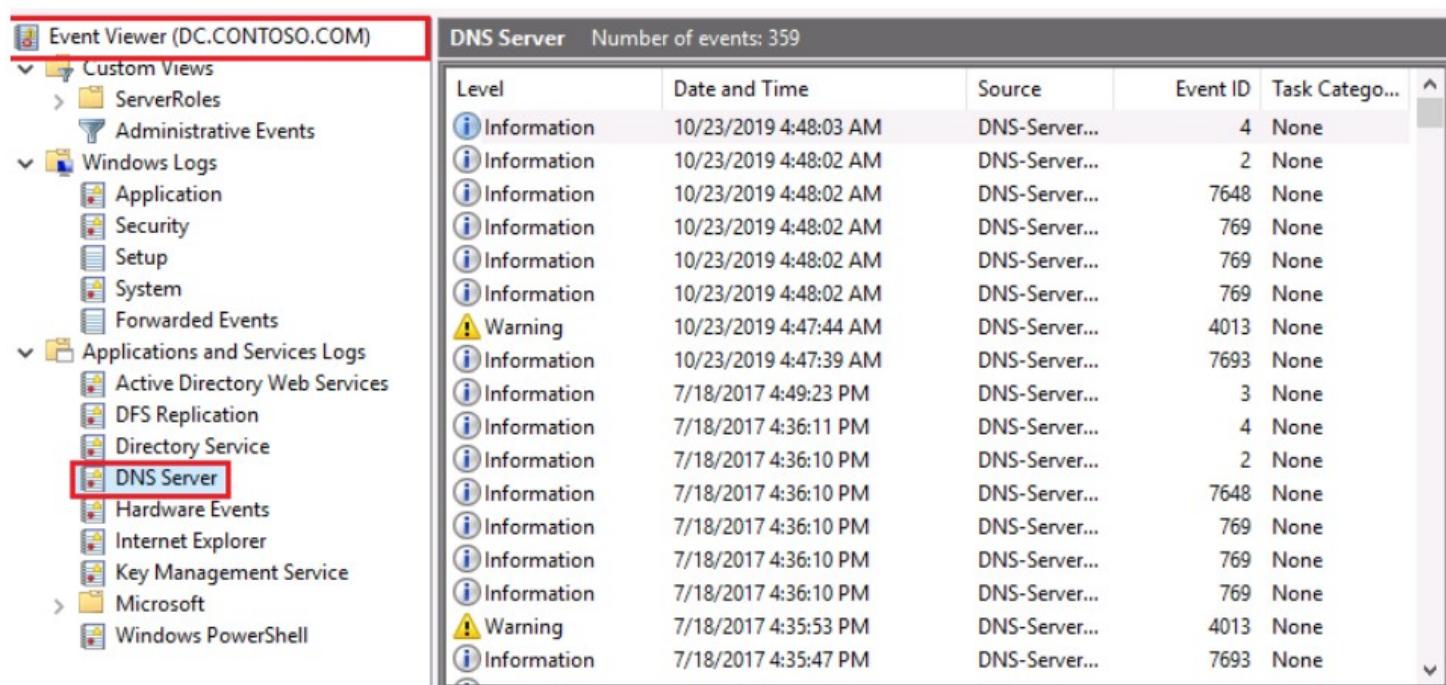
3.8 .以提升的权限打开 CMD，并键入以下命令:

“域名系统服务器” /ca: O:BAG:SYD:(一；；0xf0007；；西)(一；；0x7；；文学士)

(一); ; 0x5; ; (一); ; 0x1; ; 国际单位)(一; ; 0x1; ; 苏)(一; ; 0x1; ; s-1-5-3)(A; ; 0x2; ; 一次总付(甲); ; 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: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)
C:\windows\system32>
```

3.9 .DNS 管理器现在可以读取“DNS 服务器”的事件日志



The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various log sources under 'Custom Views' and 'Windows Logs'. Under 'Windows Logs', 'Application', 'Security', 'Setup', 'System', and 'Forwarded Events' are listed. Under 'Applications and Services Logs', 'Active Directory Web Services', 'DFS Replication', 'Directory Service', and 'DNS Server' are listed. The 'DNS Server' node is highlighted with a red box. On the right, a table titled 'DNS Server Number of events: 359' displays event details. The columns are 'Level', 'Date and Time', 'Source', 'Event ID', and 'Task Category...'. The table contains 359 rows of event data.

Level	Date and Time	Source	Event ID	Task Category...
Information	10/23/2019 4:48:03 AM	DNS-Server...	4	None
Information	10/23/2019 4:48:02 AM	DNS-Server...	2	None
Information	10/23/2019 4:48:02 AM	DNS-Server...	7648	None
Information	10/23/2019 4:48:02 AM	DNS-Server...	769	None
Information	10/23/2019 4:48:02 AM	DNS-Server...	769	None
Warning	10/23/2019 4:47:44 AM	DNS-Server...	4013	None
Information	10/23/2019 4:47:39 AM	DNS-Server...	7693	None
Information	7/18/2017 4:49:23 PM	DNS-Server...	3	None
Information	7/18/2017 4:36:11 PM	DNS-Server...	4	None
Information	7/18/2017 4:36:10 PM	DNS-Server...	2	None
Information	7/18/2017 4:36:10 PM	DNS-Server...	7648	None
Information	7/18/2017 4:36:10 PM	DNS-Server...	769	None
Information	7/18/2017 4:36:10 PM	DNS-Server...	769	None
Information	7/18/2017 4:36:10 PM	DNS-Server...	769	None
Warning	7/18/2017 4:35:53 PM	DNS-Server...	4013	None
Information	7/18/2017 4:35:47 PM	DNS-Server...	7693	None

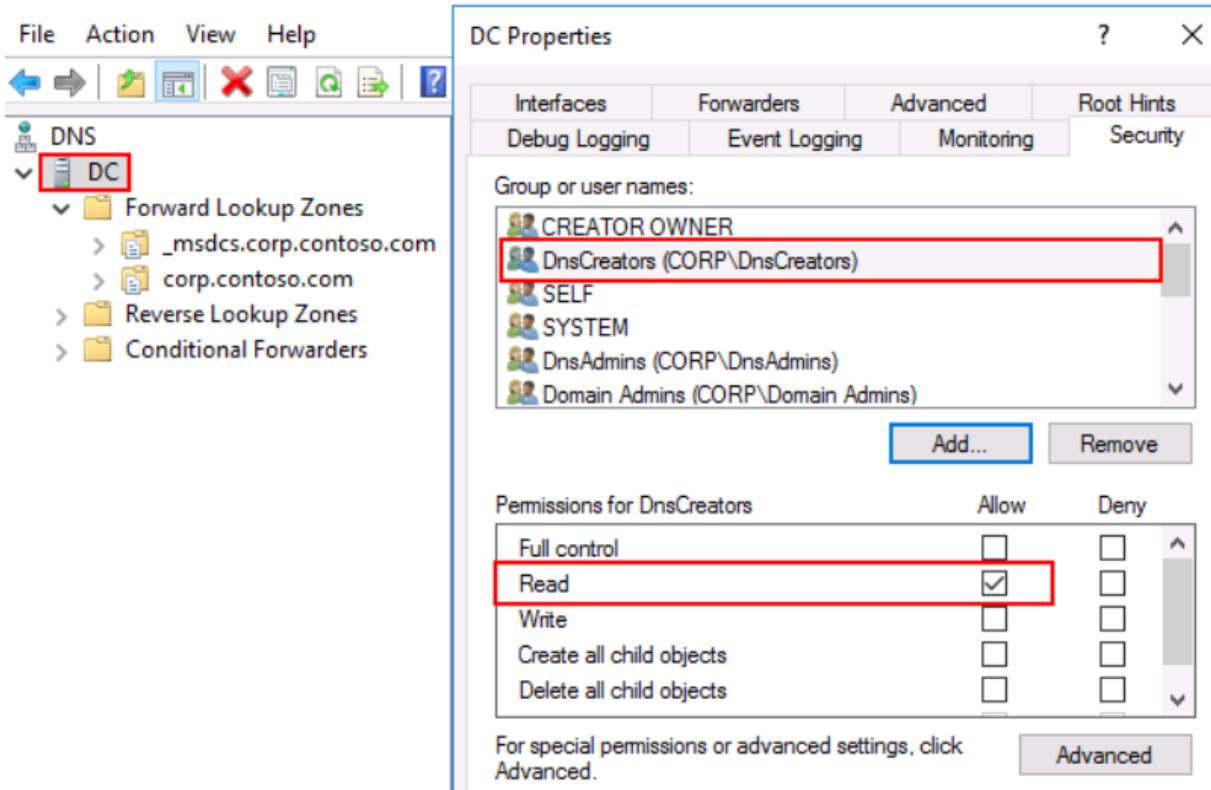
3.10。丹麦经理现在拥有我们在 RBAC 管理的所有权利

模型。

DnsCreators

将“域名创建者”组添加到域名系统对象的 DACL，并仅确保

分配了“读取所有属性”。就这样。

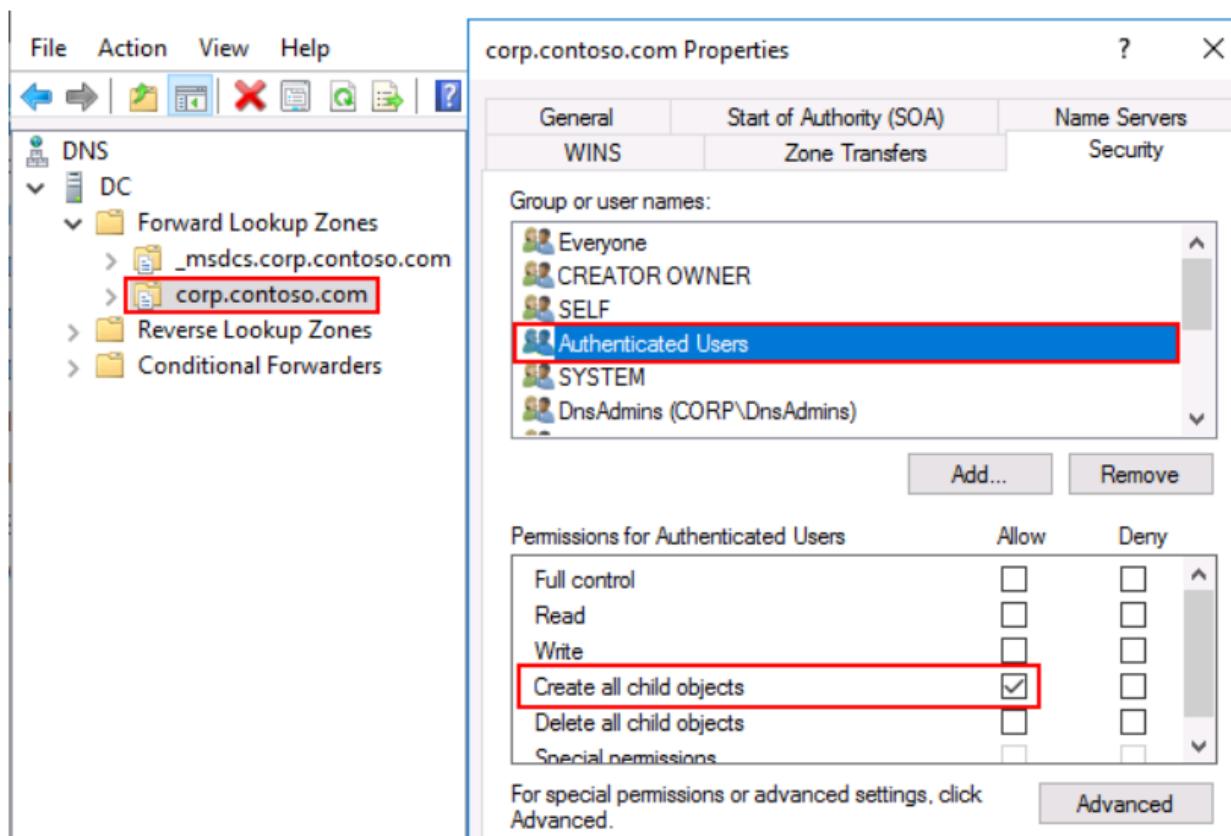


...)

默认情况下，“经过身份验证的用户”已经具有“创建所有子对象”

这意味着域名创建者可以创建域名系统

记录。如果它对 DNS 对象本身具有“读取”权限。



3.2 -确保对域名系统进行备份，并
安全储存

所有与域名系统记录等相关的信息存储在以下内容中

位置:C:\窗口\System32\dns

...)

...)

打开域名系统管理器

展开正向查找区域，容器。

The screenshot shows the Windows DNS Manager interface. The left pane displays the navigation tree with 'DNS' and 'DC' nodes, and under 'Forward Lookup Zones', it lists '_msdcs.contoso.com' and 'contoso.com'. The right pane shows a table of zones:

Name	Type	Status
_msdcs.contoso.com	Active Directory-Integrated Pr...	Running
contoso.com	Active Directory-Integrated Pr...	Running

...)

...)

以提升的权限打开 PowerShell 或 CMD

键入以下命令：

1.dnscmd/zone export _ 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>
```

2.contoso.com contoso.com.txt 区出口

```
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.打开计算机:\窗口\系统32\dns，您可以看到我们的备份

Name	Date modified	Type	Size
backup	9/17/2019 5:10 AM	File folder	
samples	10/31/2016 2:40 PM	File folder	
_msdcs.contoso.com.dns	10/31/2016 2:41 PM	DNS File	1 KB
_msdcs.contoso.com.txt	9/17/2019 5:26 AM	Text Document	2 KB
CACHE.DNS	10/31/2016 2:40 PM	DNS File	4 KB
contoso.com.dns	10/31/2016 2:41 PM	DNS File	1 KB
contoso.com.txt	9/17/2019 5:28 AM	Text Document	4 KB
dns.log	9/17/2019 5:10 AM	Text Document	0 KB

• Recommendation

...)

...)

...)

...)

...)

将域名系统备份本地存储在未加入广告的服务器上。

如果您尚未备份域名系统，请启动备份程序。

比如说。我们什么时候做备份？每个月，

一周，几天？

开始为灾难做准备。当有人不小心

删除了您的整个正向查找区域？你将如何恢复它

尽快减少停机时间？你知道如何恢复它吗？

这些问题你可能会问你的团队。

尽量避免或限制 DnsAdmins，因为它几乎不需要。

部署管理域名系统的 RBAC 模型降低了分配的风险

用户拥有 DnsAdmins 权限。

4.1 -具有公钥基础设施的 RBAC

要求	实施 RBAC 管理和批准授权
描述	应该部署一个 RBAC 模型来委派 CA 中的管理任务，以确保没有一个个人能够危害整个计算机辅助服务器。
补充	有两项重要的任务特别侧重于证书颁发机构 管理认证中心 颁发和管理证书

	默认情况下，域管理员或同等人员能够管理这两项任务，但不应使用该组来管理加州。 应创建两个新组，并授予其中一个组根据上述许可。他们都不应该能够完成两项任务。
编号	AD-CS-001
版本	1.1
例外	<在此插入您的例外>

任务

认证机构管理员	CA 经理
配置和维护认证中心。	批准证书注册和撤销请求。

谁能做什么？

认证机构管理员

创建证书模板
将用户和计算机注册到创建的证书模板中
启动和停止活动目录证书服务
配置扩展
配置角色
定义关键恢复代理
限制证书管理员
删除证书颁发机构中的一行
批量删除 CA 行
启用、发布或配置证书吊销列表计划

阅读认证中心数据库

阅读认证中心配置

配置策略和现有模块

认证经理

颁发和批准证书

拒绝证书

吊销证书

重新激活被搁置的证书

续订证书模板

恢复存档的密钥

阅读认证中心数据库

阅读认证中心配置

从在广告中创建两个新组开始

--)

--)

认证机构管理员

认证经理

Name	Type	Description
 CA Administrators	Security Group...	Configure and maintain the CA
 CA Managers	Security Group...	Approve certificate enrollment and revocation requests

打开 ADSI 编辑→配置→核心网=服务→核心网=公钥服务

下列标有红色的容器是

我们需要使用来委派管理任务。

...)

...)

CN =证书模板

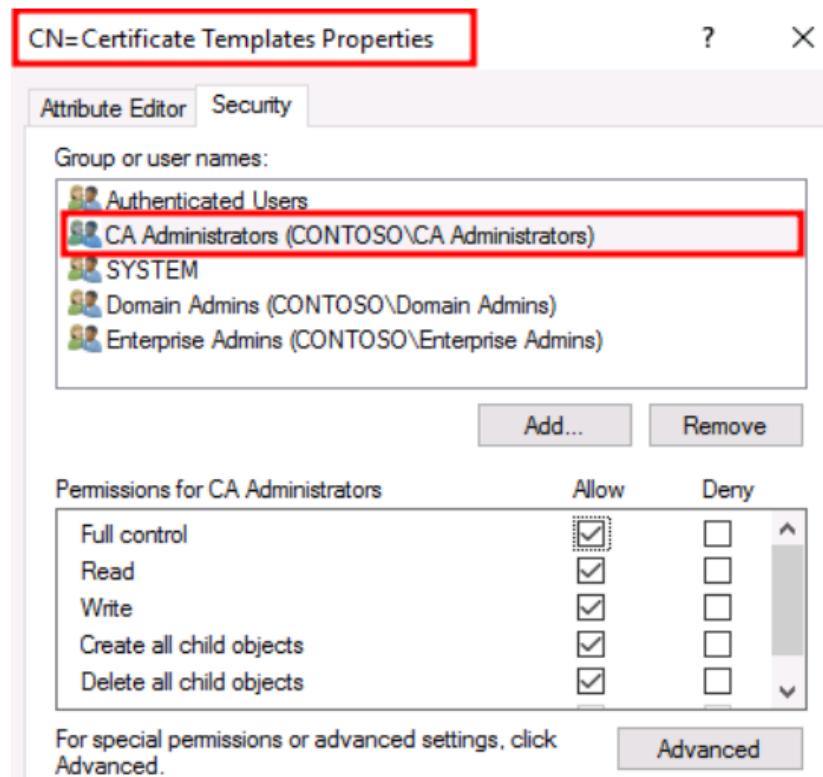
中国=OID

Name	Class	Distinguished Name
CN=AIA	container	CN=AIA,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=CDP	container	CN=CDP,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=Certificate Templates	container	CN=Certificate Templates,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=Certification Authorities	container	CN=Certification Authorities,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=Enrollment Services	container	CN=Enrollment Services,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=KRA	container	CN=KRA,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=OID	msPKI-Enterprise	CN=OID,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM
CN=NTAuthCertificates	certification	CN=NTAuthCertificates,CN=Public Key Services,CN=PKI,CN=Services,DC=CONTOSO,DC=COM

...)

右键单击证书模板→安全→添加→认证

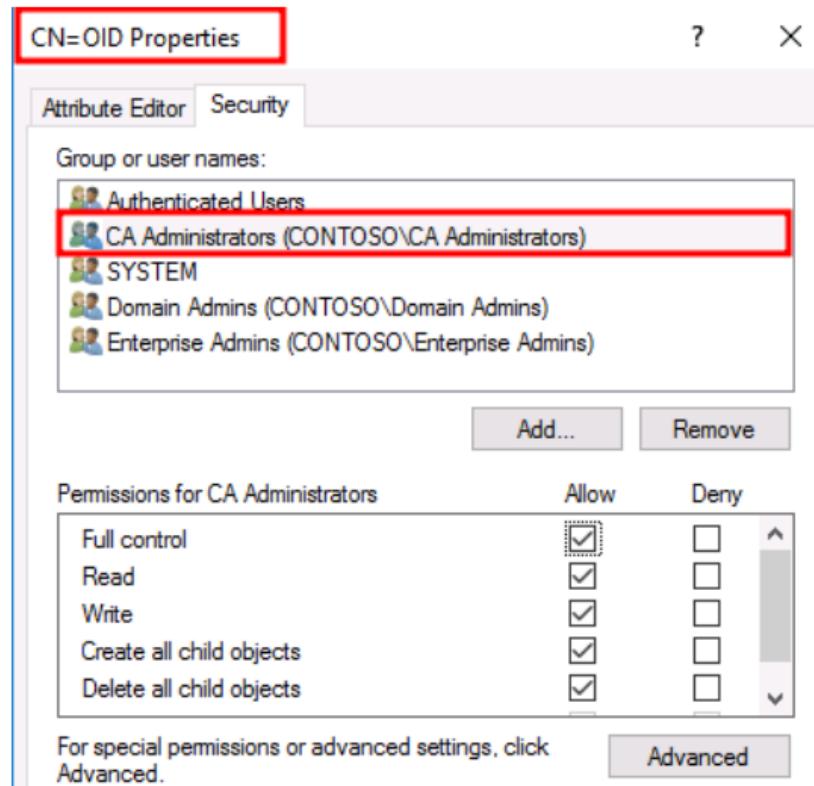
管理员→完全控制



...)

右键单击加拿大=OID → 安全→添加→认证管理员→满

控制

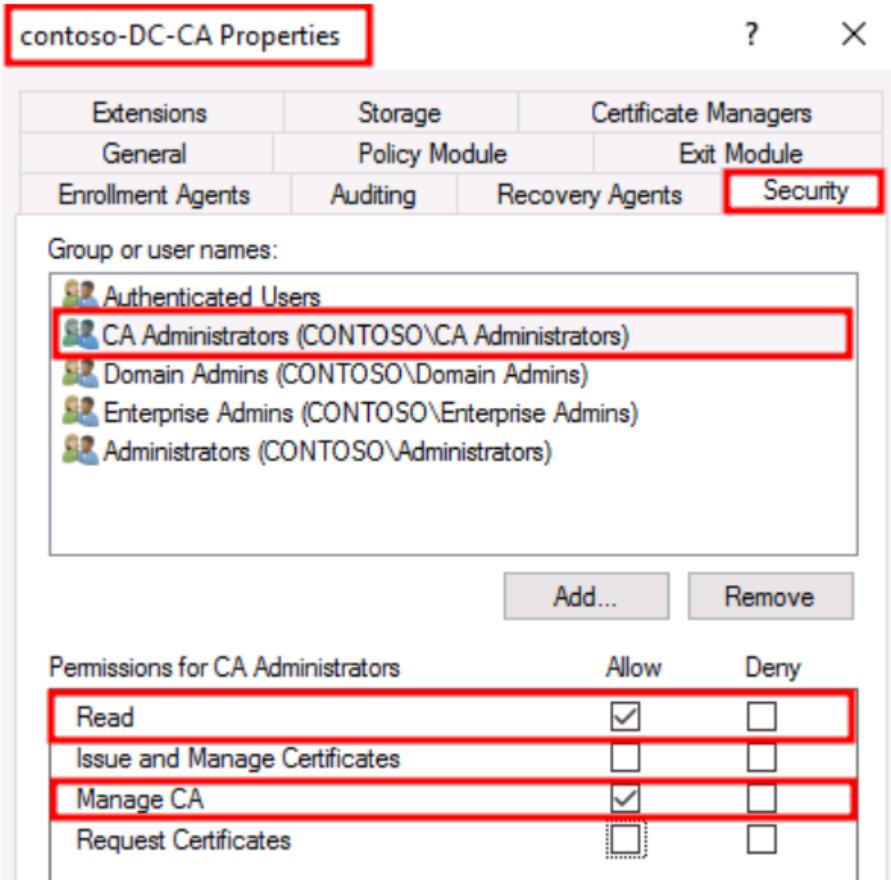


...)

打开证书颁发机构→右键单击证书颁发机构服务器对象→安全性→

添加→证书颁发机构管理员→读取→管理证书颁发机构→取消选中“”请求

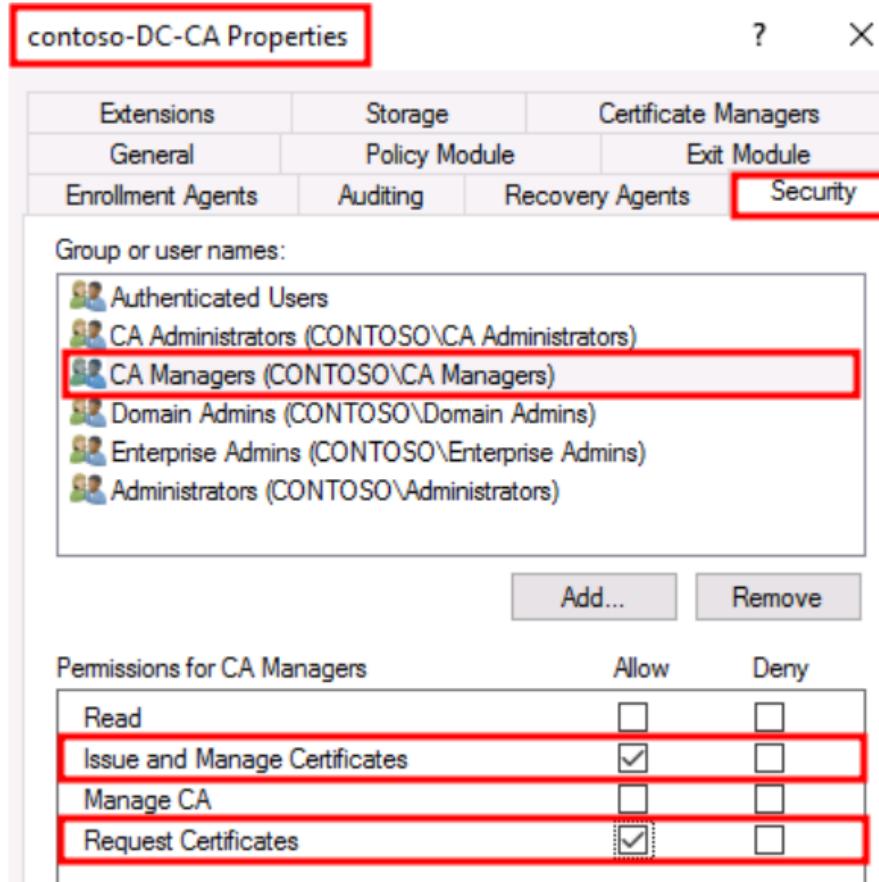
证书“”



CA 管理员的委派已经完成。

打开证书颁发机构→右键单击证书颁发机构服务器对象→安全性→添加→

认证中心经理→颁发和管理证书→申请证书



现在我们已经完成了认证中心经理的委派。

4.2 -确保在公钥基础设施服务器上启用审计

事件日志被转发到 SIEM

要求	打开证书颁发机构审计
描述	默认情况下，所有与 CA 相关的事件都不是记录在案。需要启用这些审核规则，并且由安全团队管理，类似于 SOC/SIEM 例如。
补充	因为公钥基础设施是一项重要资产。应严格监控环境。 日志记录是确保证书颁发机构的安全性。
编号	AD-CS-003
例外	公钥基础设施通常是一项关键资产，但这并不意味着它是为了全世界所有的公司。

任务

SOC/SIEM

配置审计规则

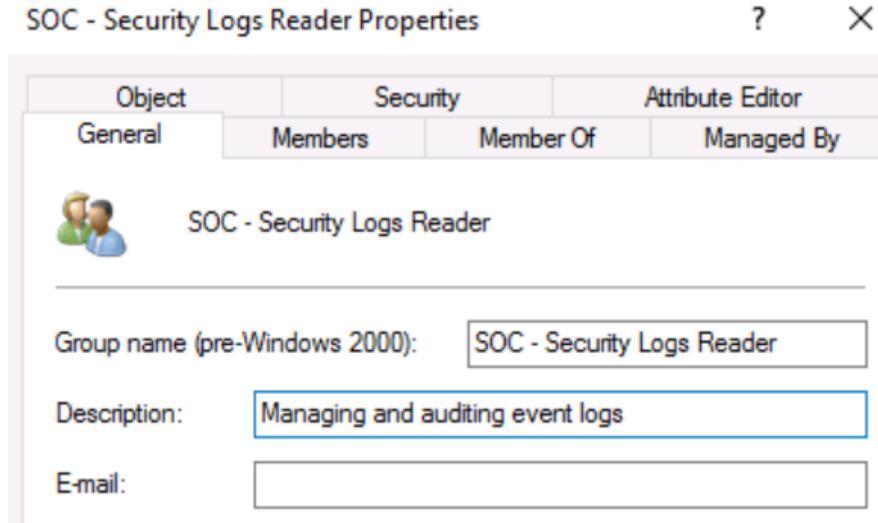
在事件查看器中管理审计日志

在事件查看器中导入和导出事件日志

清除事件日志

首先，应该创建一个负责管理认证中心的新组

审核日志。



组创建后。添加将负责的所有人

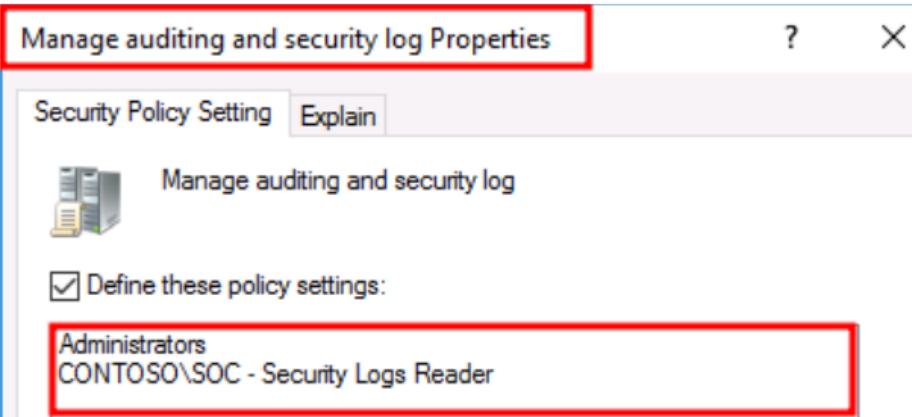
关注加州。通常是足球。

登录证书颁发机构服务器并打开本地安全策略→策略→窗口

设置→安全设置→本地策略→用户权限分配→

管理审计和安全日志

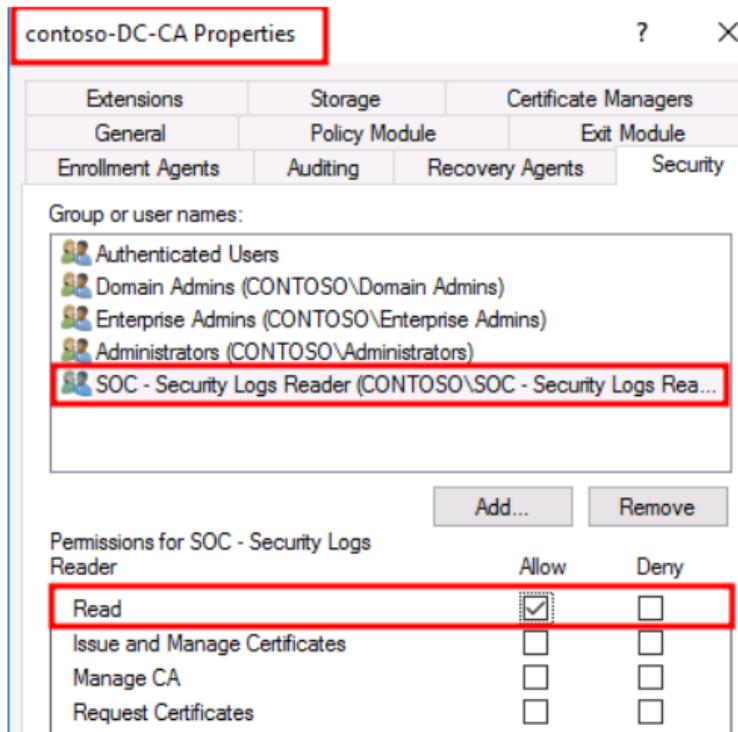
添加 SOC - 安全日志阅读器



...)

现在授予“系统芯片安全日志读取器”对证书颁发机构的“读取”权限

服务器。



...)

现在，系统芯片安全日志阅读器中的每个人都可以打开

审核规则并收集与广告客户服务相关的事件日志。

Extensions		Storage	Certificate Managers			
General		Policy Module	Exit Module			
Enrollment Agents	Auditing	Recovery Agents	Security			
To start logging events to the security log, you must enable the 'Audit object access' setting in Group Policy.						
Events to audit:						
<input checked="" type="checkbox"/> Back up and restore the CA database <input checked="" type="checkbox"/> Change CA configuration <input checked="" type="checkbox"/> Change CA security settings <input type="checkbox"/> Issue and manage certificate requests <input checked="" type="checkbox"/> Revoke certificates and publish CRLs <input checked="" type="checkbox"/> Store and retrieve archived keys <input checked="" type="checkbox"/> Start and stop Active Directory Certificate Services						

为了获得更好的可见性，建议打开“”认证

服务“”子类别也是如此。

...)

审核/设置/子类别：“认证服务” /成功:启用

/failure:启用

```
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> _
```

审计/获取/类别:*

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

所有与广告客户服务相关的活动标识都可以在这里找到:

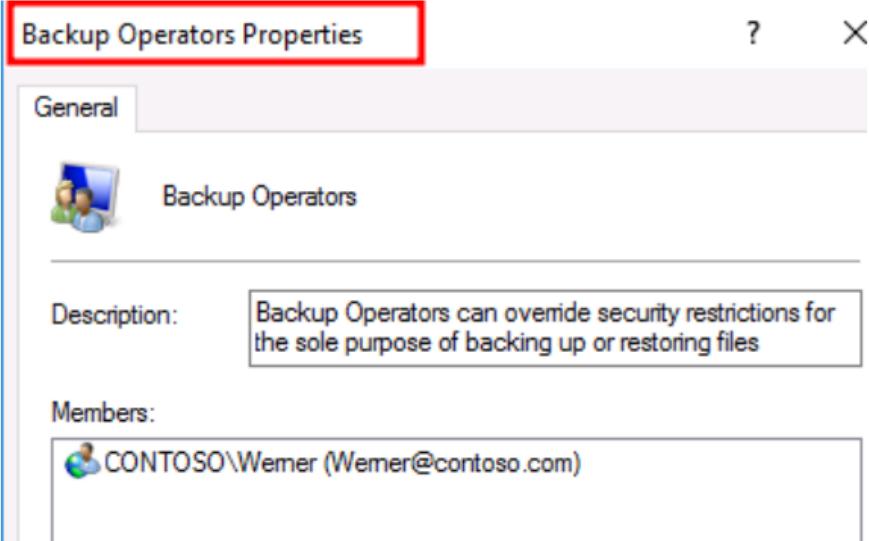
[http://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786423\(v=ws.11\)](http://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786423(v=ws.11))

4.3 -确保制作和存储公钥基础设施的备份
安全地

登录认证服务器→打开计算机管理→本地用户和

组→组→备份操作员→添加适当的成员

负责备份。



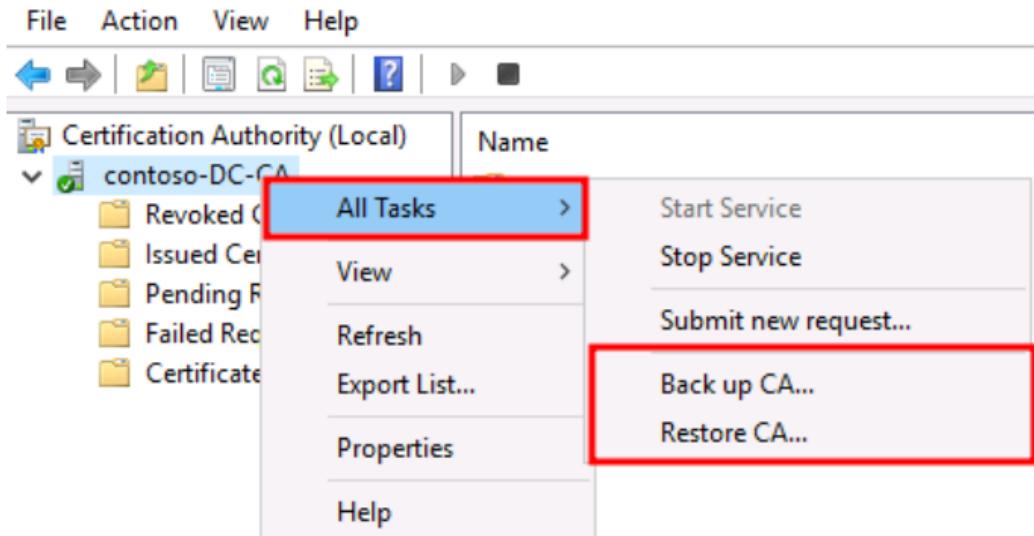
...)

...)

备份操作员有权在本地登录 CA 服务器，但它

无法通过 RDP 登录。

所有任务→备份 CA...



执行计算机辅助分析备份时。确保涵盖以下内容。

认证证书和私钥

CA 数据库备份

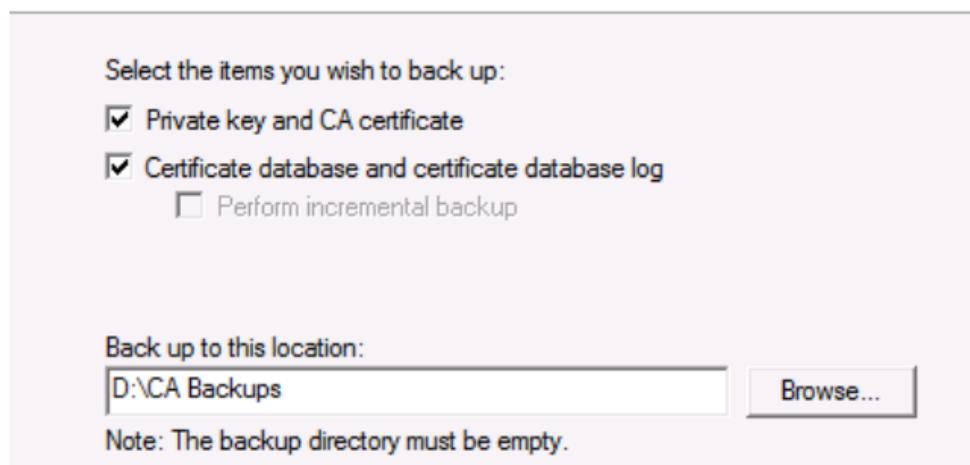
认证机构注册信息

提示:考虑将证书颁发机构备份到另一个与接口的安全位置

备份系统，而不是让备份系统直接连接到 CA。

Items to Back Up

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



确保您选择了两个选项

Completing the Certification Authority Backup Wizard

You have selected the following settings:

Private Key and CA Certificate
Issued Log and Pending Requests

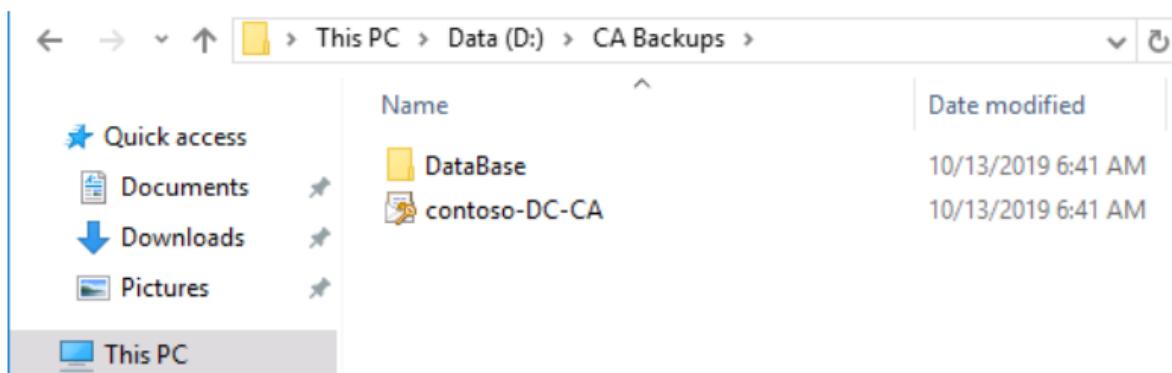
< | >

To close this wizard and begin backup, click Finish.

--)

在这里我们可以看到备份已经完成。确保

私钥有一个强密码。



...)

...)

请确保您在公钥基础设施服务器上也覆盖了证书颁发机构注册表项。这

可以在这里找到:HKLM\系统\当前控制集\服务\

CertSVC\配置\CAname

导出确切的注册表路径

Name	Type	Data
(Default)	REG_SZ	(value not set)
CACertHash	REG_MULTI_SZ	db 29 08 bc ce cf 72 fe 89 40 ad 97 t
CACertPublicati...	REG_MULTI_SZ	1:C:\Windows\system32\CertSrv\CD...
CA Server Name	REG_SZ	DC.contoso.com
CAType	REG_DWORD	0x00000000 (0)
CAXchgCertHash	REG_MULTI_SZ	
CAXchgOverlap...	REG_SZ	Days
CAXchgOverlap...	REG_DWORD	0x00000001 (1)
CAXchgValidity...	REG_SZ	Weeks
CAXchgValidity...	REG_DWORD	0x00000001 (1)
CertEnrollComp...	REG_DWORD	0x00000000 (0)
ClockSkewMinu...	REG_DWORD	0x0000000a (10)
CommonName	REG_SZ	contoso-DC-CA
CRLDeltaOverla...	REG_SZ	Minutes
CRLDeltaOverla...	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	Days
CRLDeltaPeriod...	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	90 f9 df ad f4 26 e4 01
CRLOverlapPeri...	REG_SZ	Hours

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\contoso-DC-CA

• Recommendations

...)

...)

...)

...)

...)

...)

不要忘记备份认证服务器。

在证书颁发机构服务器上启用审计

将公钥基础设施安全事件转发到 SIEM

也备份证书颁发机构的注册表项

在未加入广告的服务器上本地存储备份。

在自动数据交换系统上部署 RBAC 模型有助于您管理公钥基础设施，而无需

在域管理员或同等人员中有不必要的用户。

5.1 -确保默认域控制器策略

被更安全的集中 GPO 取代

默认情况下，存在已知的“默认域控制器策略”，即

链接到域控制器。

默认情况下部署在“”默认域控制器中的设置

策略“”不安全，不。我不会解释“为什么”

The screenshot shows the 'Group Policy Management' interface. On the left, under 'Forest: corp.contoso.com > Domains > corp.contoso.com > Domain Controllers', the 'Default Domain Controllers Policy' is highlighted with a red box. The right pane is titled 'Default Domain Controllers Policy' and shows the 'Links' tab. It displays a table with one row: 'Domain Controllers' (Location), 'No' (Enforced), 'Yes' (Link Enabled), and 'corp.contoso.com/Domain Controllers' (Path). A dropdown menu above the table shows 'corp.contoso.com'.

...)

创建一个新的 GPO，并用更“安全”的思想来代替它

设置。

The screenshot shows the 'New GPO' dialog box. In the 'Name:' field, 'Security GPO' is typed. The 'Source Starter GPO:' dropdown is set to '(none)'. At the bottom are 'OK' and 'Cancel' buttons. To the left of the dialog, there is a list of existing GPOs: Default Domain Controllers Policy, Default Domain Policy, Internet Explorer Zone Settings, Remote Desktop Access, Windows PowerShell Execution Policy, WMI Filters, and Starter GPOs.

...)

使用以下设置编辑创建的 GPO，这些设置可以在

用户权限分配

用户权利分配

从访问这台计算机 网络	管理员、经过身份验证的用户， 企业域控制器
将工作站添加到域	管理员
允许本地登录	管理员、备份操作员
允许通过远程登录 桌面服务	管理员

备份文件和目录	管理员、备份操作员
恢复文件和目录	管理员、备份操作员
更改系统时间	管理员
调试程序	管理员
拒绝访问这台计算机 从网络上	客人们, DC
拒绝通过远程登录 桌面服务	客人们, DC
关闭系统	管理员
作为服务登录	需要作为 服务
作为批处理作业登录	计划任务的服务帐户

安全选项

允许格式化和弹出 可移动媒体	管理员
设备:防止用户 安装打印机驱动程序	使能够
域控制器:允许服务器 操作员安排任务	有缺陷的
网络访问:不允许 SAM 的匿名枚举 帐目	使能够
网络访问:不允许 SAM 的匿名枚举 账户和股份	使能够
网络安全:局域网管理器 认证级别	仅发送 NTLMv2 响应(测试此 首先)

• Recommendation

...)

...)

将新的安全 GPO 链接到域控制器

取消“默认域控制器策略”与域的链接

控制器。

The screenshot shows the Group Policy Management console. On the left, under 'Forest: corp.contoso.com / Domains / corp.contoso.com', the 'Default Domain Controllers Policy' is selected. On the right, the 'Default Domain Controllers Policy' details page is displayed. In the 'Links' section, it shows 'Domain Controllers' is linked with 'Link Enabled' set to 'No'. A red box highlights the 'Link Enabled' column.

Location	Enforced	Link Enabled	Path
Domain Controllers	No	No	corp.contoso.com/Domain Controllers

5.2 - DSRM 作为碎玻璃账户

目录服务还原模式(DSRM)是的安全模式引导选项

Windows 服务器域控制器。DSRM 允许管理员修复或

恢复以修复或恢复活动目录数据库。

这就像灾难恢复活动目录的击碎玻璃账户。

资料来源:<http://search.windowsserver.techtarget.com/definition/Directory-service-recovery-mode-DSRM>

服务-恢复-模式-DSRM

...)

...)

你知道谁有这个帐户的密码吗？

密码最后一次被重置是什么时候？

用 ntdsutil 重设 DSRM 的密码

1. 具有提升权限的开放式 CMD(需要授权或同等权限)

2.类型:ntdsutil

3.类型:设置 DSRM 密码

```
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.类型:重置 DC 服务器上的密码

我们的域控制器名叫做“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.现在为 DSRM 账户选择一个密码

```
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.

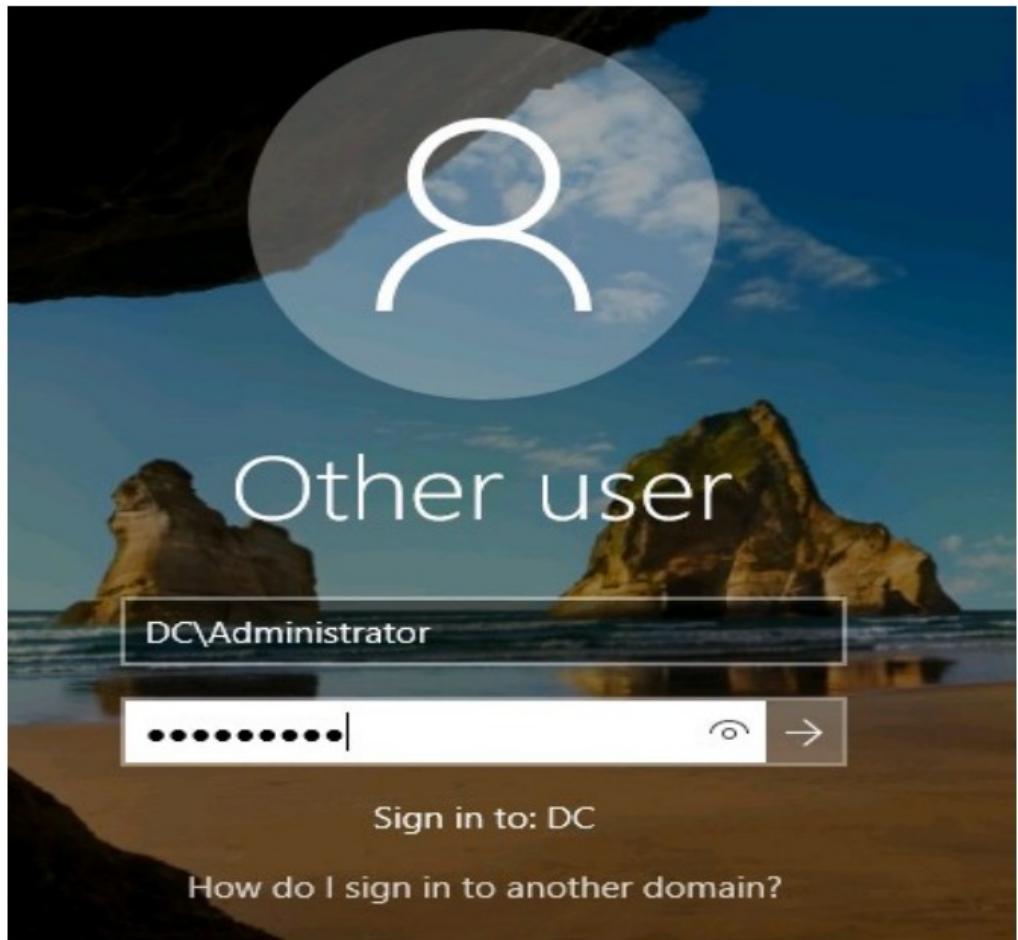
Reset DSRM Administrator Password: q
ntdsutil:
```

6.类型:退出

7.类型:退出

8.类型:退出

9.现在，当您想使用 DSRM 帐户登录时:



- Recommendations

DSRM 就像域控制器的碎玻璃账户

确保密码不会在所有广告管理员之间共享。

...)

...)

如果您从未更改过此帐户的密码。这是正确的

是时候这么做了。

你知道谁有 DSRM 账户的密码吗？

5.3 - 确保 Windows 服务器备份或同等产品
安装在 DC 以备份域
控制器

备份在活动目录中是一项非常重要的任务

对马士基的 ransomware 攻击是一个很好的例子，说明了为什么你应该

备份并很好地保护它们。

就像马士基的 CISO 一样。' '离线备份至关重要，即使在

非常大的网络”



Jake Williams

@MalwareJake

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

The damage

IT Services

- DHCP and Active Directory badly damaged
 - DHCP gives your computer an address
 - A.D. is the phone book
- Enterprise Service Bus destroyed
- vCenter (the thing that controls the cloud) damaged and unstable

End User Devices

- 49,000 laptops destroyed
- All print capability destroyed
- File shares unavailable

Applications and Servers

All our 1200 applications were inaccessible and approximately 1000 were destroyed. Data was preserved through backup but the applications themselves couldn't be restored from backup as they would immediately have been reinfected.

The impact on servers was that 3,500 out of 6,200 servers were destroyed. Again they couldn't be restored from backup due to reinfestation.

...)

可以从“添加角色和”安装窗口服务器备份

服务器管理器中的功能“”。默认情况下不安装。

wbadm - [Windows Server Backup (Local)\Local Backup]

File Action View Help



Windows Server Backup (L)
Local Backup

Local Backup



You can perform a single backup or schedule a regular backup using this application.



Windows Server Backup is not installed on this computer. To install Windows Server Backup, from Server Manager, open the Add Roles and Features wizard to select the Windows Server Backup feature.

确保域控制器中安装了 Windows 服务器备份。

Before You Begin

Installation Type

Server Selection

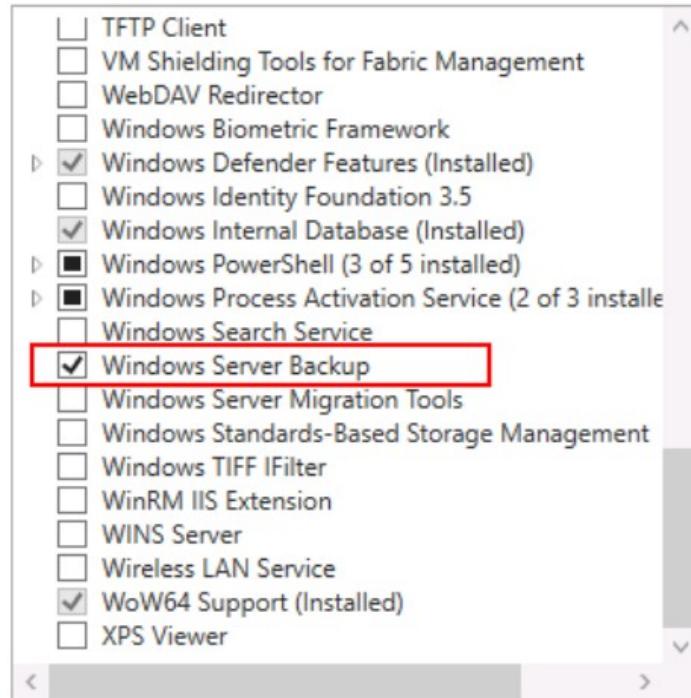
Server Roles

Features

Windows Server Essential...

Confirmation

Results



因为备份在活动目录中至关重要。我会花时间散步

你经历了不同的步骤。

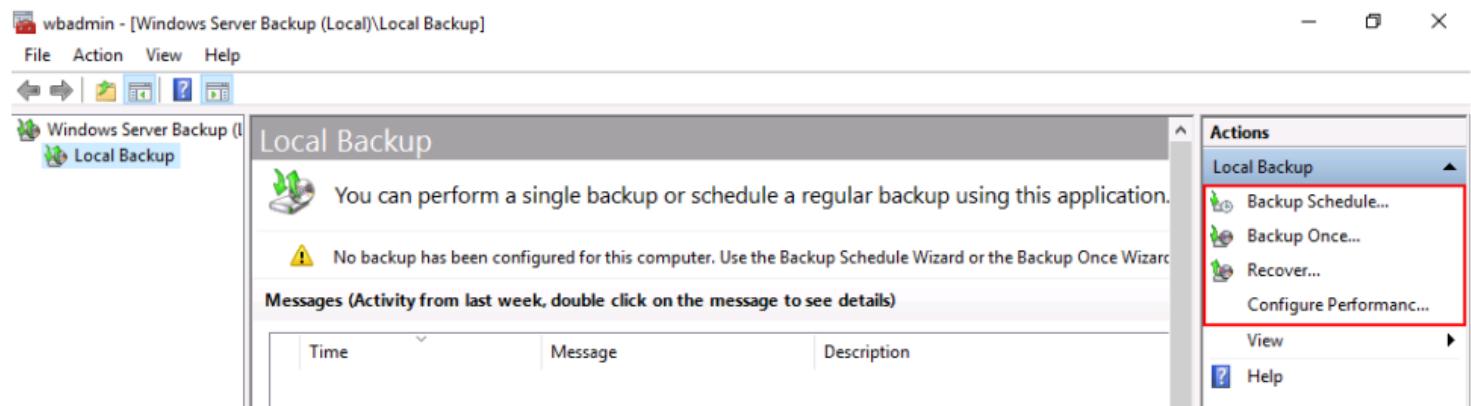
创建备份有两个选项，如下所示：

...)

...)

备份计划→自动备份的任务计划程序

备份一次→手动备份广告/DC



在本例中，我将选择“备份时间表”。

...)

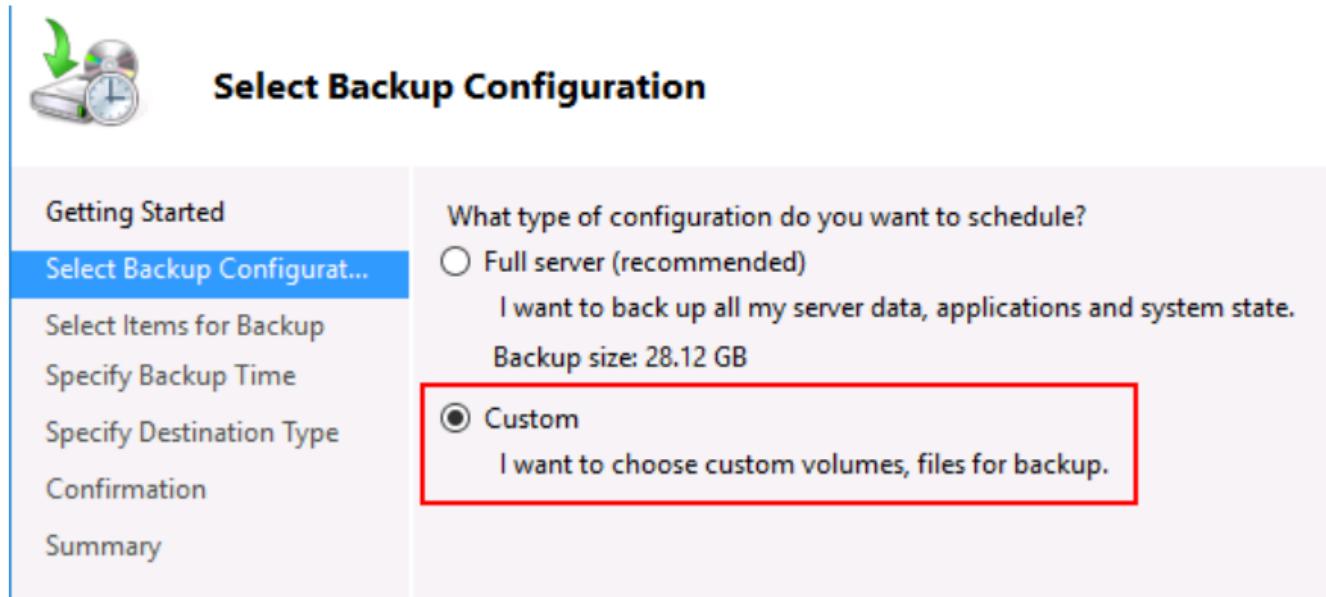
...)

...)

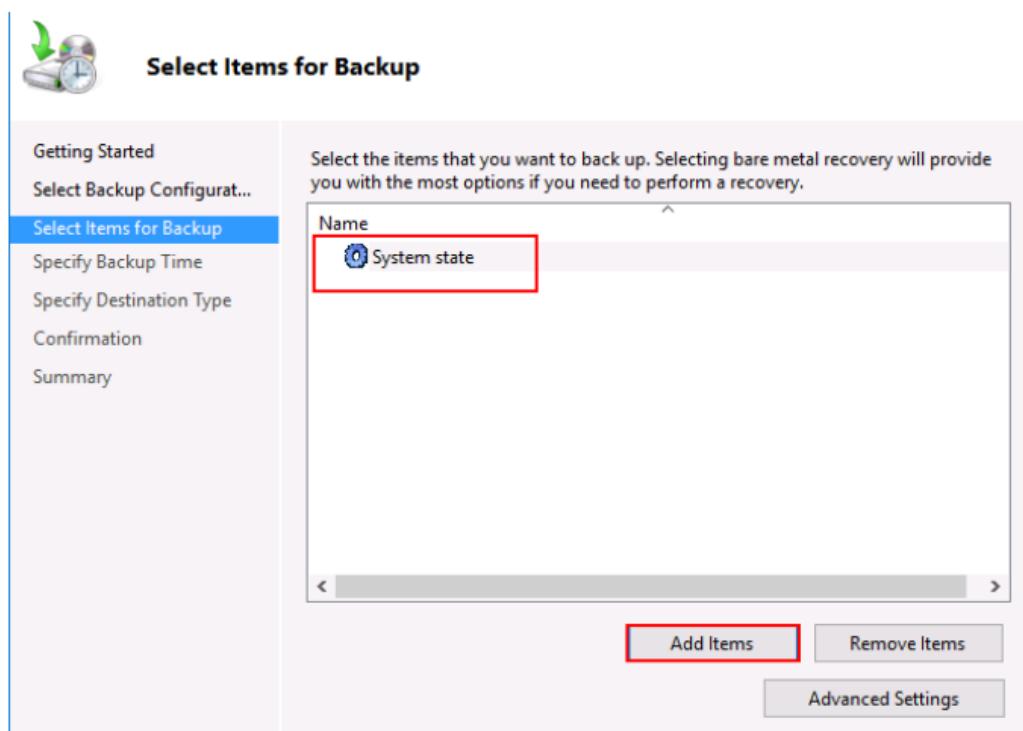
单击备份时间表

单击下一步

单击自定义



单击添加项目并选择系统状态



...)

...)

单击“高级设置”和“VSS 设置”

如果您没有任何备份软件或

相当于备份广告/DC

Advanced Settings >

File exclusions count: 0

VSS settings: VSS Full Backup

[Exclusions](#) [VSS Settings](#)

Choose what type of Volume Shadow Copy Service (VSS) backup you want to create.

VSS full Backup

Choose this option if you are not using any other product to back up applications. This option updates the backup history of each file and clears the application log files.

VSS copy Backup

Choose this option if you are using another product to back up applications that are on the volumes included in the backup. This option retains the application log files.

...)

...)

单击下一步

现在选择您喜欢的备份时间。

Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Confirmation
Summary

How often and when do you want to run backups?

Once a day
Select time of day: 9:00 PM

More than once a day
Click an available time and then click Add to add it to the backup schedule.

Available time:
Scheduled time:
Add >
< Remove

...)

...)

单击下一步

在目的地类型。选择你喜欢的一个。

Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Volume
Confirmation
Summary

Where do you want to store the backups?

Back up to a hard disk that is dedicated for backups (recommended)
Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

Back up to a volume
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

Back up to a shared network folder
Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.

现在，单击下一步，您会看到如下内容

Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary

Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.

Available disks:

Disk	Name	Size	Used Space	Volumes in D...
<input checked="" type="checkbox"/> 1	Virtual HD ATA Device	127.00 GB	490.79 MB	D:\

Show All Available Disks...

...)

...)

单击下一步

单击完成

Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary

You are about to create the following backup schedule.

Backup times: 9:00 PM
Files excluded: None
Advanced option: VSS Full Backup

Backup destinations

Name	Label	Size	Used Space
Virtual HD AT...	DC 2019_12_29 ...	127.00 GB	239.71 MB

Backup items

Name
System state

< Previous Next > **Finish** Cancel

备份计划已经完成！

Getting Started
Select Backup Configuration...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary

Status: You have successfully created the backup schedule.
Your first scheduled backup will happen at 12/29/2019 9:00 PM.
Make sure that the disks you are using to store scheduled backups are attached to this computer and are available.

...)

...)

现在将创建一个名为“”的计划任务

WindowsBackup 备份“”

位置:\微软\窗口\备份

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

PS C:\windows\system32> Get-ScheduledTask -TaskName Microsoft-Windows-WindowsBackup
TaskPath          TaskName          State
-----          -----          -----
\Microsoft\Windows\Backup\          Microsoft-Windows-WindowsBackup      Ready

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

Computer Management (Local)

- System Tools
- Task Scheduler
 - Task Scheduler Library
 - Microsoft
 - Windows
 - .NET Framework
 - Active Directory Rig
 - AppID
 - Application Experience
 - ApplicationData
 - AppxDeploymentClient
 - Autochk
 - Backup**
 - Bluetooth
 - CertificateServicesClient
 - Chkdsk
 - Clip
 - CloudExperienceHost

Name	Status	Triggers	Next Run Time	Last Run Time	...
Microsoft-W...	Ready	At 9:00 PM every day	12/29/2019 9:00:00 PM	11/30/1999 12:00:00 AM	T

General Triggers Actions Conditions Settings History

Name: Microsoft-Windows-Backup

Location: \Microsoft\Windows\Backup

Author: CORP\DCS

备份计划完成后。它将显示“成功”

Local Backup



You can perform a single backup or schedule a regular backup using this application

Messages (Activity from last week, double click on the message to see details)

Time	Message	Description
12/29/2019 12:55 AM	Backup	Successful

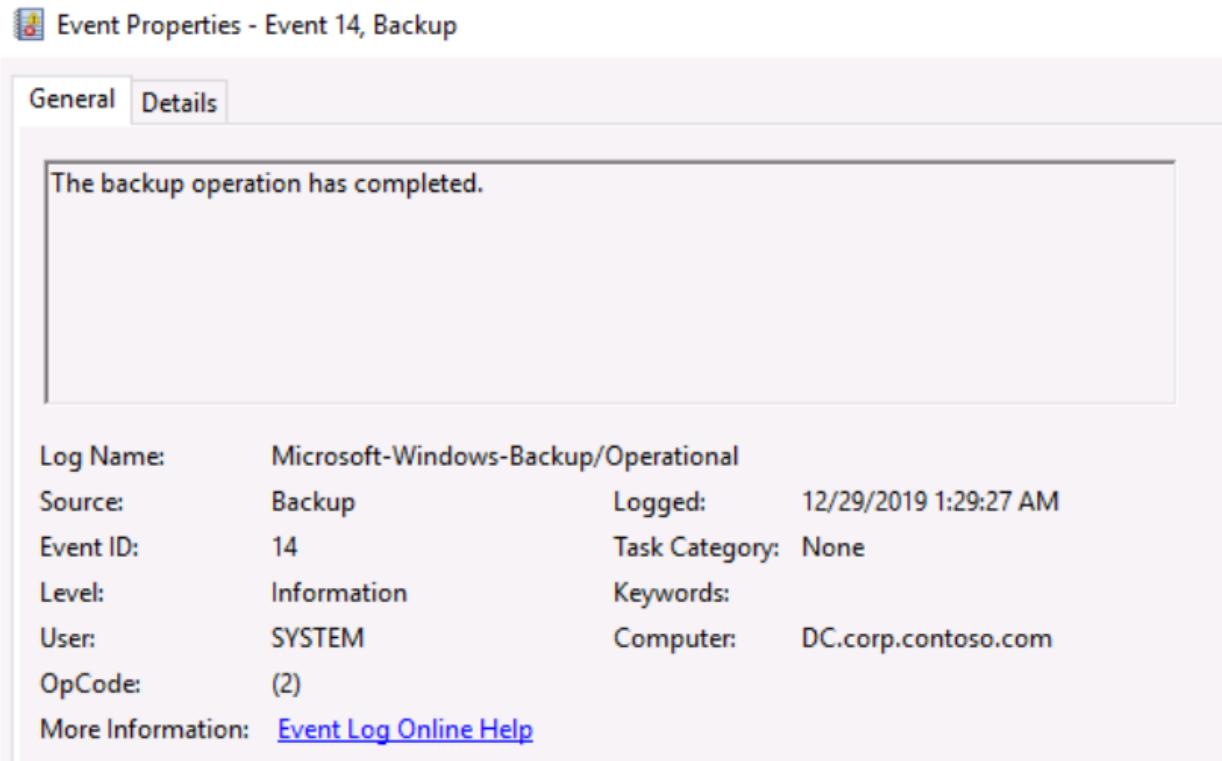
Status

Last Backup	Next Backup	A T L C G
Status: ✓ Successful Time: 12/29/2019 12:55 AM View details	Status: Scheduled Time: 12/29/2019 9:00 PM View details	

)

一切都被记录下来，当事件 14 出现时。你知道吗

备份已经完成。



- **Recommendation**

...)

...)

...)

...)

...)

广告/DC 的备份。

将备份本地存储在未通过广告加入的服务器上。

一个常见的错误是公司将备份存储在成员服务器上

在公元 100 年加入的。攻击者通常会意识到这一点，并且也会离开

备份服务器之后。

广告/DC 的备份通常来自 0 级运营。因为如果

有人想找回一些东西。需要登录访问

DC。这并不意味着需要域管理员，

因为备份操作员也足够了。

定期审核，查看备份是否也“成功”完成

6.1 - 在 GPO 处替换“认证用户”

链接到域控制器

每个经过身份验证的用户都有读取广告中 GPO 的权限。带有的工具

像猎犬这样的人能够发现错误的授权

例如，与 DC 有关的 GPO。

如果攻击者能够修改 DC 的 GPO。所有赌注都在域外

控制器，因为攻击者能够在 DC 或格兰特上运行代码

他自己“获得文件和对象的所有权”以进一步提升到域

管理员。

...)

在这里，我们可以看到用户 Werner 在

默认域控制器策略。

```
PS C:\Users\James> Get-GPPermission -Name "Default Domain Controllers Policy" -All

Trustee      : Authenticated Users
TrusteeType  : WellKnownGroup
Permission    : GpoApply
Inherited    : False

Trustee      : Domain Admins
TrusteeType  : Group
Permission   : GpoCustom
Inherited    : False

Trustee      : Enterprise Admins
TrusteeType  : Group
Permission   : GpoCustom
Inherited    : False

Trustee      : Werner
TrusteeType  : User
Permission   : GpoEdit
Inherited    : False

Trustee      : ENTERPRISE DOMAIN CONTROLLERS
TrusteeType  : WellKnownGroup
Permission   : GpoRead
Inherited    : False

Trustee      : SYSTEM
TrusteeType  : WellKnownGroup
Permission   : GpoEditDeleteModifySecurity
Inherited    : False
```

• Recommendation

减慢侦探犬等工具的速度。这是一个目标选择

GPO 的安全筛选中的“域控制器”组，它们是

适用于所有 DC 的。

The screenshot shows the Windows Group Policy Management console. On the left, under 'Group Policy Objects', the 'Default Domain Controllers Policy' is selected and highlighted with a red box. The right pane displays the 'Security Filtering' settings for this policy. A second red box highlights the 'Name' column in the table, which lists 'Domain Controllers (CORP\Domain Controllers)'.

Name
Domain Controllers (CORP\Domain Controllers)

Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:

结果

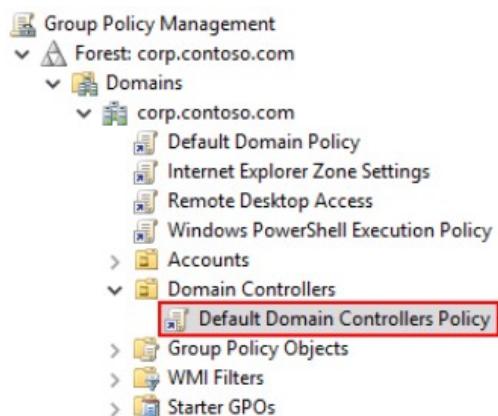
```
PS C:\Users\James> Import-Module ActiveDirectory
PS C:\Users\James> Get-GPPermission -Name "Default Domain Controllers Policy" -All
Get-GPPermission : The "Default Domain Controllers Policy" GPO was not found in the corp.contoso.com domain.
Parameter name: gpoDisplayName
At line:1 char:1
+ Get-GPPermission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

6.2 -链接到第 0 层资源的 GPO 需要
由 0 级管理员管理。

在大型组织中。常见的情况是，权限已经
在 GPO 级别以错误的方式委托。

...)

这里有一个例子，你可以看到一个随机用户有 GpoEdit
默认域控制器策略 GPO 的权限。



The screenshot shows the 'Default Domain Controllers Policy' properties window with the 'Delegation' tab selected. It displays a table of groups and users with their allowed permissions:

Name	Allowed Permissions	Inherited
Domain Admins (CORP\Domain Admins)	Custom	No
Domain Controllers (CORP\Domain Controllers)	Read (from Security Filtering)	No
Enterprise Admins (CORP\Enterprise Admins)	Custom	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No
Timo Werner (Werner@corp.contoso.com)	Edit settings	No

...)

这里有人决定添加对具有完全权限的域用户
默认域策略。

Default Domain Policy

Scope Details Settings Delegation

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (CORP\Domain Admins)	Custom	No
Domain Users (CORP\Domain Users)	Edit settings, delete, modify security	No
Enterprise Admins (CORP\Enterprise Admins)	Custom	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

如下图所示。有一个管理层

用于减轻凭证盗窃的模型。第 0 层管理员无法登录

第 1 层资源和第 1 层管理员不能登录第 2 层资源。

The left pane shows the organizational unit structure:

- Admin
 - Tier 0
 - Accounts
 - Devices
 - Groups
 - Service Accounts
 - Tier 0 Servers
 - Tier 1
 - Accounts
 - Devices
 - Groups
 - Service Accounts
 - Tier 2
 - Accounts
 - Devices
 - Groups
 - Service Accounts

The right pane is a table of resources:

Name	Type	Description
Tier 0	Organizational...	
Tier 1	Organizational...	
Tier 2	Organizational...	

...)

...)

应该管理应用于第 0 层服务器的所有 GPO

由 0 级管理员执行。

第 0 层服务器通常是关键服务器，如 ADFS、天青广告

连接、公钥基础设施、域控制器等。

The screenshot shows a Windows-based management interface. On the left, there is a navigation tree under the 'Admin' section. The tree includes 'Tier 0' (Accounts, Devices, Groups, Service Accounts, Tier 0 Servers), 'Tier 1' (Accounts, Devices, Groups, Service Accounts), and 'Tier 2' (Accounts, Devices, Groups, Service Accounts). The 'Tier 0 Servers' node is highlighted with a red box. On the right, there is a table with three rows:

Name	Type	Description
Tier 0	Organizational...	
Tier 1	Organizational...	
Tier 2	Organizational...	

• Recommendation

...)

...)

适用于域级别和域控制器需求的 GPO

由 0 级管理员管理。

应用于第 0 层服务器的 GPO 需要由第 0 层管理

管理员。

6.3 -停止使用组策略创建者所有者

组策略创建者所有者是广告中一个现成的内置组

拥有比需要更多的权利。

我们都知道组策略创建者 Owners 只能创建 GPO，但是

无法将它链接到某个东西，这已经使得使用它变得有点无用。

这个群体有点无用的另一个原因是，因为很难

委派对 CN =组策略中默认安全脚本的权限-

容器架构属性。此架构属性代表组策略。

...)

在这里，您可以看到域管理员和组策略创建者所有者

可以创建 GPO

The screenshot shows the 'Group Policy Objects in contoso.com' delegation page. On the left, the navigation pane shows 'Forest: contoso.com' and 'Domains'. Under 'Domains', 'contoso.com' is expanded, showing 'CertificatePolicy', 'Default Domain Policy', 'Domain Controllers', 'Managed-Objects', 'Group Policy Objects' (which is selected and highlighted with a red box), and 'WMI Filters'. The main pane title is 'Group Policy Objects in contoso.com'. It has tabs for 'Contents' and 'Delegation'. Below the tabs, it says 'The following groups and users can create GPOs in this domain.' A table lists 'Groups and users' with columns for 'Name', 'Inherited', and 'No'. The entries are: 'Domain Admins (CONTOSO\Domain Admins)' with 'Inherited' set to 'No'; 'Group Policy Creator Owners (CONTOSO\Group Policy Creator Owners)' with 'Inherited' set to 'No'; and 'SYSTEM' with 'Inherited' set to 'No'.

Name	Inherited
Domain Admins (CONTOSO\Domain Admins)	No
Group Policy Creator Owners (CONTOSO\Group Policy Creator Owners)	No
SYSTEM	No

...)

现在我已经向它添加了一个委托组。该组现在还可以创建

GPO

The screenshot shows the 'Group Policy Objects in contoso.com' delegation page. The navigation pane is identical to the previous one, with 'Group Policy Objects' selected. The main pane title is 'Group Policy Objects in contoso.com'. It has tabs for 'Contents' and 'Delegation'. Below the tabs, it says 'The following groups and users can create GPOs in this domain.' A table lists 'Groups and users' with columns for 'Name'. The entries are: 'Domain Admins (CONTOSO\Domain Admins)', 'Group Policy Creator Owners (CONTOSO\Group Policy Creator Owners)', 'SYSTEM', and 'TestGPOAdmins (CONTOSO\TestGPOAdmins)' (which is highlighted with a red box). The 'TestGPOAdmins' entry is part of a newly added delegation entry.

Name
Domain Admins (CONTOSO\Domain Admins)
Group Policy Creator Owners (CONTOSO\Group Policy Creator Owners)
SYSTEM
TestGPOAdmins (CONTOSO\TestGPOAdmins)

• Recommendations

以高效的方式管理组策略，而没有不必要的

特权需要以下条件：

...)

创建一个组并将其委托给组策略对象。允许此组

创建 GPO

The screenshot shows two windows side-by-side. On the left is the 'Group Policy Management' console under 'Forest: contoso.com'. In the 'Domains' section, 'contoso.com' is expanded, and 'Group Policy Objects' is selected and highlighted with a red box. On the right is a 'Group Policy Objects in contoso.com' window. It has tabs for 'Contents' and 'Delegation'. The 'Delegation' tab is active, showing the message: 'The following groups and users can create GPOs in this domain.' Below this is a list titled 'Groups and users:' with a 'Name' column. Four entries are listed: 'Domain Admins (CONTOSO\Domain Admins)', 'Group Policy Creator Owners (CONTOSO\Group Policy Creator Owners)', 'SYSTEM', and 'TestGPOAdmins (CONTOSO\TestGPOAdmins)'. The 'TestGPOAdmins' entry is also highlighted with a red box.

获取委托组的样本号

```
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
```

开放 ADSI。编辑和搜索 CN =组策略-容器

CN=Group-Policy-Container Properties	
Attribute Editor Security	
Attributes:	
Attribute	Value
adminDescription	Group-Policy-Container
adminDisplayName	Group-Policy-Container
auxiliaryClass	<not set>
classDisplayName	<not set>
cn	Group-Policy-Container
defaultHidingValue	TRUE
defaultObjectCategory	CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=contoso,DC=com
defaultSecurityDescriptor	D:P(A;CI;RPWPCCDCLCLORCWOWD;O;WD)
description	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=contoso,DC=com
dSASignature	<not set>
dSCorePropagationData	0x0 = ()

复制默认安全脚本并粘贴到记事本中：

付款交单(甲); CI; RPWPCCDCLCLOLORCWOWDSDDTSW; ; 裁军部)(一; CI;
RPWPCCDCLCLOLORCWOWDSDDTSW; ; 预期成绩)(一; CI;
RPWPCCDCLCLOLORCWOWDSDDTSW; ; 一氧化碳)(甲; CI;
RPWPCCdclCLOCLORCWwdSDDTSW; ; ; 西)(一; CI; 遥控门锁发射器; ; ; 非盟)(OA;
CI; 捷克共和国; edacfd 8f-FFB 3-11 D1-b41d-00 a 0 c 968 f 939; ; 非盟)

File Edit Format View Help

D:P(A;CI;RPWPCCDCLCLOLORCWOWDSDTSW;;;DA)(A;CI;RPWPCCDCLCLOLORCWOWDSDTSW;;;EA)(A;CI;RPWPCLCLOLORCWOWDSDTSW;;;EA)

现在复制以下部分：

付款交单(甲); CI; RPWPCCDCLCLOLCWOWDSDDTSW; ;

D:P(A;CI;RPWPCCDCLCLOLCWOWDSDDTSW;;;DA)(A;CI;RPWPCCDCLCLOLCWOWDSDDTSW;;;EA)(A;CI;RPWPCCDCLCLOLCWOWDSDDTSW;;;EA)

复制委托组的样本号

```
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
```

...)

将组的样本号放在上面复制部分的末尾。哪个

意味着你会得到这样的东西。

付款交单(甲); CI; RPWPCCDCLCLOLCWOWDSDDTSW; ; s-1-5-21-2367645265-
33317674-1292933090-12602)

现在复制整个默认安全脚本:

付款交单(甲); CI; RPWPCCDCLCLOLCWOWDSDDTSW; ; s-1-5-21-2367645265-
33317674-1292933090-12602)

...)

将其粘贴到默认安全性描述符的末尾，位于CN =组策略-

集装箱。它看起来会像这样:

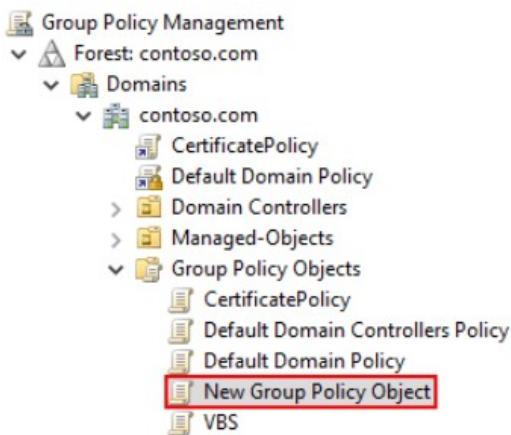
丁:(一); ; RPWPCRCCdcclCLOCLORCWOWdSDDTSW; ; ; 裁军部)(一; ;
RPWPCRCCdcclCLOCLORCWOWdSDDTSW; ; ; 教育署)(甲; ;
RPWPCRCCdcclCLOCLORCWOWdSDDTSW; ; ; 西)(一; ;
RPWPCRCCdcclCLOCLORCWOWdSDDTSW; ; ; 一氧化碳)

(一); ; 遥控门锁发射器; ; ; WD)D:P(A; CI; RPWPCCdcclcolorowDSDDTS W; ; ; s-1-5-21-
2367645265-33317674-1292933090-12602)

...)

现在，当用户创建 GPO 时。委派的组将是

以完全权限自动添加到其中。



The screenshot shows the 'New Group Policy Object' dialog box with the 'Scope' tab selected. It lists 'Groups and users:' with their 'Name' and 'Allowed Permissions'. A group named 'TestGPOAdmins (CONTOSO\TestGPOAdmins)' is highlighted with a red box.

Name	Allowed Permissions
Authenticated Users	Read (from Security Filtering)
Domain Admins (CONTOSO\Domain Admins)	Edit settings, delete, modify security
Enterprise Admins (CONTOSO\Enterprise Admins)	Edit settings, delete, modify security
ENTERPRISE DOMAIN CONTROLLERS	Read
SYSTEM	Edit settings, delete, modify security
TestGPOAdmins (CONTOSO\TestGPOAdmins)	Edit settings, delete, modify security

...)

...)

...)

如果您想允许委派组链接 GPO。给

OU 上的以下权限:

写入 gpLink → 链接 GPO 的权限

写入 gpOptions → 阻止继承的权限

7.1 -不要使用账户操作员

不要使用帐户操作符，因为它有很多现成的权限。

帐户操作员中的用户可能提升到域管理员。

The screenshot shows the 'Account Operators Properties' dialog box with the 'Members' tab selected. It lists a single member: 'Active Directory Domain Services Folder'.

Name
Active Directory Domain Services Folder

...)

...)

...)

攻击路径:

账户操作员→通用卡→交换信任子系统→

成员→交换窗口权限→在 DNC 上写入数据

DCSync

帐户操作符→通用代码→ DnsAdmins → 以

DC 系统=域管理员

参考:[https://ired . team/attack-security-experiments/active-directory-](https://ired.team/attack-security-experiments/active-directory-Kerberos-滥用/从 dnsadmins 到系统到域-妥协)

Kerberos-滥用/从 dnsadmins 到系统到域-妥协

参考:[https://dirkjanm . io/abusing-exchange-one-API-call-away-from-](https://dirkjanm . io/abusing-exchange-one-API-call-away-from-域管理员/)

域管理员/

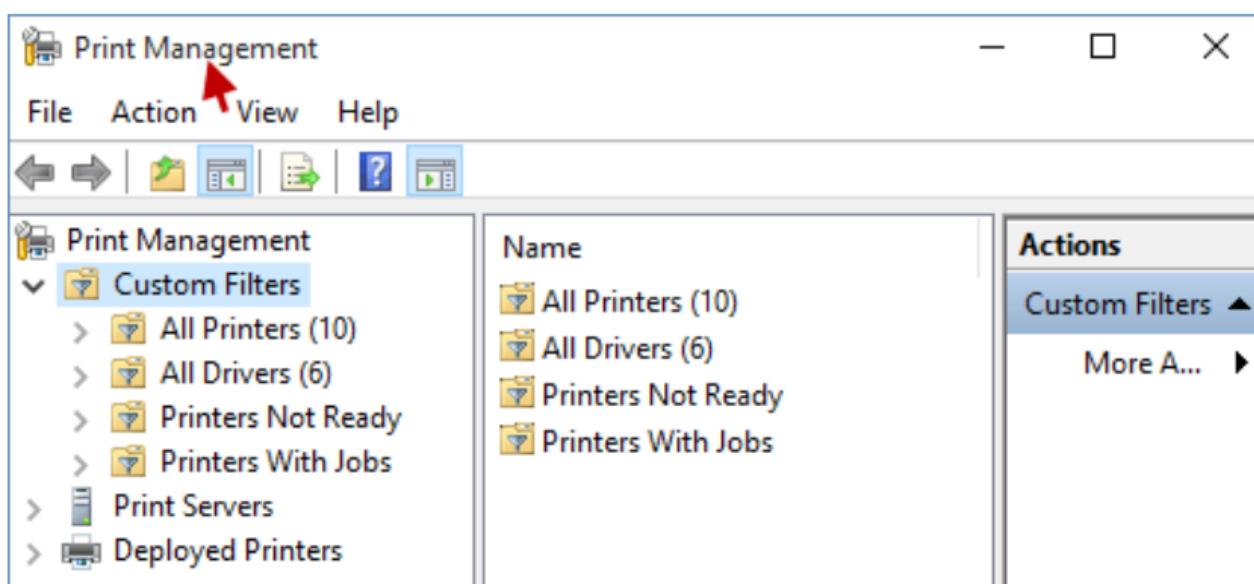
7.2 -不要使用打印操作员

默认情况下，打印操作员拥有域控制器的登录权限，即

这个团体绝对不需要。

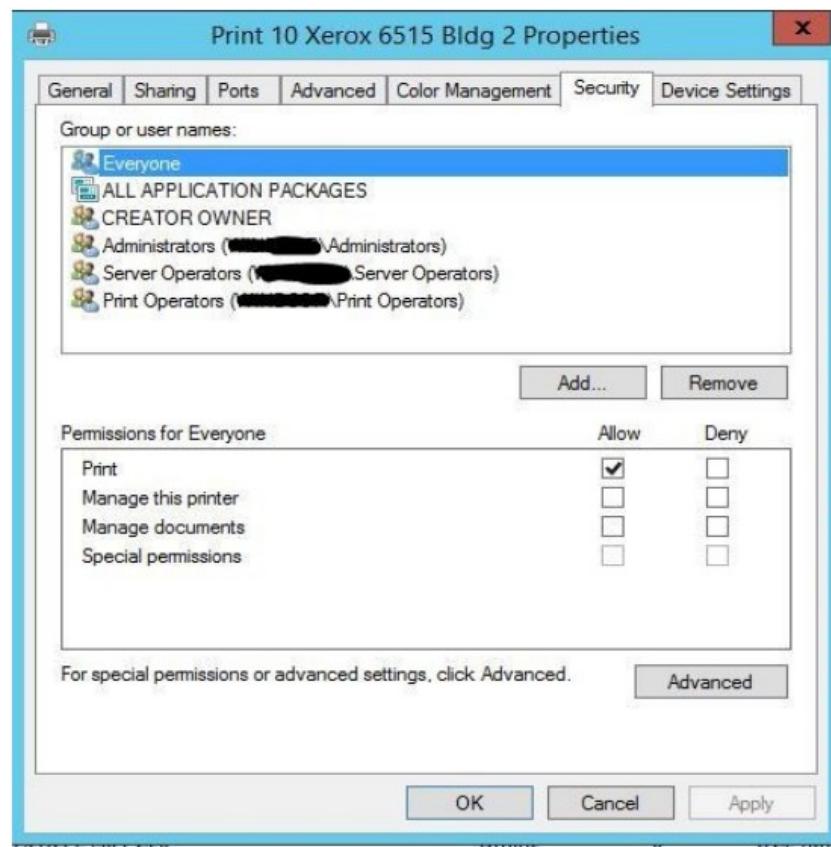
如果您确实使用了打印操作符。所有的权利也可以通过

打印管理。



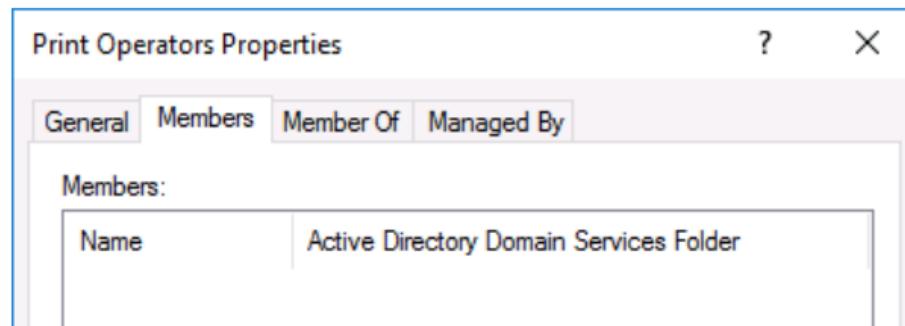
...)

像这样。您可以向 DACL 添加一个新组，并将所需的权限。



• Recommendation

确保打印操作员组为空。



7.3 -不要使用服务器运营商

服务器操作员是一个默认情况下也拥有很多权限的组，它

包括 DC 登录访问。这个群体通常被称为“DC 管理员”

我会避免使用这个组。

更多信息:<http://www.thenetworkencyclopedia.com/entry/server->

操作员-内置组/

7.4 - 打开活动目录回收站

假设您意外删除了活动目录中的一个对象，如

你的首席执行官的账户。

如果你能再次恢复它会有多好？

活动目录回收站默认情况下未启用。启用回收站

会帮助您恢复很多场景，其中有人意外运行了

例如，编写和删除大量计算机对象。

如何检查广告回收站是否已启用？

“获得采用”功能-过滤“类似名称的“回收站功能”

如你所见。我的域中没有启用它

```
PS C:\Users\Werner> Import-Module ActiveDirectory
PS C:\Users\Werner> Get-ADOptionalFeature -Filter 'name -like "Recycle Bin Feature"'

DistinguishedName : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=corp,DC=contoso,DC=com
EnabledScopes    : {}
FeatureGUID     : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
FeatureScope     : {ForestOrConfigurationSet}
IsDisableable   : False
Name            : Recycle Bin Feature
ObjectClass      : msDS-OptionalFeature
ObjectGUID       : f0ddcac6-909c-4970-9698-5644e941c002
RequiredDomainMode :
RequiredForestMode : Windows2008R2Forest
```

启用-采用功能“回收站功能”-范围

森林配置集-目标 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

打开活动目录回收站

...)

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

DistinguishedName : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=corp,DC=contoso,DC=com
EnabledScopes    : {CN=Partitions,CN=Configuration,DC=corp,DC=contoso,DC=com, CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=contoso,DC=com}
FeatureGUID      : /66ddcd8-acd0-445e-t3b9-a/t9b6/44t2a
FeatureScope     : {ForestOrConfigurationSet}
IsDisableable    : False
Name             : Recycle Bin Feature
ObjectClass      : msDS-OptionalFeature
ObjectGUID       : f0ddcac6-909c-4970-9698-5644e941c002
RequiredDomainMode :
RequiredForestMode : Windows2008R2Forest
```

7.5 -将恢复权限委托给第 1 级管理员
删除的对象

第 1 层或第 2 层管理员正在创建对象，但有时。可能会有一些情况

有人不小心删除了一个对象。

默认情况下，域管理员或等效人员可以恢复已删除的对象。好的

新闻是我们可以授权。

...)

...)

...)

首先，我们必须拥有“已删除对象”容器的所有权。

以数据助理权限运行 PowerShell

“中国=已删除对象， DC =公司， DC=contoso， DC=com”

/接管

```
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
Allow NT AUTHORITY\SYSTEM SPECIAL ACCESS
    DELETE
    READ PERMISSONS
    WRITE PERMISSIONS
    CHANGE OWNERSHIP
    CREATE CHILD
    DELETE CHILD
    LIST CONTENTS
    WRITE SELF
    WRITE PROPERTY
    READ PROPERTY

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

...)

现在，我们将委托“第1层”组上的权限，以便能够
还原对象。

DC =公司， DC =公司， DC =公司

第1层:LCRPWP

```
PS C:\windows\system32> dsacl "CN=Deleted Objects,DC=corp,DC=contoso,DC=com" /g CORP\Tier1:LCRPWP
Owner: CORP\Domain Admins
Group: NT AUTHORITY\SYSTEM

Access list:
{This object is protected from inheriting permissions from the parent}
Allow CORP\Tier1          SPECIAL ACCESS
                           LIST CONTENTS
                           WRITE PROPERTY
                           READ PROPERTY
Allow BUILTIN\Administrators SPECIAL ACCESS
                           LIST CONTENTS
                           READ PROPERTY
Allow NT AUTHORITY\SYSTEM   SPECIAL ACCESS
                           DELETE
                           READ PERMISSONS
                           WRITE PERMISSIONS
                           CHANGE OWNERSHIP
                           CREATE CHILD
                           DELETE CHILD
                           LIST CONTENTS
                           WRITE SELF
                           WRITE PROPERTY
                           READ PROPERTY

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

现在属于第 1 层组的每个人都可以恢复已删除的对象。

7.6 - 第 0 层管理员需要成为“受保护”的一部分
用户“”组

受保护用户是一个全局安全组，其主要功能是

防止用户的凭据在他们登录的设备上被滥用。

运行 Windows 8.1 的设备支持受保护用户组功能

和视窗服务器 2012(或更高版本)。

资料来源:<https://www.Petri.com/windows-server-protected-privileged-accounts>

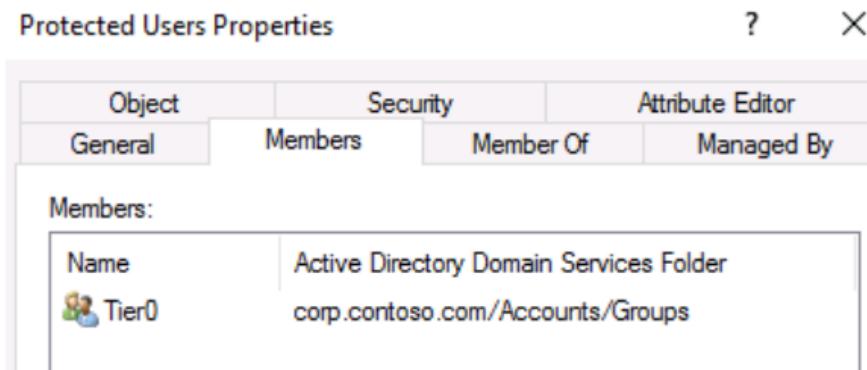
...)

0 级管理员通常是能够访问最关键的

资源，如域控制器等。



向受保护用户组添加第 0 层管理员。



7.7 - 第 0 层管理员需要拥有“”帐户
敏感且无法委派”复选标记

帐户是敏感的，不能委托确保帐户的

凭据不能转发到网络上的其他计算机或服务

受信任的应用程序。

允许应用程序代表用户工作的特性称为

Kerberos 代表团。

资料来源:<http://blogs.TechNet.Microsoft.com/poshchap/2015/05/01/security->

焦点分析账户是敏感的，不能授权给特权者

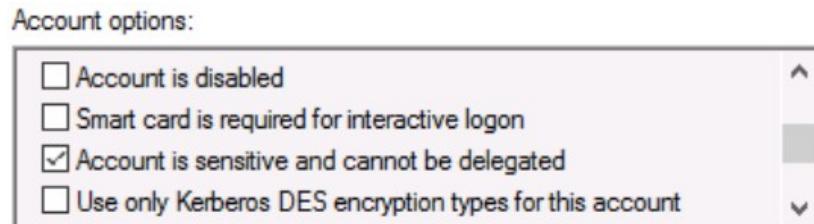
账户/

因为 0 级管理员是拥有最高权限的人。是的

建议所有第 0 层管理员启用此复选标记。

Name	Type	Description
Tier 0	Organizational...	
Tier 1	Organizational...	
Tier 2	Organizational...	

帐户是敏感的，不能委托，复选标记。



7.8 -重置 KRBTGT 的密码两次

每个活动目录环境的“KRBTGT”帐户都处于活动状态

目录。

KRBTGT 是 KDC 的服务负责人，负责加密和

签署域中的所有 Kerberos 票证。

如果攻击者成功获得了 KRBTGT 帐户的 NTLM 哈希。

可以创建黄金票据来模拟域中的每个用户

保持毅力。

这通常需要授权许可或同等权限，因此这意味着攻击者

已经在您的环境中拥有领域优势。

...)

...)

重置 KRBTGT 的密码两次，以制作金券

对攻击者无效。

您上次重设密码两次是什么时候？

```
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
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

...)

...)

每半年重置 KRBTGT 账户两次。这已经讨论过了

很多次，但这是一个常见的行业最佳实践。就像 STIG 建议的那样。

每 180 天重置一次。

确保在进行第二次之前有 10-24 小时的延迟

重置。换句话说。首先重置 KRBTGT 的密码，然后等待

进行第二次密码重置前 10-24 小时。微软建议

这个。

仅重置一次密码会发生什么情况？

攻击者仍然可以使用他的金券。

```
.#####. 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

mimikatz # [Administrator: C:\WINDOWS\SYSTEM32\cmd.exe]
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
```

当您重置密码两次时会发生什么？

金券失效。

```
.#####. 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' @ 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 -监控活动中的高特权群体

目录

像域管理员和企业管理员这样的高特权群体至关重要

监视，因为攻击者很可能会攻击这些组织

请记住，有更多的高特权群体，他们通常

忘记，例如内置\管理员、模式管理员、帐户

操作员、备份操作员、服务器操作员、打印操作员，

DnsAdmins，组织管理，交换信任子系统，

交换窗口权限。

...)

...)

当有人被添加到企业管理员组时，您是否进行监控

例如。

这是添加到企业管理员组的一个 SQL 服务帐户。

The screenshot shows the 'Enterprise Admins Properties' dialog box with the 'Members' tab selected. The 'Members:' section displays a table with two rows. The first row contains 'Administrator' and 'corp.contoso.com/Users'. The second row, which includes 'SQL Agent S...', is highlighted with a red box. The table has columns for 'Name' and 'Active Directory Domain Services Folder'.

Name	Active Directory Domain Services Folder
Administrator	corp.contoso.com/Users
SQL Agent S...	corp.contoso.com/Accounts/Services

- **Recommendation**

...)

...)

开始监控高特权组，但不仅限于域或

企业管理组

事件 4728 ''成员已添加到启用安全的组''-

监控此事件，因为这可能是滥用权限的迹象。喜欢

将服务帐户添加到域管理等。



Event Properties - Event 4728, Microsoft Windows security auditing.

General Details

A member was added to a security-enabled global group.

Subject:

Security ID: CORP\Mark
Account Name: Mark
Account Domain: CORP
Logon ID: 0x1CE6AD

Log Name: Security

Source: Microsoft Windows security Logged: 12/29/2019 9:59:08 AM

Event ID: 4728 Task Category: Security Group Management

Level: Information

Keywords: Audit Success

User: N/A

Computer: DC.corp.contoso.com

OpCode: Info

More Information: [Event Log Online Help](#)

8.2 -部署蜂蜜用户进行 Kerberoasting 测试

我们都可能听说过 Kerberoasting。这种攻击允许

通过身份验证的用户使用

服务原则名称。

有了这些服务票，他们就可以导出并离线破解。如果你

对如何进行攻击很好奇。

请看看:<https://attack.stealthbits.com/cracking-kerberos-tgs->

使用 kerberoasting 测试的票据

这是攻击者的步骤。

...)

...)

...)

...)

使用 SPN 扫描帐户

申请服务票

出口服务票

快客服务票

[例子]

...)

攻击者枚举域管理员组并发现服务

使用 SPN 帐户，在这种情况下。"SQLAgent"

```
PS C:\Users\Mark> net group "Domain Admins" /domain
Group name      Domain Admins
Comment        Designated administrators of the domain

Members

Administrator      Mark      Peter
SQLAgent           SQLAgent
The command completed successfully.

PS C:\Users\Mark> setspn -L SQLAgent
Registered ServicePrincipalNames for CN=SQL Agent Service Account,OU=Services,OU=Accounts,DC=corp,DC=contoso,DC=com:
MSSQLSvc/corp.contoso.com:DBA:1443
PS C:\Users\Mark> -
```

攻击者请求 "SQLAgent" 帐户的服务票证。

```
PS C:\Users\Mark> setspn -L SQLAgent
Registered ServicePrincipalNames for CN=SQL Agent Service Account,OU=Services,OU=Accounts,DC=corp,DC=contoso,DC=com:
  MSSQLSvc/corp.contoso.com:DBA:1443
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:1443"

Id          : uuid-34abd67b-3d2d-4a5e-be8e-8ca8696fe918-1
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom   : 12/29/2019 7:37:27 PM
ValidTo     : 12/30/2019 5:37:27 AM
ServicePrincipalName : MSSQLSvc/corp.contoso.com:DBA:1443
SecurityKey  : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

...)

...)

事件 4769 将显示在安全日志中。"一张 Kerberos 服务票证

被请求"

如你所见。马克向 SQLAgent 申请了一张服务票。这

服务帐户是我们亲爱的用户。

Event Properties - Event 4769, Microsoft Windows security auditing.

General Details

Account Name:	Mark@CORP.CONTOSO.COM
Account Domain:	CORP.CONTOSO.COM
Logon GUID:	{4366a6d1-904a-1189-bd90-529bcf738881}
Service Information:	
Service Name:	SQLAgent
Service ID:	CORP\SQLAgent
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4769
Level:	Information
User:	N/A
OpCode:	Info
Keywords:	Audit Success
Computer:	DC.corp.contoso.com
Logged:	12/29/2019 11:37:27 AM
Task Category:	Kerberos Service Ticket Operation:
More Information:	Event Log Online Help

• Recommendation

...)

...)

...)

...)

创建一个虚假的服务帐户，但尽可能让它看起来真实。

给帐户分配一个假的 SPN。

将蜂蜜用户添加到域管理或类似的功能中。

监控何时有人向您亲爱的用户申请服务票

账户。4769

[例子]

我已经在域管理员组中添加了一个蜜用户帐户。

Domain Admins Properties

Object		Security		Attribute Editor	
General	Members	Member Of	Managed By		
Members:					
Name	Active Directory Domain Service Account				
Administrator	corp.contoso.com/Users				
Mark Hassall	corp.contoso.com/Accounts				
Peter Houston	corp.contoso.com/Accounts				
SQL Agent Service Account	corp.contoso.com/Accounts				
SQL DB Engine Service Account	corp.contoso.com/Accounts				

在蜂蜜用户上注册一个假 SPN。

```
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=contoso
MSSQLSvc/corp.contoso.com:DBA:1334
Updated object
PS C:\windows\system32>
```

在这里，我们可以看到 SQLDBEngine 现在有了一个假的 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=contoso
MSSQLSvc/corp.contoso.com:DBA:1334
PS C:\windows\system32>
```

现在，当攻击者请求我们的蜂蜜用户的 SPN 时。

```
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=contoso
MSSQLSvc/corp.contoso.com:DBA:1334
PS C:\windows\system32> Add-Type -AssemblyName System.IdentityModel
PS C:\windows\system32> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/corp.contoso.com:DBA:1334"

Id : uuid-58906ec6-6df0-4c11-a666-f474301e9ddd-1
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 12/29/2019 7:58:25 PM
ValidTo : 12/30/2019 5:27:14 AM
ServicePrincipalName : MSSQLSvc/corp.contoso.com:DBA:1334
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

...)

...)

我们可以抓住他或她。

在这里我们可以看到马克已经向一个

未映射到广告中任何内容的帐户。

 Event Properties - Event 4769, Microsoft Windows security auditing.

General Details

Account Name:	Mark@CORP.CONTOSO.COM
Account Domain:	CORP.CONTOSO.COM
Logon GUID:	{7c7f5b3c-d5cd-1103-fa95-d76e8648f580}

Service Information:

Service Name:	SQLDBEngine
Service ID:	CORP\SQLDBEngine

Log Name: Security
Source: Microsoft Windows security Logged: 12/29/2019 11:58:25 AM
Event ID: 4769 Task Category: Kerberos Service Ticket Operation:
Level: Information Keywords: Audit Success
User: N/A Computer: DC.corp.contoso.com
OpCode: Info
More Information: [Event Log Online Help](#)

9.1 -理解管理系统管理的概念

分层模型

微软管理层模型的目的是通过以下方式减少凭据

使用不同的级别。第 1、2 和 3 层。

第 0 层=有权访问最关键的域管理员或同等人员

像域控制器、天青广告、ADFS 和公钥基础设施这样的服务器。

第 1 层=通常是可以访问不同服务器的服务器管理员，例如

文件服务器、打印服务器、exchange 等。

第 2 层=可以访问工作站的工作站/服务台管理员

客户。

第 0 层管理员只能访问第 0 层资源。第 1 层管理员只能访问

第 1 层资源和第 2 层管理员只能访问第 2 层资源。

[例子]

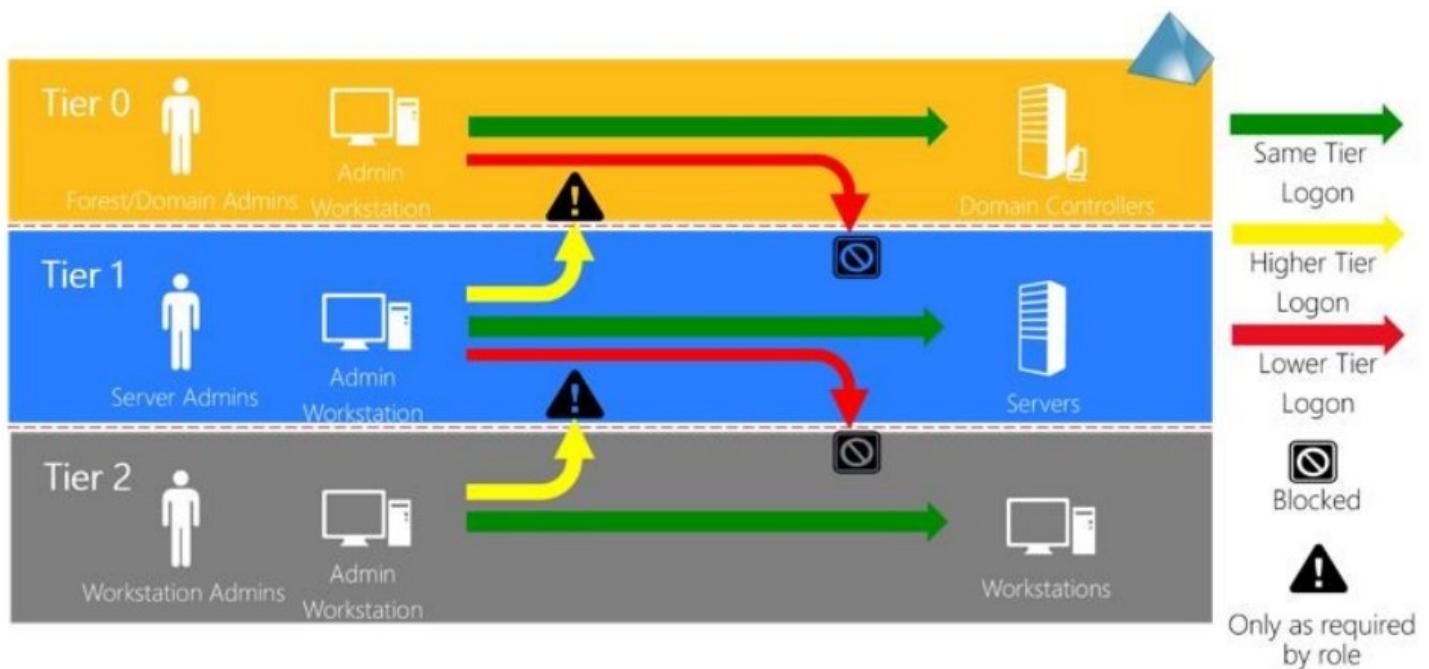
第 0 层管理员无法登录第 1 层服务器或工作站，因为他不是

允许这样做。

第 2 层管理员不能登录第 1 层服务器，因为不允许他们登录。

第 1 层管理员不能登录第 0 层或第 2 层等。

有道理吗？



9.2 -如何设计微软管理层模型？

首先，您需要创建一个类似如下的 ou 结构：

	Name	Type	Description
	Tier 0	Organizational...	
	Tier 1	Organizational...	
	Tier 2	Organizational...	

第 0 层

...)

...)

...)

...)

...)

帐户=活动目录中所有第 0 层管理员的帐户

设备=所有第 0 层管理员的计算机对象。

组=第 0 层管理员的广告组

服务帐户=在第 0 层上作为服务运行的服务帐户

服务器

第 0 层服务器=蓝色广告连接的计算机对象，ADFS，公钥基础设施，

核动力源等。

域控制器也是如此，但是我建议将它们留在域中

控制器 OU。

第 1 层

...)

...)

...)

...)

...)

帐户=活动目录中所有第 1 层管理员的帐户

设备=所有第 1 层管理员的计算机对象。

组=第 1 层管理员的广告组

服务帐户=在第 1 层上作为服务运行的服务帐户

服务器

第 1 层服务器=文件服务器、打印服务器、SQL 的计算机对象

服务器等。您环境中的其余服务器。

第 2 层

...)

...)

...)

...)

...)

帐户=活动目录中所有第 2 层管理员的帐户

设备=所有第 2 层管理员的计算机对象

组=第 2 层管理员的广告组

服务帐户=在上作为服务运行的服务帐户

客户端工作站

第 2 层工作站=所有客户端的工作站

这就是它的样子。这是一个设计，所以你有一种感觉

可以实现模型。我只会从第 0 层的角度来指导它。在那里

是处理这个模型的更不同的方法。

[例子]

...)

...)

在第 0 层的“组”OU 中创建一个组。

将属于第 0 层的所有用户添加到此组。

The screenshot shows the Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane displays the following structure:

- Active Directory Users and Computers [DC.corp.contoso.com]
- Saved Queries
- corp.contoso.com
 - Accounts
 - Admin
 - Tier 0
 - Groups (highlighted with a red box)
 - Accounts
 - Devices
 - Service Accounts
 - Tier 0 Servers

On the right, a table lists the group 'Tier0' with its details:

Name	Type	Description
Tier0	Security Group...	Tier 0 admins

...)

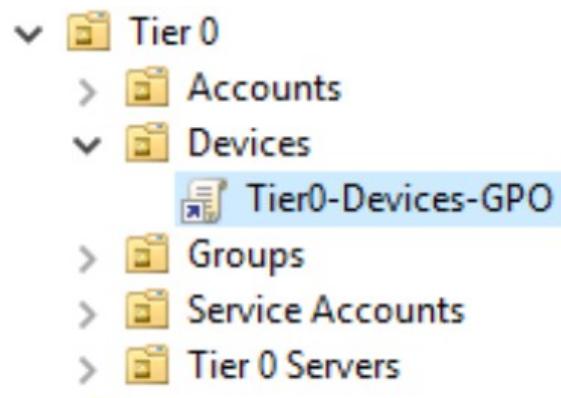
...)

现在我们将创建一个 GPO，并将其链接到层中的“设备”OU

0

正如你在图片中看到的。我创建了一个 GPO，并将其链接到

组织单位“设备”



现在我将使用以下设置编辑该 GPO:

在第 0 层管理员的设备上。只有本地管理员帐户和

Tier0 组应该是本地管理员组的成员。

Name	Action	SID
CORP\Tier0	ADD	S-1-5-21-3566
Administrator	ADD	

第 0 层设备上的下列组应该为空。

...)

备份操作员、加密操作员、网络配置

操作、超级用户、远程桌面用户、复制器

The screenshot shows the Windows Local Users and Groups snap-in. On the left, the navigation pane lists 'Tier1-Devices-GPO [DC.CORP.C...' under 'Computer Configuration' and 'Preferences'. Under 'Preferences', 'Local Users and Groups' is selected. The main pane displays a table of local groups:

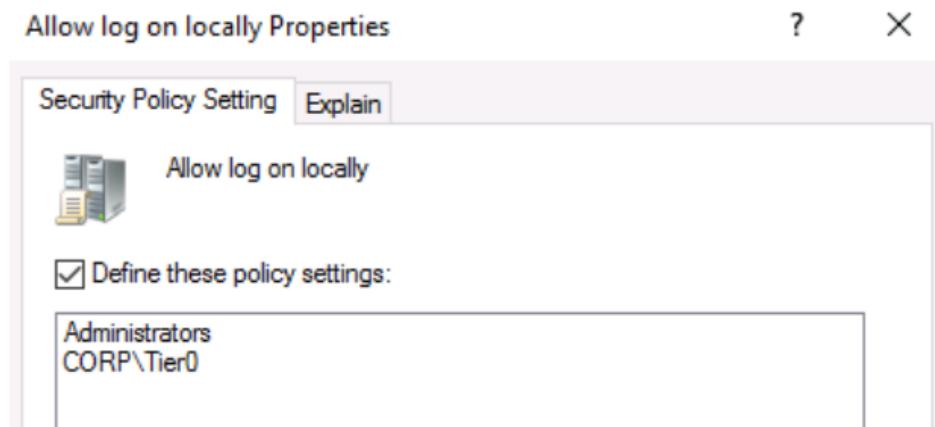
Name	Order	Action	Full Name	Description
Administrators (built-in)	1	Update	N/A	Built-in Administrators
Backup Operators (built-in)	2	Update	N/A	
Cryptographic Operators (built-in)	3	Update	N/A	
Network Configuration Operators (built-in)	4	Update	N/A	
Power Users (built-in)	5	Update	N/A	
Remote Desktop Users (built-in)	6	Update	N/A	
Replicators (built-in)	7	Update	N/A	

The 'Administrators (built-in)' row is highlighted with a red box.

...)

在用户权限分配-我已经允许管理员和第 0 层用户

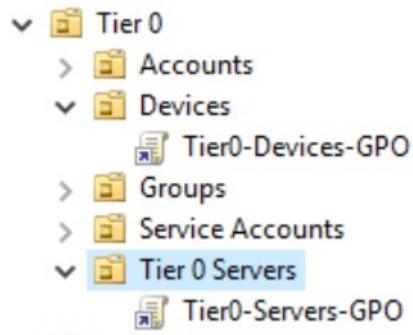
能够本地登录设备。



现在我已经用这个 GPO 完成了。

现在，我必须创建一个新的 GPO，并将其链接到层中的“第 0 层服务器” OU

0.这个 GPO 被称为“tier 0-服务器-GPO”



...)

...)

该图形处理器应包含与第 0 层设备图形处理器相同的设置。

确保只有本地管理员和第 0 层管理员

第 0 层服务器上本地管理员组的成员。

确保第 0 层服务器上的以下组为空:

备份运营商、加密运营商、网络

配置操作、超级用户、远程桌面用户，

复制者

...)

...)

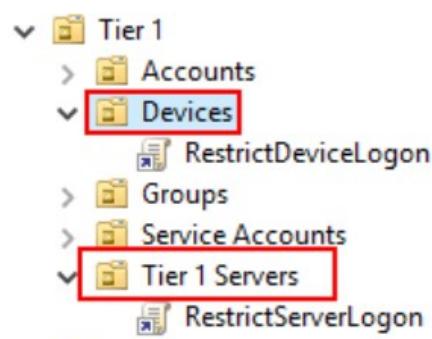
因为我们都知道第 0 层管理员通常是域管理员或

等效物。我们必须拒绝对较低层的登录访问，这就是

凯斯。第 1 层和第 2 层。

我创建了两个 GPO，并将其链接到“设备”和“第 1 层”

第 1 层的服务器 “” OU



...)

...)

...)

两个 GPO 都包含以下设置:用户权限分配

拒绝从网络访问这台计算机:域管理员，

企业管理员、模式管理员、Tier0

拒绝本地登录:域管理员、企业管理员、架构

管理员, Tier0

拒绝通过远程桌面服务登录:域管理员，

企业管理员、模式管理员、Tier0

...)

...)

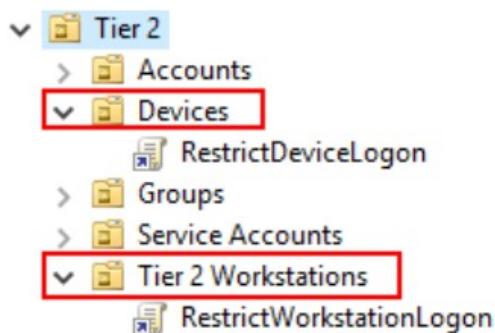
现在我已经链接了完全相同的 GPO，称为

“限制设备登录” 到第 2 层的 OU“设备”

我已经用完全相同的设置创建了一个新的 GPO，但是只使用了

不同的名字，也就是“限制性工作站登录”和我有

将此链接到“第 2 层工作站”OU



• Recommendation

...)

...)

在我的例子中。我只是从第 0 层演示了它。你仍然需要

确保第 1 层设备处于干净状态，并且只有本地设备

管理员和第 1 层组是本地管理员的一部分

第 1 层设备和第 1 层服务器上的组。

除此之外，您需要确保第 1 层管理员不能登录第 1 层

2 项资产。例如，第 2 层管理员的设备或

客户端的工作站。

...)

...)

...)

在第 2 层区域。只有本地管理员和第 2 层组应该是

第 2 层管理员和的设备上的本地管理员组的一部分

客户的工作站。

我在每一层都创建了一个名为“服务帐户”的组织单位——很好

例如，有很多供应商声称拥有“授权厂商”特权，或者

否则他们不会支持。分层模式有助于减少停机服务

帐户登录到较低层。

有关更多信息：

<http://docs.Microsoft.com/en-us/windows-server/identity/securing->

特权访问/安全特权访问参考资料

9.3 -从第 0 层管理 Azure 广告连接

Azure 广告连接服务器包含关键的身份数据，应该

视为活动目录中记录的第 0 层组件

管理层模型。

资料来源:<https://docs.Microsoft.com/en-us/azure/active-directory/hybrid/how-to->

连接-安装-先决条件# azure-ad-连接-服务器

...)

在这里，您可以看到 Azure 广告连接是从第 0 层管理的操作。

The screenshot shows the Windows Active Directory Users and Computers (ADUC) interface. On the left, there is a navigation tree for the domain 'corp.contoso.com'. The 'Admin' node is expanded, showing 'Tier 0', 'Tier 1', and 'Tier 2' sub-nodes. Under 'Tier 0', the 'Service Accounts' node is also expanded, showing 'Tier 0 Servers' as the final child node. On the right, a table lists objects in the current view. One row is highlighted with a red border: 'AADCONNECT' (Type: Computer, Description: Azure AD Connect). The 'Tier 0 Servers' node in the navigation tree is also highlighted with a red box.

Name	Type	Description
AADCONNECT	Computer	Azure AD Connect

• Recommendations

...)

...)

从第 0 层操作管理 Azure 广告连接。本地攻击者

对 AAD 服务器的管理员访问会危及整个活动服务器

目录域。

Azure 广告连接需要作为第二个域控制器受到威胁。

资料来源:<https://blog.xpnsec.com/azuread-connect-for-redteam/>

...)

所有应用于 Azure 广告连接的 GPO 都需要管理

从第 0 层操作或其他未经授权的用户将能够

将自己添加到本地管理员组。

9.4 -从 0 级管理 ADFS

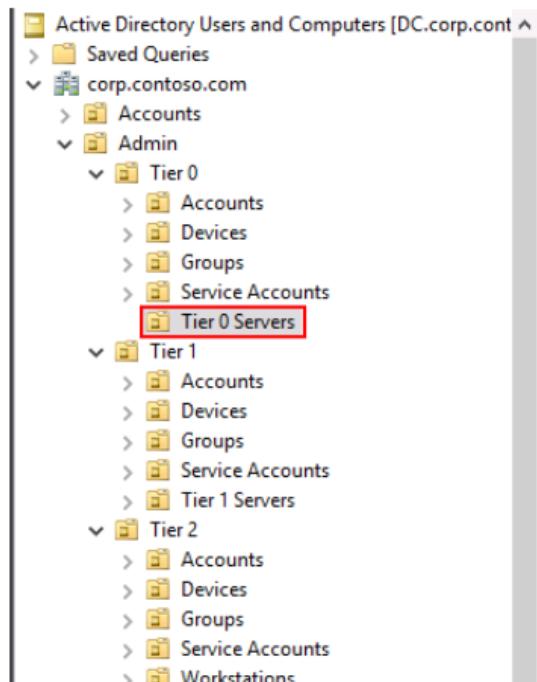
从根本上说，广告金融服务是一个认证系统。因此，它应该得到治疗

作为“第 0 层”系统，与网络上的其他身份系统一样。

来源：

[http://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/best-ad-fs 的安全规划和部署实践](http://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/best-ad-fs的安全规划和部署实践)

在这里，您可以看到 ADFS 是从 0 级运营管理的。



Name	Type	Description
AADCONNECT	Computer	Azure AD Connect
ADFS	Computer	Active Directory Federation Services

• Recommendations

...)

...)

从 0 级开始管理 ADFS

确保 ADFS 服务器上应用的所有 GPO

从第 0 层管理。

10.1 -部署 Azure 广告密码保护

蓝色广告密码保护帮助您更好地了解用户，

使用或挑选糟糕的密码。

蓝色广告密码保护最酷的一点是，它还

适用于内部，而不仅仅是云。

我们总是遇到攻击者使用不同技术的问题，

例如密码喷洒。因为用户选择了糟糕的密码，而且

攻击者喜欢追逐他们。

在下图中。你可以看到攻击者取得了一些成功

通过使用“密码 123456”

密码喷洒

```
Saruy
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
```

...)

学分:<https://ired.team/offensive-security-experiments/active->

目录-Kerberos-滥用/active-目录-密码喷洒

注意:如果您计划在内部使用 Azure 广告密码保护。它

仅在公共云中受支持。因为 Azure 没有内部版本

广告密码保护

要求

...)

...)

...)

...)

...)

...)

...)

蓝色广告高级 P1 或 P2

所有域控制器必须至少运行视窗服务器 2012 或

稍后安装 DC 代理软件

所有域控制器都需要微软。已安装. NET 4.5

Azure 广告密码保护代理所在的所有成员服务器

将安装服务。必须在 2012 R2 或更高版本的视窗服务器上运行。

所有带有 Azure 广告密码保护代理服务的成员服务器

必须有微软。已安装. NET 4.7。

至少一个域控制器之间必须存在网络连接

在每个域和至少一个托管代理服务的服务器中

密码保护。这种连接必须允许域控制器

要访问上的 RPC 端点映射器端口 135 和 RPC 服务器端口

代理服务

安装了 Azure 广告密码保护的所有成员服务器

必须能够通过网络访问以下内容:

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

...)

列表还在继续，所以请在这里进一步阅读：

<http://git hub . com/MicroSoft DOCs/azure-DOCs/blob/master/articles/active->

目录/认证/如何-密码-禁止-内部错误-部署. md

我假设您已经阅读了链接，并且完全理解

在部署 Azure 广告密码保护之前，您必须首先做什么。它

给你一个完整的演练。

<http://tech community . Microsoft . com/t5/ITOps-Talk-Blog/分步->

实现-Azure-AD-密码-保护-开启/ba-p/563342

请在测试环境中进行测试，因为你有机会

做些蠢事。

注意：这是在测试环境中测试的。

...)

...)

如果一切顺利。您现在将在收到以下活动

Microsoft-AZUReadPasswordProtection-DCagent/Admin

事件：3006 ' ' 服务现在强制执行以下 Azure 密码

策略 “”

The screenshot shows the Windows Event Viewer interface. On the left is a tree view of logs, and on the right is a list of events. One event is selected, highlighted with a red border.

Level	Date and Time	Source	Event ID	Task Category
Information	12/30/2019 7:16:04 AM	DCAgent	30006	None

Event details for Event 30006, DCAgent:

The service is now enforcing the following Azure password policy.

Enabled: 1
AuditOnly: 1
Global policy date: 2019-11-03T00:00:00.000000000Z
Tenant policy date: 1601-01-01T00:00:00.000000100Z
Enforce tenant policy: 1

这就是我当前的设置。

...)

Custom banned password list ⓘ

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

...)

现在我将把它改为“强制”，而不是审计。我会的

阻止被禁止的密码。

Manage

Authentication method policy (...)

Password protection

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Passw0rd!
qwerty123456

Custom banned password list ⓘ

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

...)

这里有一个例子，艾米的密码已经过期，所以她需要

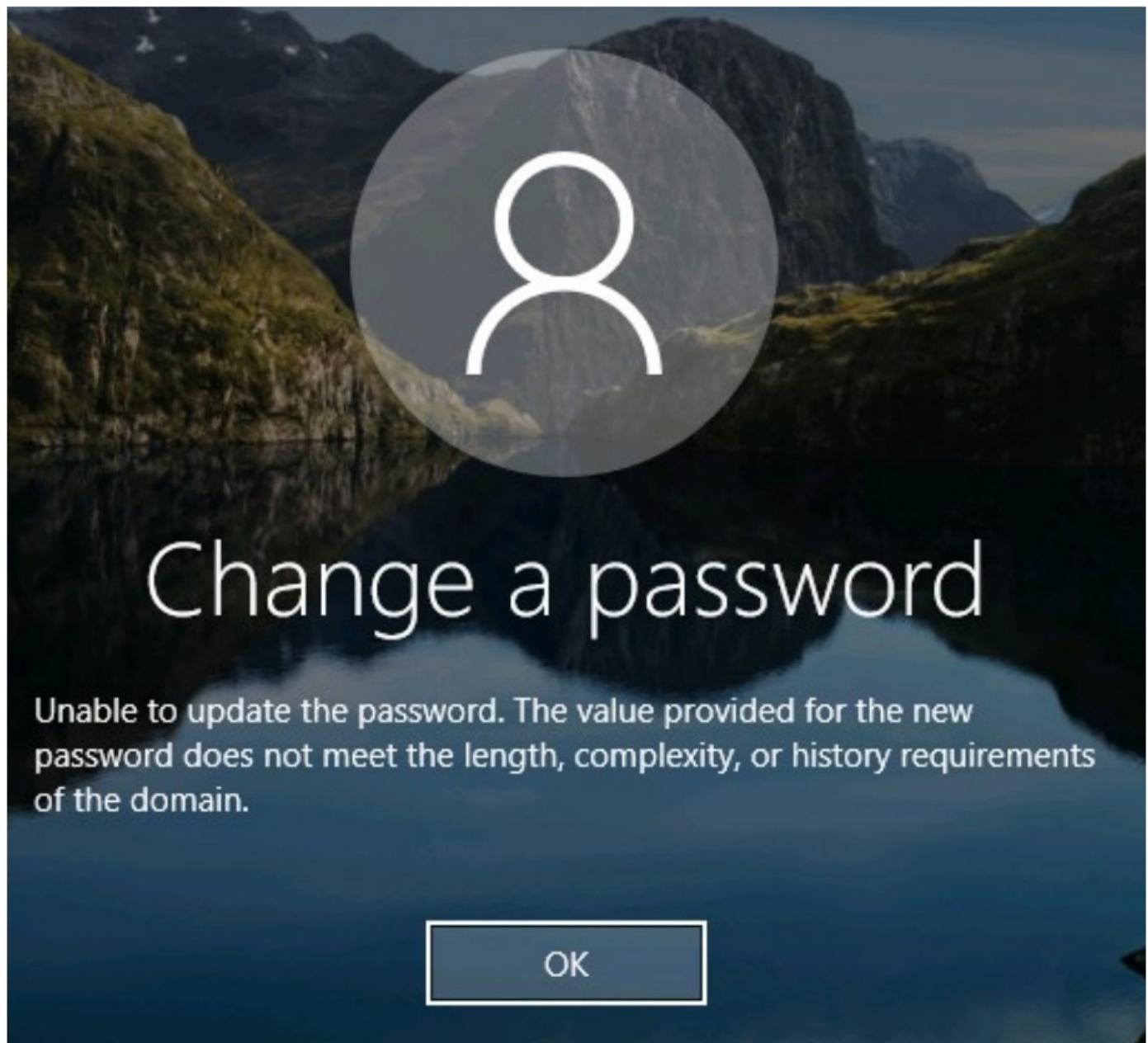
改变她的密码。



--)

当她决定将密码更改为“密码 0rd! \\ '还是什么

相似。将会发生以下情况。



--)

全局禁止密码列表基于以下信息

可以在这里找到：

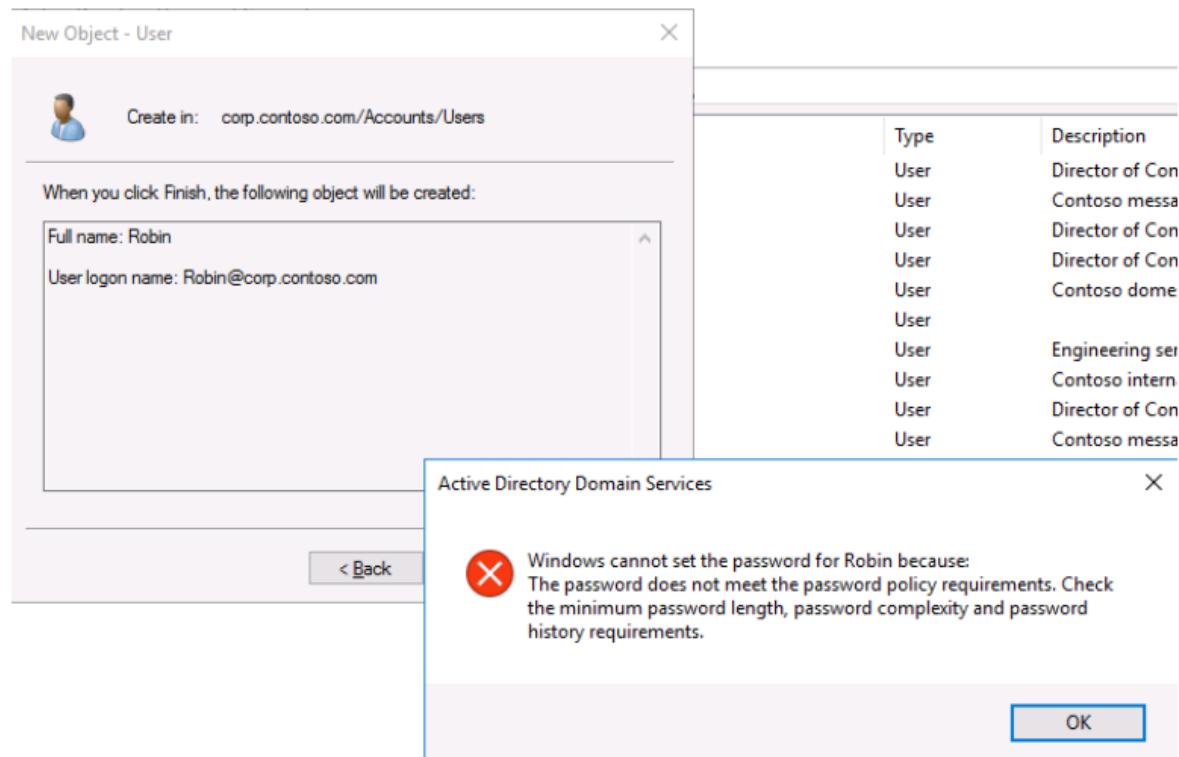
<http://git hub . com/MicroSoft DOCs/azure-DOCs/blob/master/articles/active->

目录/认证/概念-密码-禁止-坏. md

...)

当有人创建一个新用户并决定选择一个穷人时

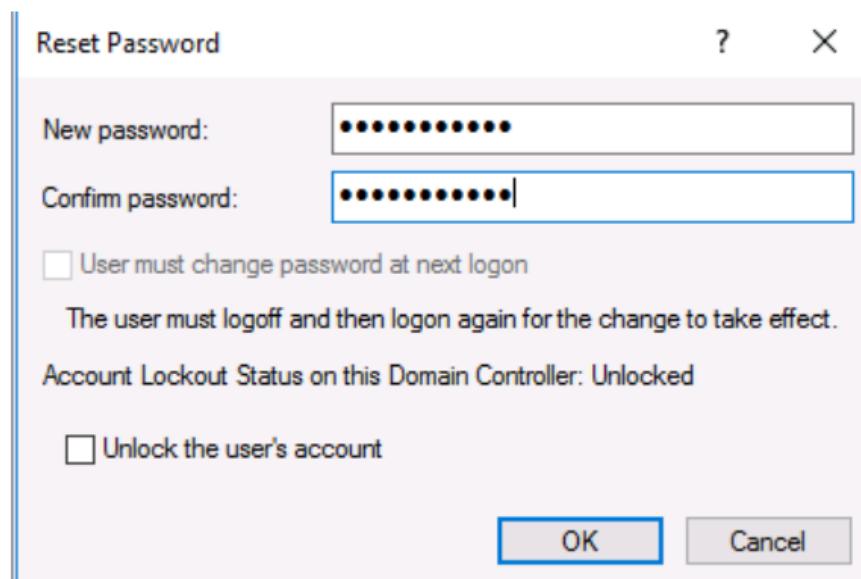
密码。将显示以下消息



...)

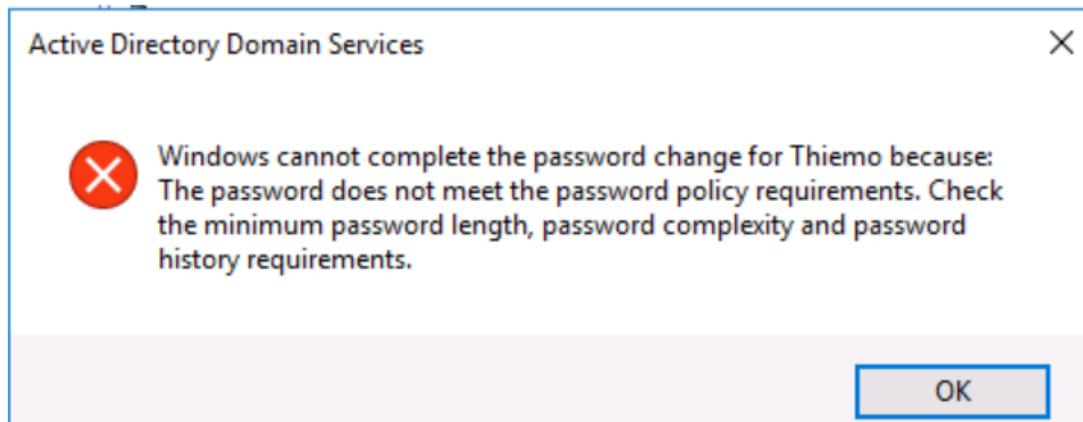
当有人想要重置用户的密码并决定

选择弱密码...



将显示以下消息

...)



...)

当它处于审计模式时。你会看到事件 3009，上面写着

密码已被接受，但在

禁止的密码列表。

Event Viewer (Local)

Custom Views

Windows Logs

Applications and Services Logs

Active Directory Web Server

AD FS

Device Registration Service

DFS Replication

Directory Service

DNS Server

File Replication Service

Forefront Identity Manager

Hardware Events

Internet Explorer

Key Management Service

Microsoft

AppV

AzureADConnect

AzureADPasswordPrc

DCAgent

Admin

Operational

Trace

Admin Number of events: 11

Level	Date and Time	Source	Event ID	Task Category
Information	12/30/2019 7:46:32 AM	DCAgent	10025	None
Information	12/30/2019 7:46:32 AM	DCAgent	30009	None
Information	12/30/2019 7:39:25 AM	DCAgent	10025	None
Information	12/30/2019 7:39:25 AM	DCAgent	30009	None
Information	12/30/2019 7:34:10 AM	DCAgent	10025	None
Information	12/30/2019 7:34:10 AM	DCAgent	30009	None

Event 3009, DCAgent

General Details

The reset password for the specified user would normally have been rejected because it matches at least one of the tokens present in the Microsoft global banned password list of the current Azure password policy. The current Azure password policy is configured for audit-only mode so the password was accepted.

UserName: Craig

FullName: Craig Dewar

- Recommendation

...)

...)

如果您尚未部署 Azure 广告密码保护，请开始部署。

在转到“强制”之前，请先从“审核”模式开始

The screenshot shows the 'Authentication methods - Password protection' settings in the Azure AD Security blade. The left sidebar has 'Manage' selected, with 'Password protection' highlighted. The main area shows 'Custom smart lockout' settings: 'Lockout threshold' is set to 10, and 'Lockout duration in seconds' is set to 60. Below that is a section for 'Custom banned passwords' with a switch set to 'No'. A list of banned passwords is shown: 'Passw0rd!' and 'qwerty123456'. There's also a 'Custom banned password list' link. At the bottom, there's a section for 'Password protection for Windows Server Active Directory' with a switch set to 'Yes' and a 'Mode' switch set to 'Audit'.

...)

确保您首先在中部署了 Azure 广告密码保护

测试环境，看看您是否完全理解实现。是的

没那么难，但总会出错，

这很好。我们都可以从错误中学习！

10.2 -为来宾和默认帐户设置密码
账户

默认情况下，访客和默认帐户在广告中没有密码。好消息是

两个帐户都被禁用，但是如果有人启用它们。他们可以登录

那些账户。

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

PS C:\Users\Mark> Get-ADUser -Filter * -Properties PasswordLastSet | Where-Object {$_.PasswordLastSet -eq $null}

DistinguishedName : CN=Guest,CN=Users,DC=corp,DC=contoso,DC=com
GivenName          :
Name               :
ObjectClass        : user
ObjectGUID         : ee80aca4-ccf7-47bb-ad32-870a681b93f4
PasswordLastSet   :
SamAccountName    : Guest
SID                : S-1-5-21-3566662483-2648771335-1709913503-501
Surname           :
UserPrincipalName :



DistinguishedName : CN=DefaultAccount,CN=Users,DC=corp,DC=contoso,DC=com
GivenName          :
Name               :
ObjectClass        : user
ObjectGUID         : 84a5efa9-49c2-4de3-ac0c-8a726aed902d
PasswordLastSet   :
SamAccountName    : DefaultAccount
SID                : S-1-5-21-3566662483-2648771335-1709913503-503
Surname           :
UserPrincipalName :
```

建议

为两个帐户设置密码。

11.1 -自由访问控制列表

(DACL)由对象所有者控制的访问控制列表

指定特定用户或组对对象的访问权限。

资料来源:https://docs.microsoft.com/en-us/windows/win32/sec_gloss/d-Gly

例子

这里有一个叫保罗·韦斯特的用户。标记为红色的一侧

定义 ACL，它标识哪些用户或组被分配或拒绝

对对象的权限。

正如你在图片中看到的。有不同的组被分配给

对象，如已验证用户、证书发布者和域管理员。

Paul West Properties

? X

Published Certificates	Member Of	Password Replication	Dial-in	Object
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
Security	Environment	Sessions	Remote control	

Group or user names:

- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (CORP\Domain Admins)
- Cert Publishers (CORP\Cert Publishers)

[Add...](#) [Remove](#)

Permissions for ENTERPRISE DOMAIN CONTROLLERS

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Allowed to authenticate	<input type="checkbox"/>	<input type="checkbox"/>
Change password	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click [Advanced](#).

ACL 由对象的所有者控制。在这个例子中。

域管理员。

Advanced Security Settings for Paul West

Owner: Domain Admins (CORP\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	RAS and IAS Servers (CORP\R...	Read account restricti...	None	This object only
Allow	RAS and IAS Servers (CORP\R...	Read logon information	None	This object only
Allow	RAS and IAS Servers (CORP\R...	Read group members...	None	This object only
Allow	RAS and IAS Servers (CORP\R...	Read remote access in...	None	This object only
Allow	Cert Publishers (CORP\Cert P...		None	This object only
Allow	Windows Authorization Acce...		None	This object only
Allow	Terminal Server License Serve...		None	This object only
Allow	Terminal Server License Serve...	Read/write Terminal S...	None	This object only
Allow	Everyone	Change password	None	This object only
Allow	SELF	Change password	None	This object only

域管理员有权控制特定用户的访问

团体。例如拒绝对对象的读取访问。

Paul West Properties

Published Certificates Member Of Password Replication Dial-in Object
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization
Security Environment Sessions Remote control

Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Jeff Wang (jeff@corp.contoso.com)
- Domain Admins (CORP\Domain Admins)
- Cert Publishers (CORP\Cert Publishers)

Add... Remove

Permissions for Jeff Wang

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Allowed to authenticate	<input type="checkbox"/>	<input type="checkbox"/>
Change password	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

例子

在这里，我以用户马克的身份登录，我将对用户进行查询

保罗。

所有结果将显示给马克。

```
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
```

这里我以用户杰夫的身份登录，我也将在

用户保罗，但这次。我不会得到任何结果。因为“读取”权限

被否认了。

```
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,M
icrosoft.ActiveDirectory.Management.Commands.GetADUser
PS C:\Users\Jeff> _
```

11.2 -访问控制条目

访问控制条目是访问控制列表中的条目，包含

描述与特定安全相关的访问权限的信息

标识符或用户。

资料来源:<http://www.techopedia.com/definition/24/access-control-list-ACL>

microsoft

例子

我们在 11.1 中读到，ACL 指定了特定的访问、用户或

组拥有一个对象。

ACE 是访问控制列表中描述哪些访问权限的条目

被指派。

在这里我们可以看到丹·帕克有权修改许可

米歇尔并能接管她的账户。

Advanced Security Settings for Michelle Fredette

Owner: Domain Admins (CORP\Domain Admins) Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SELF	Read/write phone and...	None	This object only
Allow	SELF	Read/write web infor...	None	This object only
Allow	Dan Park (dan@corp.contoso.com)	Modify permissions	None	This object only
Allow	Domain Admins (CORP\Domain Admins)	Full control	None	This object only
Allow	Account Operators (CORP\Account Ope...	Full control	None	This object only
Allow	Authenticated Users	Read permissions	None	This object only
Allow	SELF	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access (...)	Special	DC=corp,DC=contoso...	Descendant InetOrgF...

可利用王牌列表:<https://wald0.com/?p=112>

11.3 -基于 ACL 的攻击示例

BloodHoundAD 是一个在活动目录中绘制不同攻击路径的工具

基于可利用的 ACL 和 ACEs。

这个工具的伟大之处主要在于它为你做的自动化。

而不是手动寻找。它将向您展示所有不同的攻击路径

例如，域管理员。

我强烈鼓励每个人在自己的环境中运行该工具，以了解

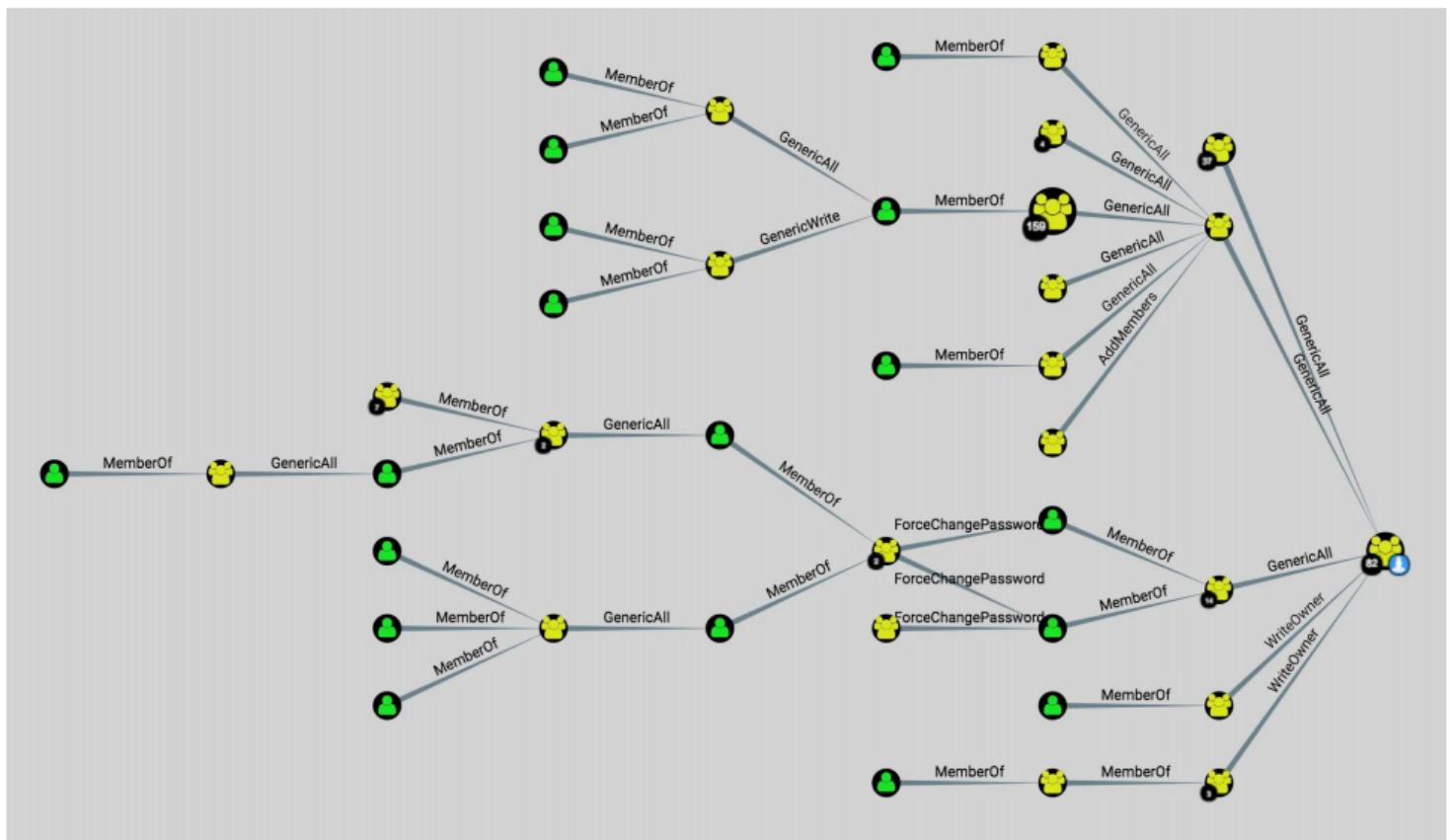
如何“保护”他们在活动目录中的配置。

在大多数环境中，有很多5年或10年前的遗留物

当你运行这个工具的时候可能会震惊你。或许域用户可以成为

域管理员？

在这里找到工具：<https://github.com/BloodHoundAD/Bloodhound/wiki>



12.1 - PingCastle

PingCastle 是一个免费的基于窗口的实用程序，用于审计广告的风险级别

基础设施并检查易受攻击的实践。

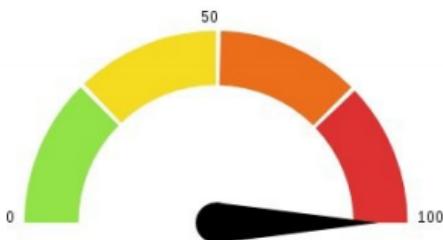
这个工具是文森特·勒图开发的，它能让你快速

概览和漂亮的仪表板，查看您在广告中的风险得分。

下载平城堡：<https://www.pingcastle.com/download/>

例子

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better



Risk model

Staled Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			Temporary admins
			Weak password

13 -确认和参考

...)

...)

...)

...)

...)

...)

...)

...)

<http://blog.fox-it.com/2018/04/26/upgrading-privileges-with-ACL-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>

我要感谢所有作者的写作和发表。确实如此

提高对活动目录的认识，组织开始

注意它。