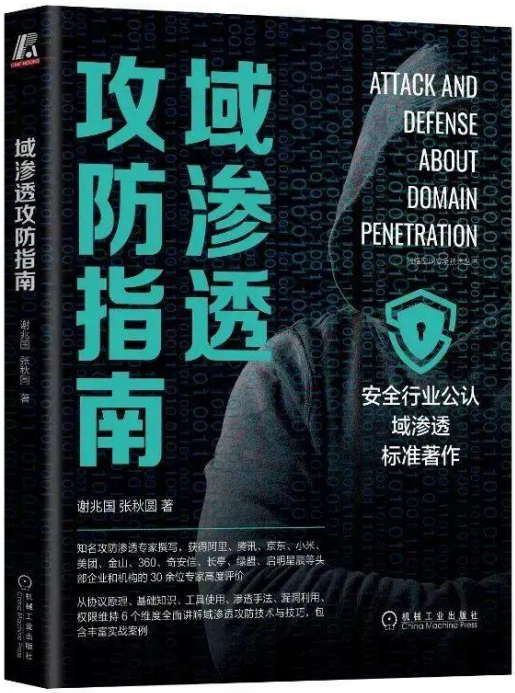
fcmit.cc

目录分区 Directory Partitions

本文部分节选于《域渗透攻防指南》，购买请长按如下图片扫码



由活动目录域服务 ADDS 控制的域林中的每个域控制器都包含目录分区 Directory Partitions。目录分区 Directory Partitions 也被称为命名上下文(Naming Context，简称 NC)。目录分区 Directory Partitions 是具有独立的复制范围和调度数据的整个目录的连续部分。默认情况下，企业的活动目录域服务包含以下目录分区：

- 域目录分区(Domain Directory Partition)：每一个域各有一个域目录分区，域目录分区包含与本地域相关联的目录对象，如用户和计算机等。一个域可以有多个域控制器，一个林可以有多个域。每个域控制器为其本地域存储域目录分区的完整副本，但不存储其他域的域目录分区的副本。如图中的 DC=xie,DC=com 就是域目录分区。

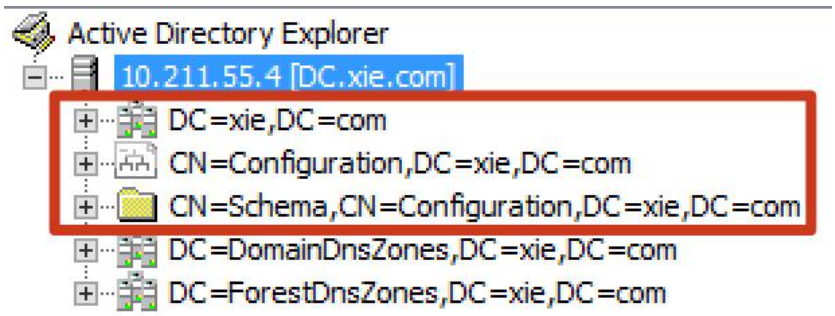
- 配置目录分区(Configuration Directory Partition)：配置目录分区包含复制拓扑和必须复制的其他配置数据。整个林内所有域共享一份相同的配置目录分区，林中的每个域控制器都有一个相同的配置目录分区的副本，对配置目录分区所做的任何更改都将复制到林中的每个域控制器。如图中的 CN=Configuration,DC=xie,DC=com 就是配置目录分区。

- 架构目录分区(Schema Directory Partition)：架构目录分区包含所有类和所有属性的条目对象，这些条目对象定义了林中可以使用的类和属性的类型。整个林内所有域共享一份相同的架构目录分区，林中的每个域控制器都有一个相同的架构目录分区的副本，对架构目录分区所做的任何更改都将复制到林中的每个域控制器。因为架构目录分区规定了信息的存储方式，因此在执行测试后，应该在必要时通过严格控制的过程对架构目录分区进行更改，以确保不会对林中的其他部分产生不利影响。如图中的 DC=Schema,CN=Configuration,DC=xie,DC=com 就是架构目录分区。

- 应用程序目录分区(Application Directory Partition)：从 Windows Server 2003 开始 ，微软引入了应用程序目录分区，其允许用户自定义分区来扩展目录分区。它提供了控制复制范围的能力，并允许以更适合动态数据的方式放置副本。应用程序目录分区会被复制到林中特定的域控中，而不是所有的域控中。如图中的 DC=DomainDnsZones,DC=xie,DC=com 和 DC=ForestDnsZones,DC=xie,DC=com 就是应用程序目录分区。

我们使用 ADExplorer 连接活动目录数据库就可以看到不同的目录分区，如图所示，用红色框住的分别是域目录分区、配置目录分区和架构目录分区，而后面两个则是应用程序目录分区。

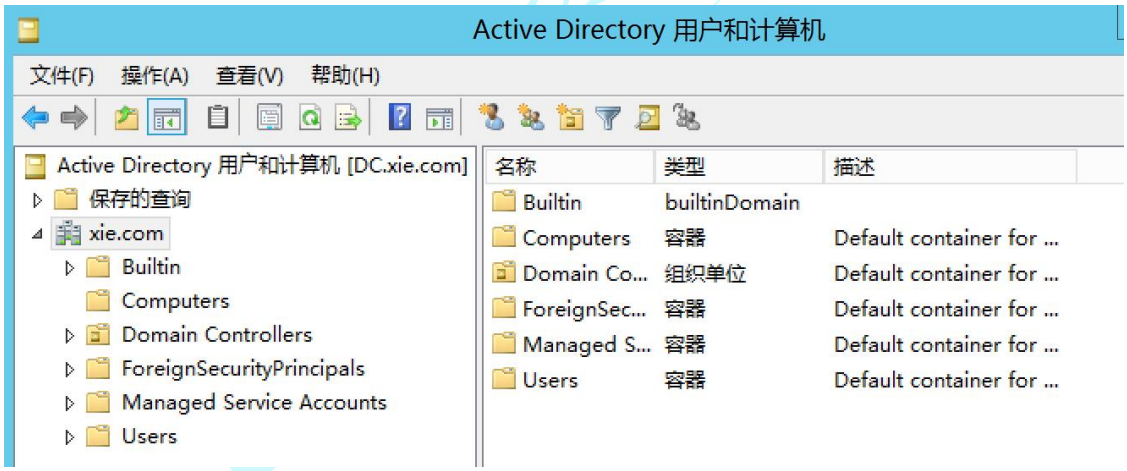
fcmit.cc



Domain Directory Partition

每一个域各有一个域目录分区(Domain Directory Partition)，不同的域有不同的域目录分区，域目录分区包含与本地域相关联的目录对象，如用户和计算机等。我们打开 Active Directory 用户和计算机查看的默认分区就是域目录分区。

如图所示，打开“Active Directory 用户和计算机”查看到的就是域目录分区。

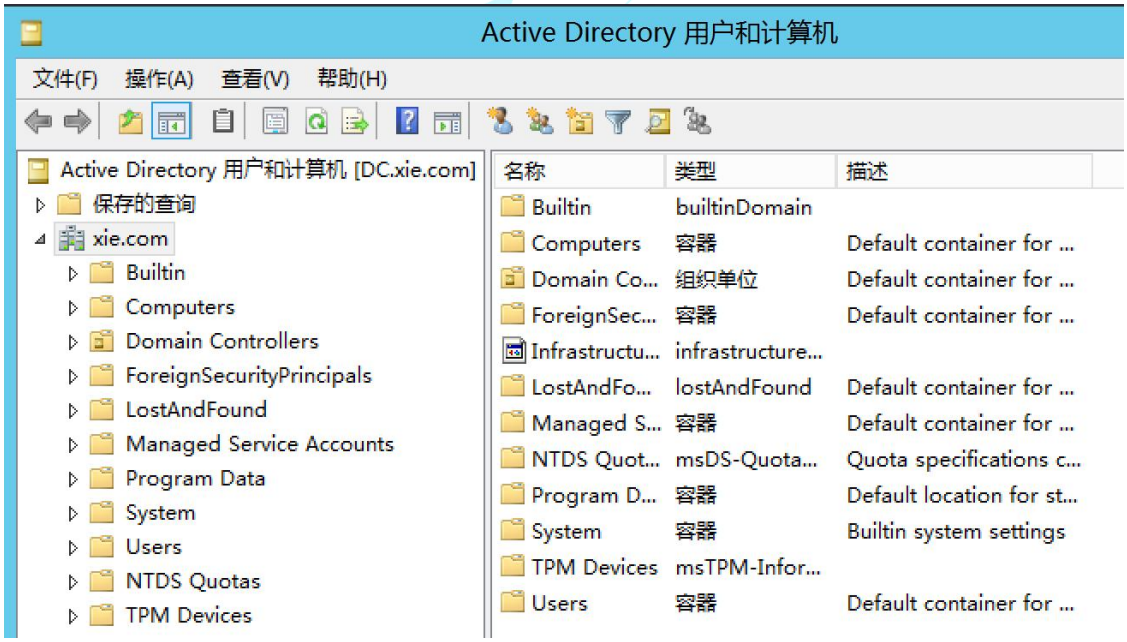


点击查看——>高级功能，如图所示：

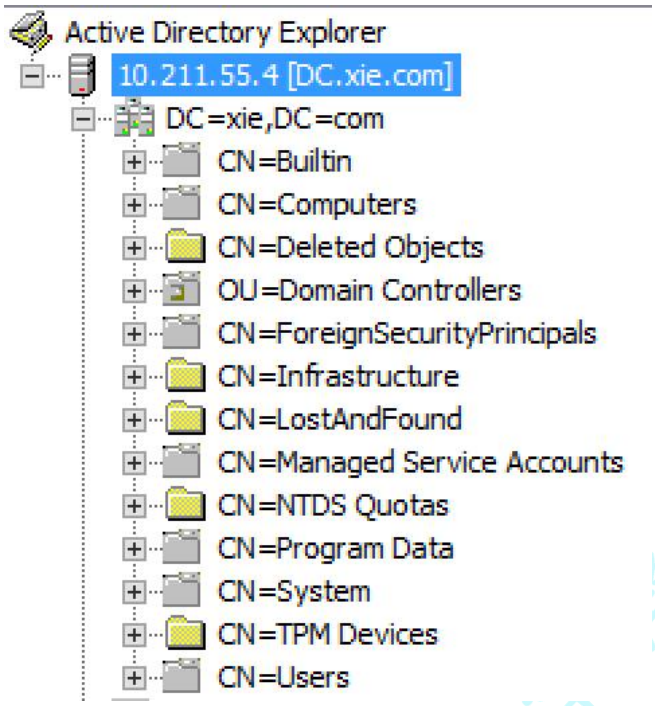
fcmit.cc

fcmit.cc

可以看到域目录分区的更多对象，如图所示：



如果使用 AD Explorer 查看域目录分区的话，默认会比“Active Directory 用户和计算机”查看的东西要多，如图 2-289 所示：



1. 域目录分区的顶级对象

如下表所示，是域目录分区的顶级对象以及这些顶级对象的说明：

RDN	说明
CN=Builtin	该容器内置了本地域组的安全组
CN=Computers	机器用户的容器，包括加入域的所有机器
OU=Domain Controllers	域控制器组织单位，包括域内所有域控
CN=ForeignSecurityPrincipals	代表域中来自森林外部域的组中的成员
CN=Managed Service Accounts	托管服务帐户的容器
CN=System	各种预配置对象的容器。包括信任对象，DNS 对象和组策略对象

fcmit.cc

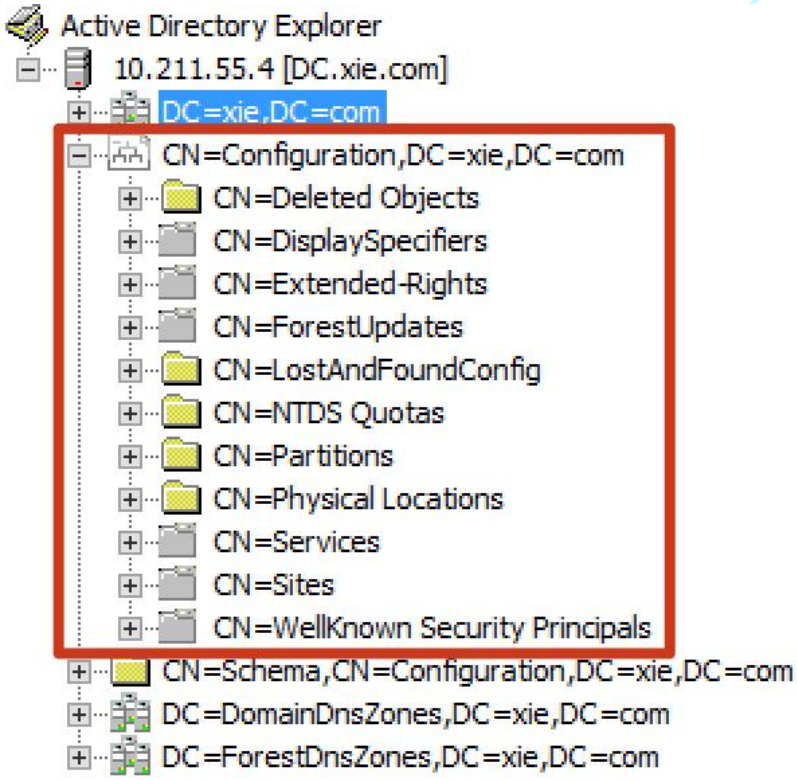
fcmit.cc

CN=Users 用户和组对象的默认容器

Configuration Directory Partition

配置目录分区(Configuration Directory Partition)包含复制拓扑和必须复制的其他配置数据，整个林内所有域共享一份相同的配置目录分区。配置目录分区是林根域的子容器。例如，xie.com 林的配置目录分区为 CN=Configuration,DC=xie,DC=com。使用“Active Directory 用户和计算机”默认无法查看到配置目录分区。

如图所示，使用 AD Explorer 查看配置目录分区。



1. 配置目录分区的顶级对象

如下表所示，是配置目录分区的顶级对象以及这些顶级对象的说明：

RDN	说明

CN=DisplaySpecifiers	定义了 Active Directory 管理单元的各种显示格式
CN=Extended-Rights	扩展权限对象的容器，我们将在域内 ACL 那篇文章里面详解
CN=ForestUpdates	包含用于表示森林状态和与域功能级别更改的对象
CN=Partitions	包含每个 Naming Context，Application Partitions 以及外部 LDAP 目录引用的对象
CN=Physical Locations	包含位置对象，可以将其与其他对象关联 以表示该对象的位置。
CN=Services	存储有关服务的配置信息，比如文件复制服务
CN=Sites	包含所有站点拓扑和复制对象
CN=WellKnown Security Principals	包含常用的外部安全性主题的对象，比如 Anonymous，Authenticated Users，Everyone 等等

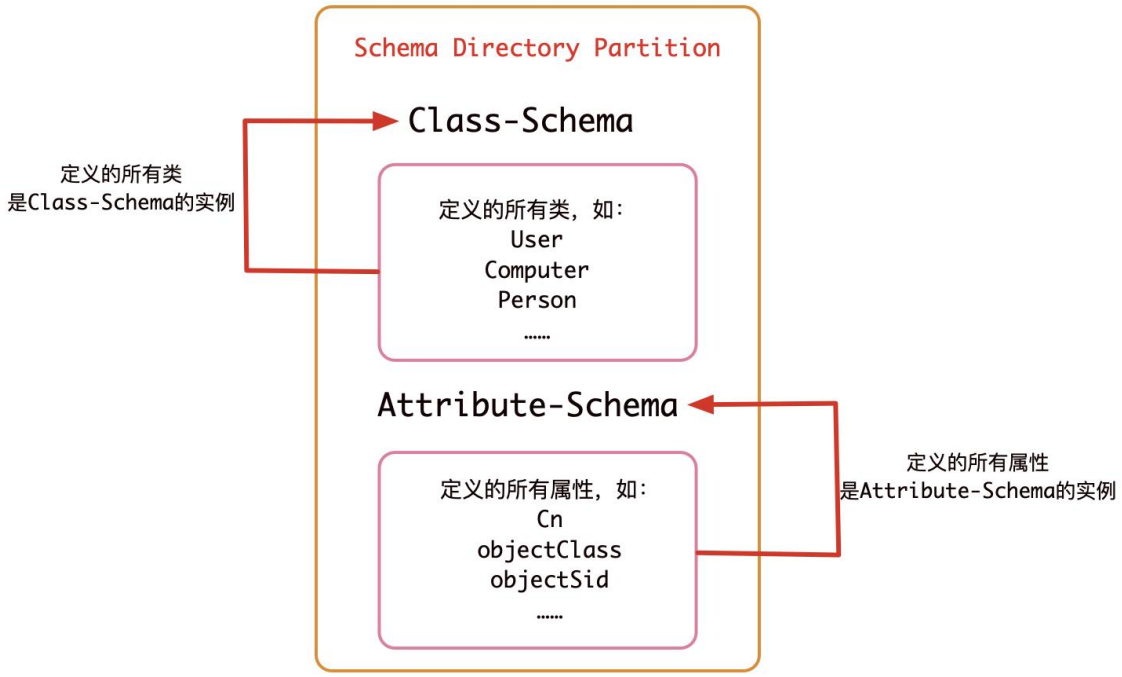
Schema Directory Partition

架构目录分区(Schema Directory Partition)包含所有类和所有属性的条目对象，这些条目对象定义了林中可以使用的类和属性的类型。整个林内所有域共享一份相同的架构目录分区，林中的每个域控制器都有一个相同的架构目录分区的副本，对架构目录分区所做的任何更改都将复制到林中的每个域控制器。因为架构目录分区规定了信息的存储方式，所以在执行测试后，应该在必要时通过严格控制的过程对架构目录分区进行更改，以确保不会对林的其他部分产生不利影响。与域目录分区和配置目录分区不同的是，架构目录分区不维护容器或组织单位的层次结构。相反，它是具有 Class-Schema ，Attribute-Schema 和 subSchema 对象的单个容器。活动目录数据库中所有类都是 Class-Schema 的实例，而所有属性是 Attribute-Schema 的实例。也就是说，架构目录分区定义了 Active Directory 中使用的所有类和属性。

fcmit.cc

fcmit.cc

如图所示，可以看到域内定义的所有属性和类与 Class-Schema、Attribute-Schema 的关系。



1. 查看 Schema Directory Partition

“Active Directory 用户和计算机”默认无法查看到架构目录分区，因此如果我们要查看架构目录分区的内容，可以使用 AD Explorer。

如图所示，使用 ADExplorer 连接查看架构目录分区。

fcmit.cc

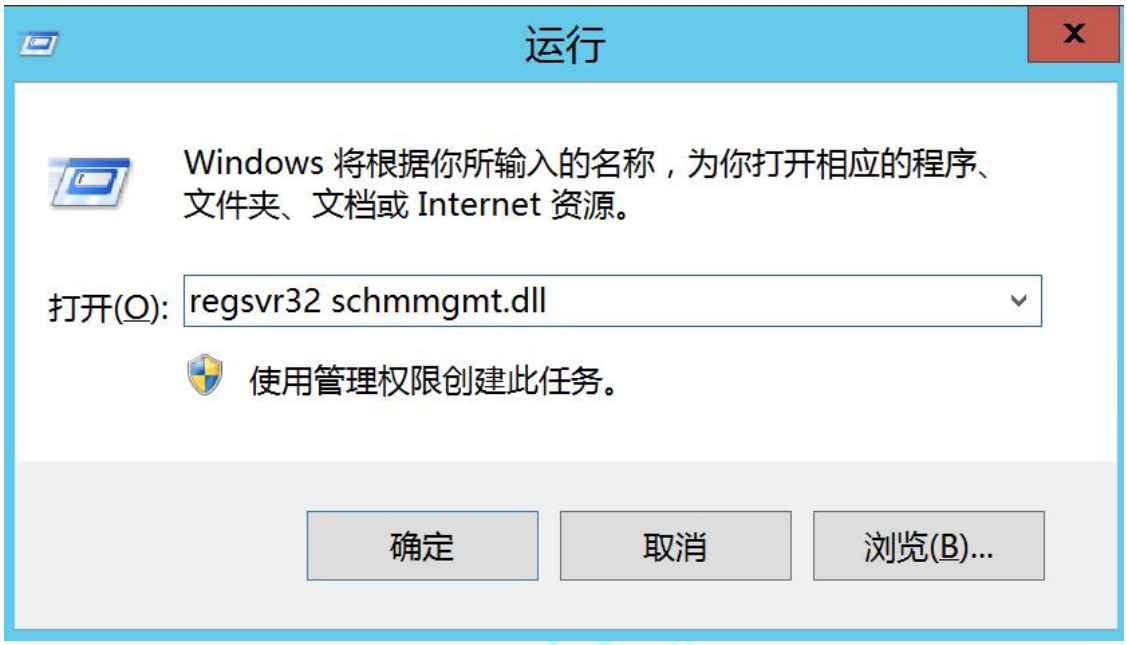
Active Directory Explorer

- 10.211.55.4 [DC.xie.com]
  - DC=xie,DC=com
  - CN=Configuration,DC=xie,DC=com
  - CN=Schema,CN=Configuration,DC=xie,DC=com
    - CN=account
    - CN=Account-Expires
    - CN=Account-Name-History
    - CN=ACS-Aggregate-Token-Rate-Per-User
    - CN=ACS-Allocable-RSVP-Bandwidth
    - CN=ACS-Cache-Timeout
    - CN=ACS-Direction
    - CN=ACS-DSBM-DeadTime
    - CN=ACS-DSBM-Priority
    - CN=ACS-DSBM-Refresh
    - CN=ACS-Enable-ACS-Service
    - CN=ACS-Enable-RSVP-Accounting
    - CN=ACS-Enable-RSVP-Message-Logging
    - CN=ACS-Event-Log-Level
    - CN=ACS-Identity-Name
    - CN=ACS-Max-Aggregate-Peak-Rate-Per-User
    - CN=ACS-Max-Duration-Per-Flow
    - CN=ACS-Max-No-Of-Account-Files
    - CN=ACS-Max-No-Of-Log-Files
    - CN=ACS-Max-Peak-Bandwidth
    - CN=ACS-Max-Peak-Bandwidth-Per-Flow
    - CN=ACS-Max-Size-Of-RSVP-Account-File
    - CN=ACS-Max-Size-Of-RSVP-Log-File
    - CN=ACS-Max-Token-Bucket-Per-Flow
    - CN=ACS-Max-Token-Rate-Per-Flow
    - CN=ACS-Maximum-SDU-Size
    - CN=ACS-Minimum-Delay-Variation
    - CN=ACS-Minimum-Latency
    - CN=ACS-Minimum-Policed-Size
    - CN=ACS-Non-Reserved-Max-SDU-Size
    - CN=ACS-Non-Reserved-Min-Policed-Size

fcmit.cc

也可以使用微软自带的 Active Directory Schema，但是默认没有注册该功能。可以通过运行 regsvr32 schmmgmt.dll 命令注册该 dll。

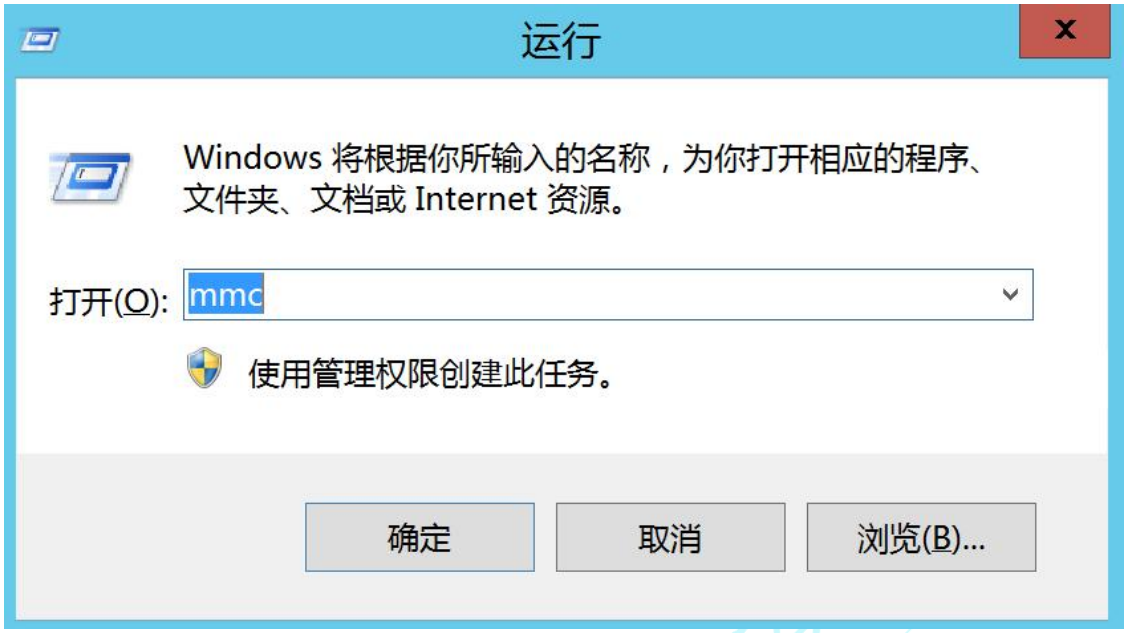
如图所示，运行 regsvr32 schmmgmt.dll 命令。



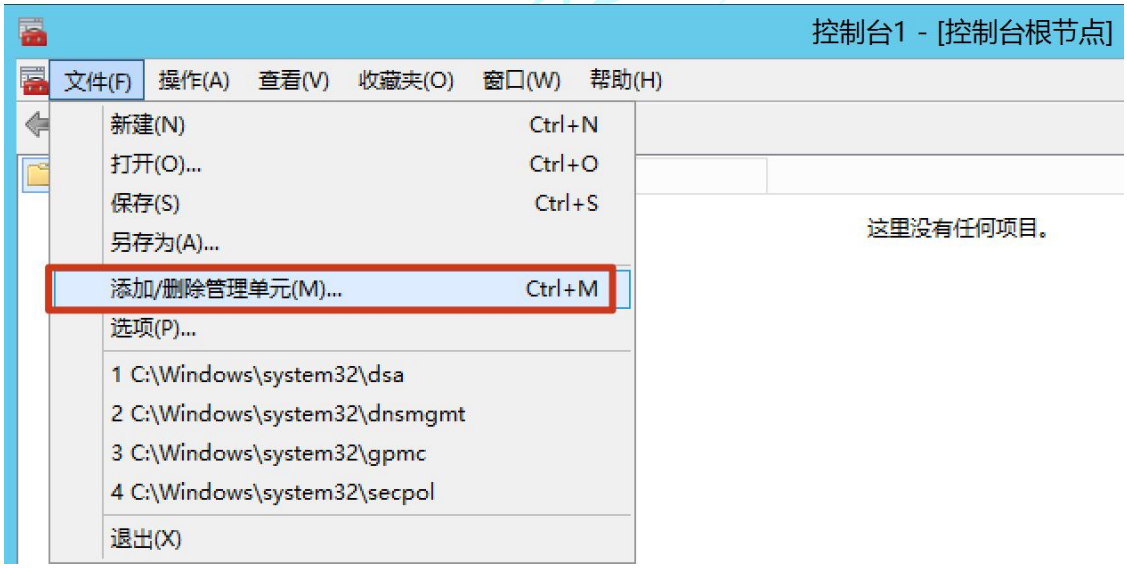
即可看到 schmmgmt.dll 注册成功，如图所示。

然后运行 mmc 打开控制台，如图所示。

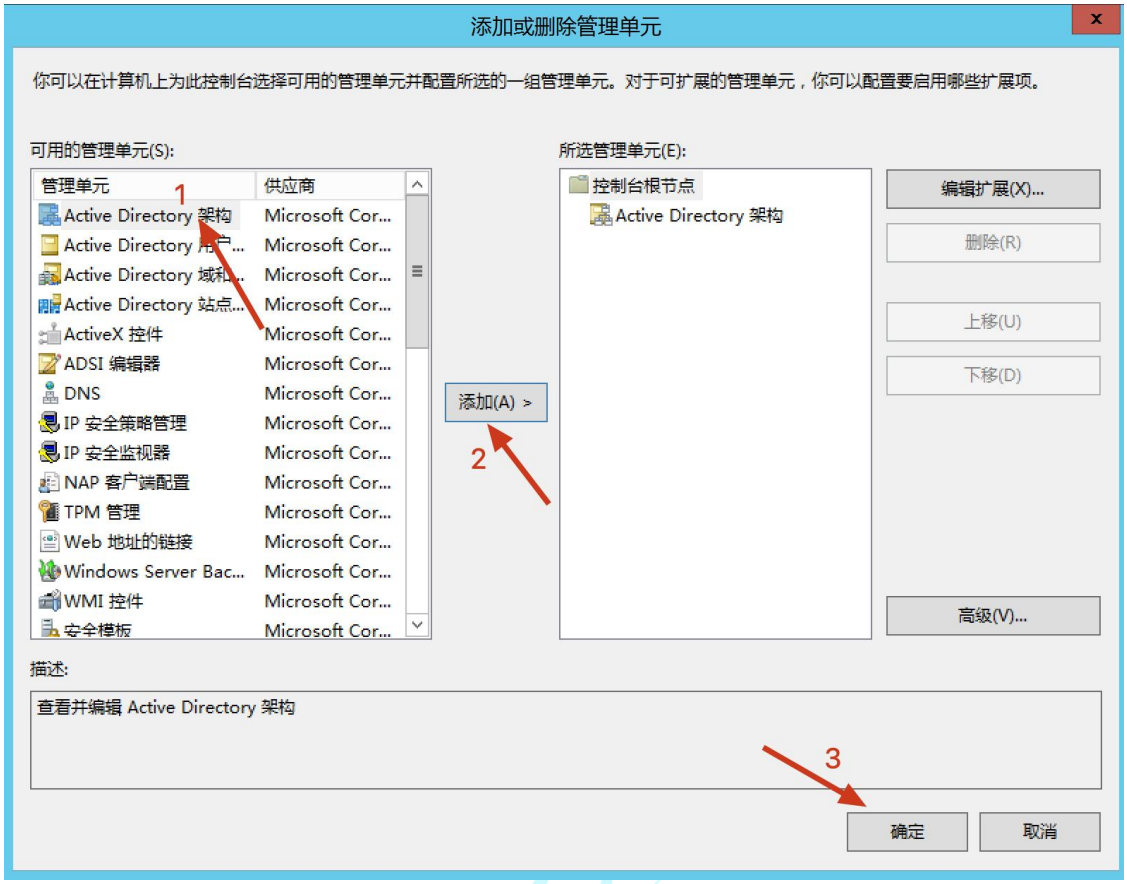
fcmit.cc



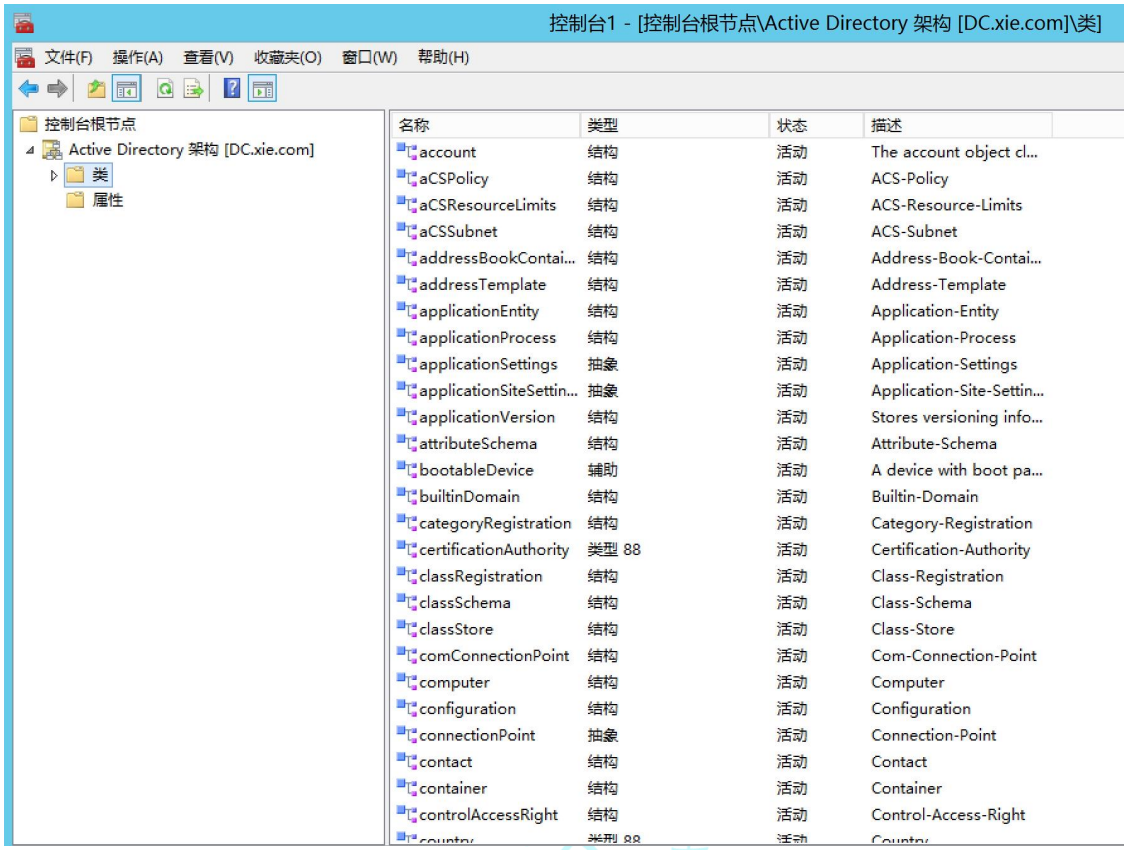
在弹出的控制台，点击文件——> 添加/删除管理单元(M)，如图所示。



然后点击 Active Directory 架构——>添加——>确定，如图所示：



即可看到活动目录中定义的所有类和属性了，如图所示：



2. LDAP 中的类和继承

在详细讲架构目录分区之前我们先来讲一下 LDAP 里面的类和继承，LDAP 里面的类和继承，跟开发里面的面向对象一样。

继承，也被称为派生，是指从现有对象类构建新对象类。新对象类称为其父对象的子类。所有结构对象类都直接或间接是抽象对象类 Top 的子类。在目录中表示的每个对象都属于 Top，因此每个条目都必须具有一个对象类属性。创建新类时，必须指定超类。如果不创建现有类的子类，则新类是 Top 的子类。新类可以从多个现有类继承强制属性和可选属性。但是，任何附加的类都必须由辅助类属性指定。如果将另一个属性添加到具有子类或辅助子类的类中，则在更新 Schema 缓存后，新属性将自动添加到子类中。这样说起来有点抽象，且看后文分析。

fcmit.cc

fcmit.cc

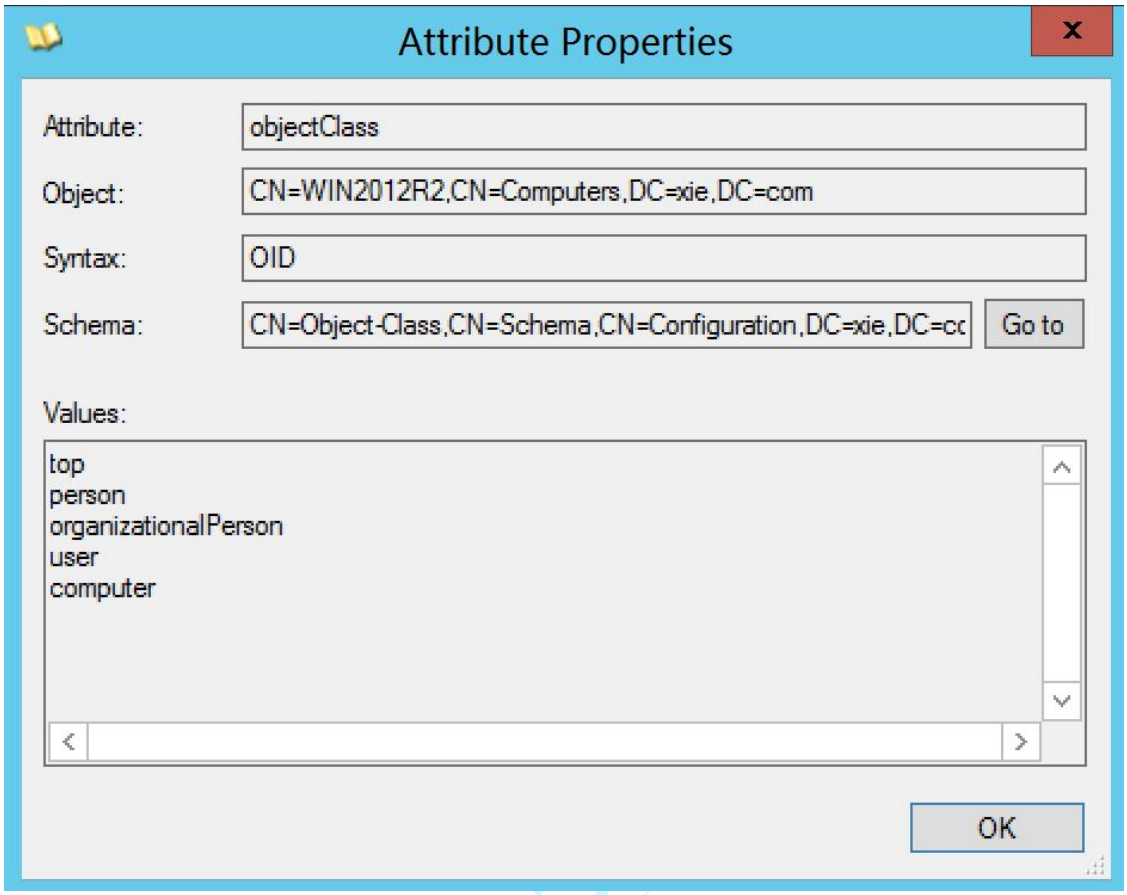
比如域内机器 CN=WIN2012R2,CN=Computers,DC=xie,DC=com 在 Active Directory 里面是一个条目对象，里面有众多属性描述该机器对象 WIN2012R2 的一些信息。

如图所示，查看机器 WIN2012R2 的属性。

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	WIN2012R2
codePage	Integer	1	0
countryCode	Integer	1	0
distinguishedName	DN	1	CN=WIN2012R2,CN=Computers,DC=xie,DC=com
dNSHostName	DirectoryString	1	Win2012R2.xie.com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	FALSE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:11:51
lastLogonTimestamp	Integer8	1	2021/10/26 22:10:25
localPolicyFlags	Integer	1	0
logonCount	Integer	1	9
mS-DS-CreatorSID	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-1105
msDS-SupportedEncryp...	Integer	1	28
name	DirectoryString	1	WIN2012R2
nTSecurityDescriptor	NTSecurityDescriptor	1	D:(OA;;WP;5f202010-79a5-11d0-9020-00c04fc2d4cf;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-21-1313979556
objectCategory	DN	1	CN=Computer,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	5	top;person;organizationalPerson;user;computer
objectGUID	OctetString	1	{05C32CBB-6440-4C9A-9301-499558F9B8ED}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-1106
operatingSystem	DirectoryString	1	Windows Server 2012 R2 Standard
operatingSystemVersion	DirectoryString	1	6.3 (9600)
primaryGroupID	Integer	1	515
pwdLastSet	Integer8	1	2021/10/16 11:50:59
sAMAccountName	DirectoryString	1	WIN2012R2$
sAMAccountType	Integer	1	805306369

而 WIN2012R2 条目对象有哪些属性是由他继承的类决定的。条目 CN=WIN2012R2,CN=Computers,DC=xie,DC=com 是类 Computer 的实例，在 objectClass 属性中可以看到。

如图所示，可以看到机器 WIN2012R2 继承自 Computer。

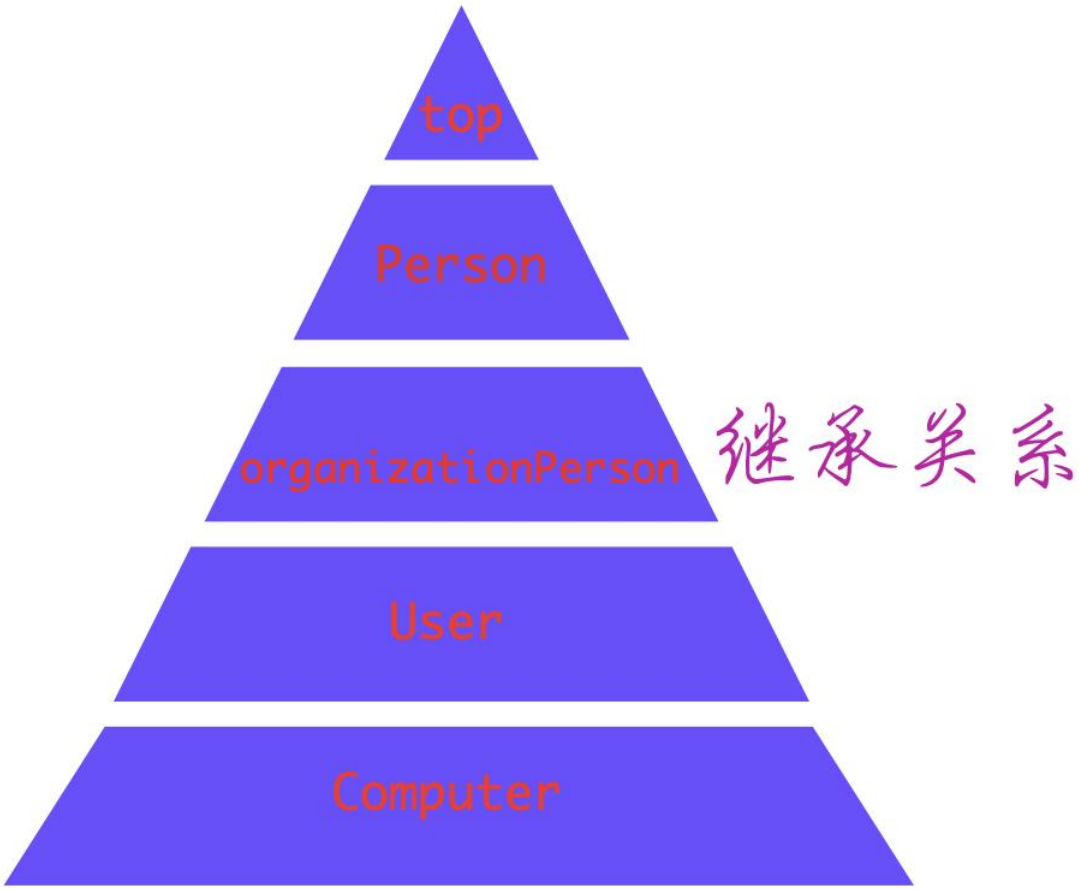


而类是可继承的，子类继承父类的所有属性，top 类是所有类的父类。所以我们看到 objectClass 里面的值除了 computer 之外，还有 top、person、organizationPerson、user。这是因为 computer 是 user 的子类，user 是 organizationPerson 的子类，organizationPerson 是 person 的子类，而 person 是 top 的子类。因此，computer 类可以继承 top、person、organizationPerson、user 的所有属性。

如图所示，是他们之间的继承关系。

fcmit.cc

fcmit.cc



那么，computer 类默认到底继承父类的哪些属性呢？这跟父类对象的以下几个属性相关：

- systemMustContain 和 MustContain 属性里的值是必选继承的属性
- systemMayContain 和 MayContain 属性里的值是可选继承的属性

我们就以 computer 类来看。该类继承于 user——>organizationalPerson——>person——>top。

那我们一个一个来看看。

如图查看 top 类的 systemMustContain 属性，可以看到 top 类的强制继承属性如下：

fcmit.cc

- objectClass
- objectCategory
- nTSecurityDescriptor
- instanceType

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Top
adminDisplayName	DirectoryString	1	Top
cn	DirectoryString	1	Top
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Top,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)
distinguishedName	DN	1	CN=Top,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	2.5.6.0
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	top
mayContain	OID	4	msSFU30PosixMemberOf;msDFSR-ComputerReferenceBL;msDFSR-MemberReferenceBL;msDS-ObjectReferenceBL
name	DirectoryString	1	Top
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	2
objectGUID	OctetString	1	{4C745911-D477-4C51-A9AC-9EA28AFD5765}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967AB7-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	114	msDS-ReplValueMetaDataExt;msDS-parentdistname;msds-memberTransitive;msds-memberOfTransitive;msDS-TDOEgressBL;msDS-TDOIngressBL;msDS-ValueTyp...
systemMustContain	OID	4	objectClass;objectCategory;nTSecurityDescriptor;instanceType
systemOnly	Boolean	1	TRUE
systemPossSuperiors	OID	1	lostAndFound
uSNChanged	Integer8	1	0x751
uSNCreated	Integer8	1	0x751
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

如图查看 person 类的 systemMustContain 属性，可以看到 person 类的强制继承属性为 cn

fcmit.cc

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Person
adminDisplayName	DirectoryString	1	Person
cn	DirectoryString	1	Person
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)
distinguishedName	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	2.5.6.6
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	person
mayContain	OID	1	attributeCertificateAttribute
name	DirectoryString	1	Person
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	0
objectGUID	OctetString	1	{8019BCF6-0A33-48A6-B2F6-092F628F572F}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967AA7-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	5	userPassword;telephoneNumber;sn;serialNumber;seeAlso
systemMustContain	OID	1	cn
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	2	organizationalUnit;container
uSNChanged	Integer8	1	0x6FA
uSNCreated	Integer8	1	0x6FA
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

如图查看 organizationalPerson 类的 systemMustContain 属性，可以看到 organizationalPerson 类没有强制属性。

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Organization
adminDisplayName	DirectoryString	1	Organization
cn	DirectoryString	1	Organization
defaultHidingValue	Boolean	1	FALSE
defaultObjectCategory	DN	1	CN=Organization,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)
distinguishedName	DN	1	CN=Organization,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	2.5.6.4
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	organization
name	DirectoryString	1	Organization
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	1
objectGUID	OctetString	1	{2B048D27-76D3-4F55-AD30-497C30421059}
rDNAttID	OID	1	o
schemaIDGUID	OctetString	1	{BF967AA3-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	20	x121Address;userPassword;telexNumber;teletexTerminalIdentifier;telephoneNumber;street;st;seeAlso;searchGuide;registere
systemMustContain	OID	1	o
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	3	locality;country;domainDNS
uSNChanged	Integer8	1	0x6F2
uSNCreated	Integer8	1	0x6F2
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

fcmit.cc

如图查看 user 类的 systemMustContain 属性，可以看到 user 类也没有强制继承属性。

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	User
adminDisplayName	DirectoryString	1	User
auxiliaryClass	OID	2	shadowAccount;posixAccount
cn	DirectoryString	1	User
defaultHidingValue	Boolean	1	FALSE
defaultObjectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPW
distinguishedName	DN	1	CN=User,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.5.9
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	user
mayContain	OID	21	msDS-SourceObjectDN;msSFU30NisDomain;msSFU30Name;x500uniqueIdentifier;userSMIMECertificate;userP
name	DirectoryString	1	User
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOC
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	1
objectGUID	OctetString	1	{E1ECD7D4-3A94-4848-B95B-2469917D6D5F}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967ABA-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	organizationalPerson
systemAuxiliaryClass	OID	3	msDS-CloudExtensions;securityPrincipal;mailRecipient
systemFlags	Integer	1	16
systemMayContain	OID	133	msDS-AuthNPolicySiloMembersBL;msDS-AssignedAuthNPolicySilo;msDS-AssignedAuthNPolicy;msDS-SyncServ
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	3	builtinDomain;organizationalUnit;domainDNS
uSNChanged	Integer8	1	0x756
uSNCreated	Integer8	1	0x756
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

因此通过继承，computer 类的强制继承属性有如下：

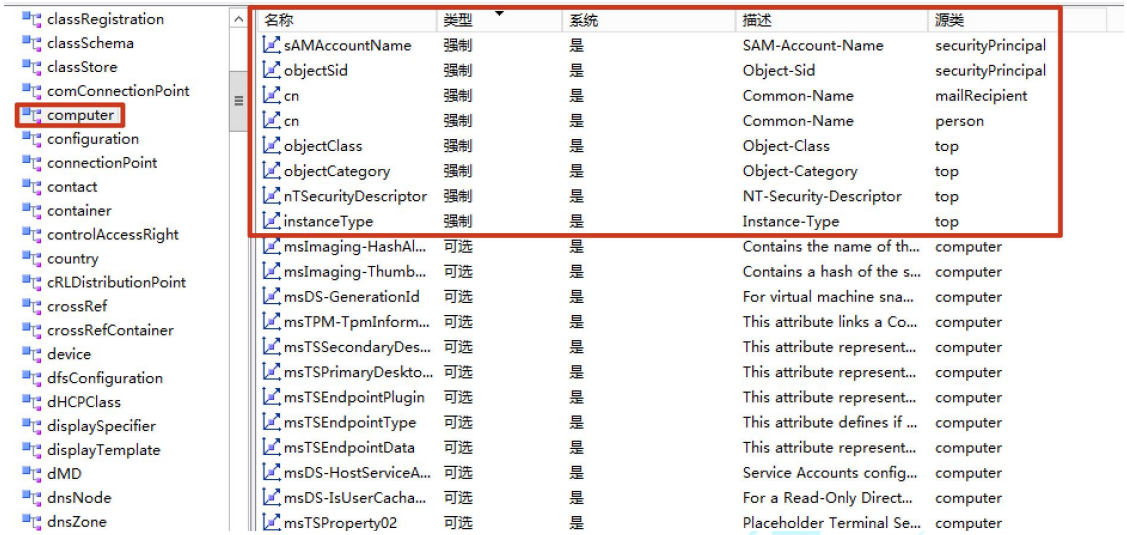
- objectClass
- objectCategory
- nTSecurityDescriptor
- instanceType
- cn

其他属性的话都是可选继承的。

我们通过 Active DirectorySchema 查看，就会看到强制继承的属性和可选继承的属性，以及源类是哪个类。

fcmit.cc

如图所示，可以看到 computer 类默认强制继承的有如下属性。



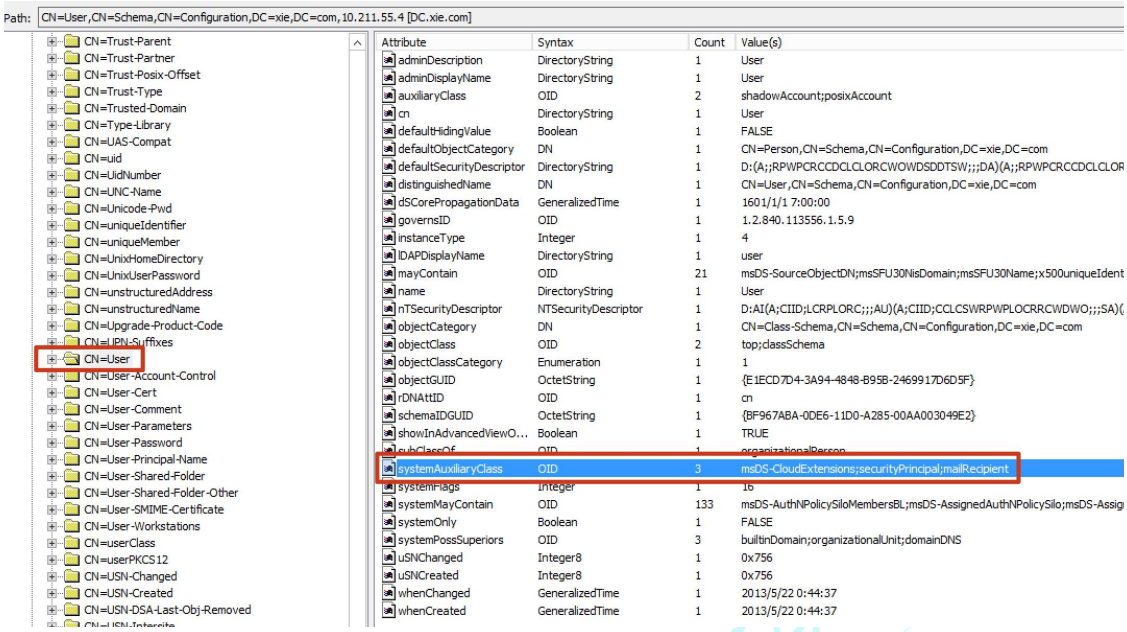
classRegistration
classSchema
classStore
comConnectionPoint
computer
configuration
connectionPoint
contact
container
controlAccessRight
country
cRLDistributionPoint
crossRef
crossRefContainer
device
dfsConfiguration
dHCPClass
displaySpecifier
displayTemplate
dMD
dnsNode
dnsZone

名称	类型	系统	描述	源类
sAMAccountName	强制	是	SAM-Account-Name	securityPrincipal
objectSid	强制	是	Object-Sid	securityPrincipal
cn	强制	是	Common-Name	mailRecipient
cn	强制	是	Common-Name	person
objectClass	强制	是	Object-Class	top
objectCategory	强制	是	Object-Category	top
nTSecurityDescriptor	强制	是	NT-Security-Descriptor	top
instanceType	强制	是	Instance-Type	top
msImaging-HashAl...	可选	是	Contains the name of th...	computer
msImaging-Thumb...	可选	是	Contains a hash of the s...	computer
msDS-GenerationId	可选	是	For virtual machine sna...	computer
msTPM-TpmInform...	可选	是	This attribute links a Co...	computer
msTSSecondaryDes...	可选	是	This attribute represent...	computer
msTSPrimaryDeskto...	可选	是	This attribute represent...	computer
msTSEndpointPlugin	可选	是	This attribute represent...	computer
msTSEndpointType	可选	是	This attribute defines if ...	computer
msTSEndpointData	可选	是	This attribute represent...	computer
msDS-HostServiceA...	可选	是	Service Accounts config...	computer
msDS-IsUserCacha...	可选	是	For a Read-Only Direct...	computer
msTSProperty02	可选	是	Placeholder Terminal Se...	computer

为什么会比我们上面查询的强制继承的属性还要多了来自于 securityPrincipal 源类的 sAMAccountName 属性和 objectSid 属性呢以及 mailRecipient 源类的 cn 属性呢?

如图所示，可以看到 user 类有个 systemAuxiliaryClass 属性(也就是辅助类)，而该辅助类属性的值也是需要继承的。因此 computer 类还需要继承来自辅助类 msDS-CloudExtensions、securityPrincipal 和 mailRecipient 的强制继承属性。

fcmit.cc



查询 msDS-CloudExtensions、securityPrincipal 和 mailRecipient 三个辅助类的强制继承属性。

如图，查看 msDS-CloudExtensions 类的 systemMustContain 属性，可以看到 msDS-CloudExtensions 类没有强制继承属性。

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	A collection of attributes used to house arbitrary cloud-relevant strings.
adminDisplayName	DirectoryString	1	ms-DS-Cloud-Extensions
cn	DirectoryString	1	ms-DS-Cloud-Extensions
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=ms-DS-Cloud-Extensions,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDI
distinguishedName	DN	1	CN=ms-DS-Cloud-Extensions,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.5.283
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	msDS-CloudExtensions
mayContain	OID	20	msDS-cloudExtensionAttribute20;msDS-cloudExtensionAttribute19;msDS-cloudExtensionA
name	DirectoryString	1	ms-DS-Cloud-Extensions
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDC
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	3
objectGUID	OctetString	1	{3C160244-D984-4E04-98E4-0DDED59F587C}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{641E87A4-8326-4771-BA2D-C706DF35E35A}
showInAdvancedViewOnly	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemOnly	Boolean	1	FALSE
uSNChanged	Integer8	1	0x7B9
uSNCreated	Integer8	1	0x7B9
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

如图，查看 securityPrincipal 类的 systemMustContain 属性，可以看到 securityPrincipal 类的强制继承属性为 sAMAccountName 和 objectSid。

fcmit.cc

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Security-Principal
adminDisplayName	DirectoryString	1	Security-Principal
cn	DirectoryString	1	Security-Principal
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Security-Principal,CN=Schema,CN=Configuration,DC=xie,DC=com
distinguishedName	DN	1	CN=Security-Principal,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.5.6
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	securityPrincipal
name	DirectoryString	1	Security-Principal
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CI
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	3
objectGUID	OctetString	1	{E6D751FE-E00C-40DA-9098-AC06C7EFE2F7}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967AB0-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewOnly	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	12	supplementalCredentials;sIDHistory;securityIdentifier;sAMAccountType;rid;toker
systemMustContain	OID	2	sAMAccountName;objectSid
systemOnly	Boolean	1	FALSE
uSNChanged	Integer8	1	0x732
uSNCreated	Integer8	1	0x732
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

如图，查看 mailRecipient 类的 systemMustContain 属性，可以看到 mailRecipient 类的强制继承属性为 cn。

fcmit.cc

fcmit.cc

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Mail-Recipient
adminDisplayName	DirectoryString	1	Mail-Recipient
cn	DirectoryString	1	Mail-Recipient
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Mail-Recipient,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOW
distinguishedName	DN	1	CN=Mail-Recipient,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.3.46
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	mailRecipient
mayContain	OID	9	msDS-GeoCoordinatesLongitude;msDS-GeoCoordinatesLatitude;msDS-GeoCoordinat
name	DirectoryString	1	Mail-Recipient
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	3
objectGUID	OctetString	1	{0462DE0C-61EB-400E-985E-36DF1BF21E7A}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967AA1-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewOnly	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	8	userCertificate;userCert;textEncodedORAddress;telephoneNumber;showInAddress
systemMustContain	OID	1	cn
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	1	container
uSNChanged	Integer8	1	0x656
uSNCreated	Integer8	1	0x656
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

综上所述，computer 类默认的强制继承属性有如下：

- 来自 top 类的 objectClass
- 来自 top 类的 objectCategory
- 来自 top 类的 nTSecurityDescriptor
- 来自 top 类的 instanceType
- 来自 person 类的 cn
- 来自 mailRecipient 类的 cn
- 来自 securityPrincipal 类的 objectSid
- 来自 securityPrincipal 类的 sAMAccountName

这正好与我们通过 Active DirectorySchema 查询的相符合，如图所示。

fcmit.cc

名称	类型	系统	描述	源类
sAMAccountName	强制	是	SAM-Account-Name	securityPrincipal
objectSid	强制	是	Object-Sid	securityPrincipal
cn	强制	是	Common-Name	mailRecipient
cn	强制	是	Common-Name	person
objectClass	强制	是	Object-Class	top
objectCategory	强制	是	Object-Category	top
nTSecurityDescriptor	强制	是	NT-Security-Descriptor	top
instanceType	强制	是	Instance-Type	top

3. Schema Directory Partition 中的类

活动目录中所有的类都在 Schema Directory Partition 内定义了，所有类都是 classSchema 的实例。

如图所示，是 class-Schema 的属性。

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Class-Schema
adminDisplayName	DirectoryString	1	Class-Schema
cn	DirectoryString	1	Class-Schema
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:S:
distinguishedName	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.3.13
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	classSchema
name	DirectoryString	1	Class-Schema
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	1
objectGUID	OctetString	1	{A5F7BF25-B124-4E86-AC99-8967578D44A0}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967A83-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	134217744
systemMayContain	OID	18	systemPossSuperiors;systemOnly;systemMustContain;systemMayContain;systemAuxiliaryClass;schemaFlagsEx;rDNAttID;possSup
systemMustContain	OID	6	subClassOf;schemaIDGUID;objectClassCategory;governsID;defaultObjectCategory;cn
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	1	dMD
uSNChanged	Integer8	1	0x5E3
uSNCreated	Integer8	1	0x5E3
whenChanged	GeneralizedTime	1	2013/5/22 0:44:36
whenCreated	GeneralizedTime	1	2013/5/22 0:44:36

活动目录中的类有三种类型，分别如下：

- 结构类(Structural)：结构类规定了对象实例的基本属性，每个条目属于且仅属于一个结构对象类。前面说过域内每个条目都是类的实例，这个类必须

是结构类，结构类是唯一可以在目录中有实例的类，结构类可以派生于抽象类或其他结构类，可以在结构类定义中包含任意数量的辅助类。

- 抽象类(Abstract)：抽象类是用于导生新结构类的模板，他没有实例，只能充当结构类或者抽象类的父类。一个新的抽象类可以从一个现有的抽象类中派生出来，它只为子类提供属性，将对象属性中公共的部分组织在一起。跟面对对象里面的抽象方法一样，比如说 top 类。

- 辅助类(Auxiliary)：辅助类包含一个属性列表，在结构类或抽象类的定义中添加一个辅助类会将辅助类属性添加到实例中。虽然不能实例化辅助类，但是可以从现有的辅助类或抽象类派生出新的辅助类。例如，Security-Principal 类是一个辅助类，它从名为 Top 的父抽象类中派生。虽然不能实例化辅助类，但可以创建一个结构类 User 的对象，该用户将 Security-Principal 类作为辅助类。因此，该用户对象将拥有辅助类 Security-Principal 的属性，Security-Principal 类的属性可以帮助系统将用户对象识别为安全帐户。辅助类规定了对象实体的扩展属性。虽然每个条目只属于一个结构对象类，但可以同时属于多个辅助对象类。

注：其实还有个 88 类，88 类不属于上述任何一个类别。88 类可以用作抽象类、结构类或辅助类，88 类的类可以继承自所有类。

条目的 objectClassCategory 属性的 count 为 1 说明他是一个结构类，为 2 说明他是一个抽象类，为 3 说明他是一个辅助类。

如图所示，Computer 类的 objectClassCategory 的属性为 1，说明他是一个结构类。而 Computer 类的实例就是域内的机器。

fcmit.cc

fcmit.cc

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Computer
adminDisplayName	DirectoryString	1	Computer
auxiliaryClass	OID	1	ipHost
cn	DirectoryString	1	Computer
defaultHidingValue	Boolean	1	FALSE
defaultObjectCategory	DN	1	CN=Computer,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;AO)(A;;RPWPCRCCDCLCLORCW
distinguishedName	DN	1	CN=Computer,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.3.30
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	computer
mayContain	OID	4	msSFU30Name;nisMapName;msSFU30NisDomain;msSFU30Aliases
name	DirectoryString	1	Computer
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	1
objectGUID	OctetString	1	{4751B44D-C567-47C2-9BDE-6DDB4CC33256}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967A86-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	user
systemFlags	Integer	1	16
systemMayContain	OID	51	msImaging-HashAlgorithm;msImaging-ThumbprintHash;msDS-GenerationId;msTPM-TpmInformationForComputer;msTSSecondaryD
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	3	container;organizationalUnit;domainDNS
uSNChanged	Integer8	1	0x5E9
uSNCreated	Integer8	1	0x5E9
whenChanged	GeneralizedTime	1	2013/5/22 0:44:36
whenCreated	GeneralizedTime	1	2013/5/22 0:44:36

如图所示，Top 类的 objectClassCategory 的属性为 2，说明他是一个抽象类。

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Top
adminDisplayName	DirectoryString	1	Top
cn	DirectoryString	1	Top
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Top,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)
distinguishedName	DN	1	CN=Top,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	2.5.6.0
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	top
mayContain	OID	4	msSFU30PosixMemberOf;msDFSR-ComputerReferenceBL;msDFSR-MemberReferenceBL;msDS-ObjectReferenceBL
name	DirectoryString	1	Top
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	2
objectGUID	OctetString	1	{4C745911-D477-4C51-A9AC-9EA28AFD5765}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967AB7-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	114	msDS-ReplValueMetaDataExt;msDS-parentdistname;msds-memberTransitive;msds-memberOfTransitive;msDS-TDOEgressBL;msDS-T
systemMustContain	OID	4	objectClass;objectCategory;nTSecurityDescriptor;instanceType
systemOnly	Boolean	1	TRUE
systemPossSuperiors	OID	1	lostAndFound
uSNChanged	Integer8	1	0x751
uSNCreated	Integer8	1	0x751
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

如图所示，Security-Principal 类的 objectClassCategory 的属性为 3，说明他是一个辅助类。

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Security-Principal
adminDisplayName	DirectoryString	1	Security-Principal
cn	DirectoryString	1	Security-Principal
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Security-Principal,CN=Schema,CN=Configuration,DC=xie,DC=com
distinguishedName	DN	1	CN=Security-Principal,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.5.6
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	securityPrincipal
name	DirectoryString	1	Security-Principal
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	3
objectGUID	OctetString	1	{E6D751FE-E00C-40DA-9098-AC06C7EFE2F7}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967AB0-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	16
systemMayContain	OID	12	supplementalCredentials;sIDHistory;securityIdentifier;sAMAccountType;rid;tokenGroupsNoGCAcceptable;tokenGroupsGlobalAndU
systemMustContain	OID	2	sAMAccountName;objectSid
systemOnly	Boolean	1	FALSE
uSNChanged	Integer8	1	0x732
uSNCreated	Integer8	1	0x732
whenChanged	GeneralizedTime	1	2013/5/22 0:44:37
whenCreated	GeneralizedTime	1	2013/5/22 0:44:37

4. Schema Directory Partition 中的属性

Schema Directory Partition 中除了定义了 Active Directory 中使用的类之外，还定义了 Active Directory 中使用的属性。每个属性在 Schema Directory Partition 内也是一个条目，是类 Attribute-Schema 的实例。

如图所示，查看 Attribute-Schema 的属性。

fcmit.cc

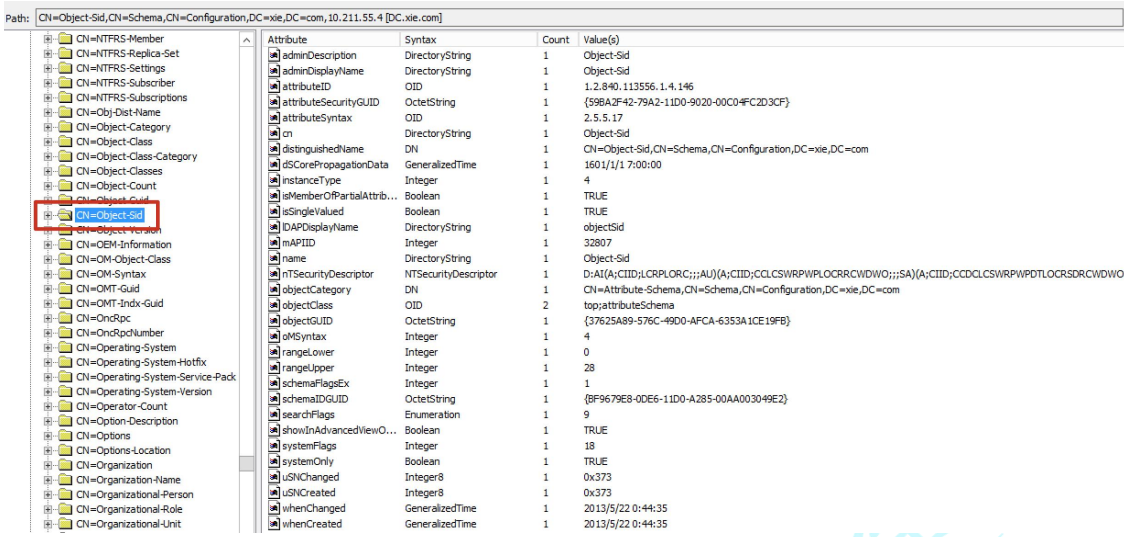
Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Attribute-Schema
adminDisplayName	DirectoryString	1	Attribute-Schema
cn	DirectoryString	1	Attribute-Schema
defaultHidingValue	Boolean	1	TRUE
defaultObjectCategory	DN	1	CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
defaultSecurityDescriptor	DirectoryString	1	D:S:
distinguishedName	DN	1	CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
governsID	OID	1	1.2.840.113556.1.3.14
instanceType	Integer	1	4
lDAPDisplayName	DirectoryString	1	attributeSchema
name	DirectoryString	1	Attribute-Schema
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
objectCategory	DN	1	CN=Class-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;classSchema
objectClassCategory	Enumeration	1	1
objectGUID	OctetString	1	{C1C44649-E964-4238-BFDD-512420CE1264}
rDNAttID	OID	1	cn
schemaIDGUID	OctetString	1	{BF967A80-0DE6-11D0-A285-00AA003049E2}
showInAdvancedViewO...	Boolean	1	TRUE
subClassOf	OID	1	top
systemFlags	Integer	1	134217744
systemMayContain	OID	16	systemOnly;searchFlags;schemaFlagsEx;rangeUpper;rangeLower;oMObjectClass;msDs-Schema-Extensions;msDS-IntId;mAP
systemMustContain	OID	7	schemaIDGUID;oMSyntax;lDAPDisplayName;isSingleValued;cn;attributeSyntax;attributeID
systemOnly	Boolean	1	FALSE
systemPossSuperiors	OID	1	dMD
uSNChanged	Integer8	1	0x5DA
uSNCreated	Integer8	1	0x5DA
whenChanged	GeneralizedTime	1	2013/5/22 0:44:36
whenCreated	GeneralizedTime	1	2013/5/22 0:44:36

在域内的所有属性必须在这里定义，而这里的条目，最主要的是限定了属性的语法定义，其实就是数据类型。属性的值的数据类型由属性条目的 attributeSyntax 属性和 oMSyntax 属性决定。这听起来有点绕口，有点像先有鸡还是先有蛋的感觉，我们往下看。

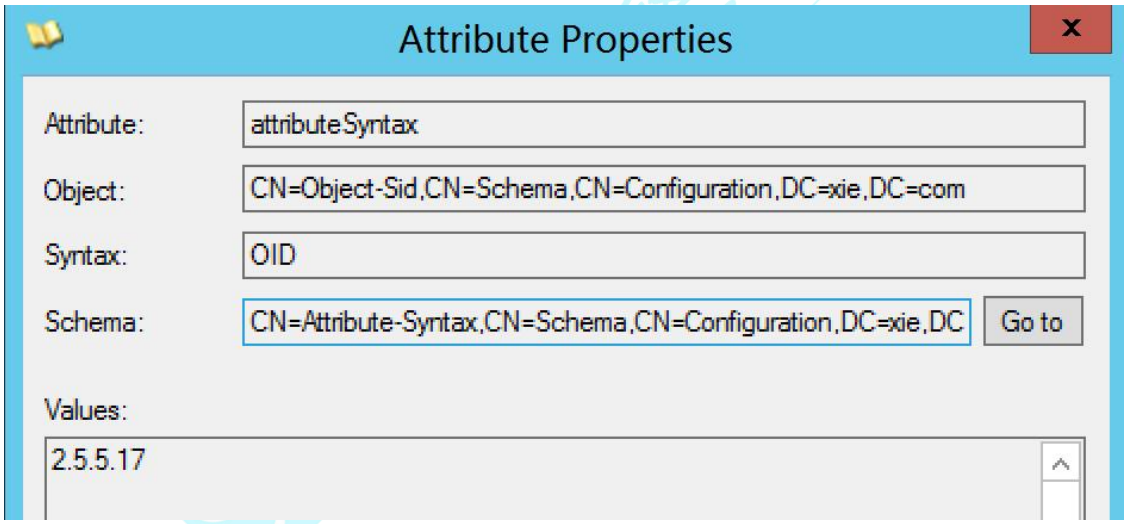
如图所示，以属性 Object-Sid (CN=Object-Sid,CN=Schema,CN=Configuration,DC=xie,DC=com)为例。

fcmit.cc

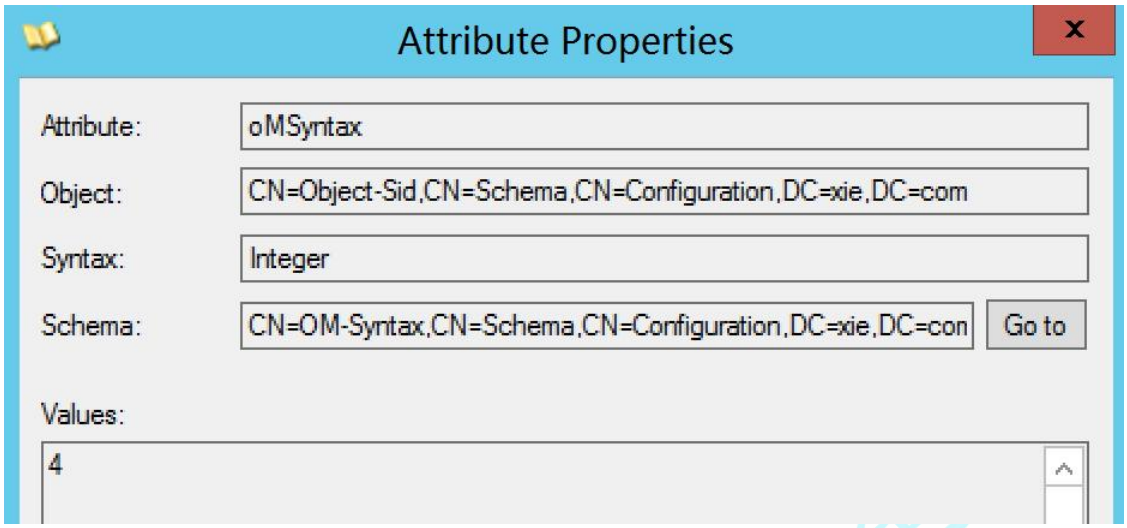
fcmit.cc



他的 attributeSyntax 属性是 2.5.5.17，如图所示。



oMSyntax 属性是 4，如图所示。



如图所示，通过查表可以得知 Object-Sid 属性的值是一个安全辨识符(SID)，因此 Object-Sid 属性的值的数据类型为 SID。

String(Sid)	2.5.5.17	4	\x550511	Security identifier (SID)

如图所示，查看 hack 对象的 objectsid 属性的值的数据类型，可以看到确实是 sid。

fcmit.cc

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	hack
codePage	Integer	1	0
countryCode	Integer	1	0
distinguishedName	DN	1	CN=hack,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
instanceType	Integer	1	4
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:25
lastLogonTimestamp	Integer8	1	2021/11/6 9:56:10
logonCount	Integer	1	11
name	DirectoryString	1	hack
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;;RS)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;;RS)(OA;;
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{908A4F43-E2C4-4994-8728-B1C42507D357}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-1105
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:37:28
sAMAccountName	DirectoryString	1	hack
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x5065
uSNCreated	Integer8	1	0x31E5
whenChanged	GeneralizedTime	1	2021/11/6 9:56:10
whenCreated	GeneralizedTime	1	2021/10/16 11:37:28

而这里的 Object-Sid 属性条目的 attributeSyntax 属性和 oMSyntax 属性又可以在 Schema Directory Partition 中找到定义。而 attributeSyntax 属性条目和 oMSyntax 属性条目自身又是通过他们自身的 attributeSyntax 属性和 oMSyntax 属性来定义数据类型的。

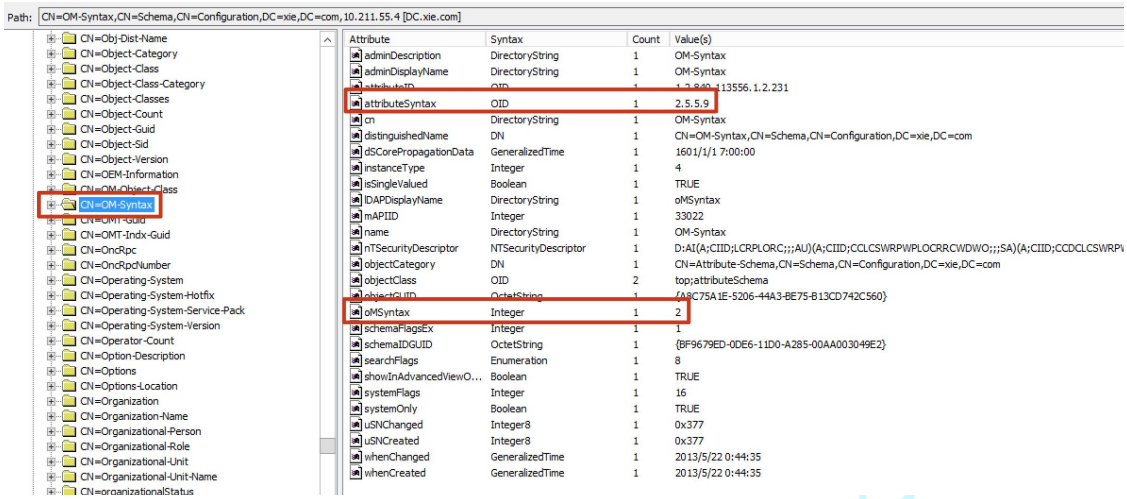
如图所示，查看条目 attribute-Syntax 的 attributeSyntax 属性和 oMSyntax 属性。

Path: CN=Attribute-Syntax,CN=Schema,CN=Configuration,DC=xie,DC=com,10.211.55.4 [DC.xie.com]

CN=Attribute-ID
CN=Attribute-Schema
CN=Attribute-SecurityGUID
CN=Attribute-Syntax
CN=Attribute-Types
CN=attributeCertificateAttribute
CN=audio
CN=Auditing-Policy
CN=Authentication-Options
CN=Authority-Revocation-List
CN=Auxiliary-Class
CN=Bad-Password-Time
CN=Bad-Pwd-Count
CN=Birth-Location
CN=BootableDevice
CN=BootFile
CN=BootParameter
CN=Bridgehead-Server-List-BL
CN=Bridgehead-Transport-List
CN=buildingName
CN=Builtin-Creation-Time
CN=Builtin-Domain
CN=Builtin-Modified-Count
CN=Business-Category
CN=Bytes-Per-Minute
CN=CA-Certificate
CN=CA-Certificate-DN
CN=CA-Connect
CN=CA-Usages

Attribute	Syntax	Count	Value(s)
adminDescription	DirectoryString	1	Attribute-Syntax
adminDisplayName	DirectoryString	1	Attribute-Syntax
attributeID	OID	1	1.2.840.113556.1.2.32
attributeSyntax	OID	1	2.5.5.2
cn	DirectoryString	1	Attribute-Syntax
distinguishedName	DN	1	CN=Attribute-Syntax,CN=Schema,CN=Configuration,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	1	1601/1/1 7:00:00
instanceType	Integer	1	4
isSingleValued	Boolean	1	TRUE
lDAPDisplayName	DirectoryString	1	attributeSyntax
name	DirectoryString	1	Attribute-Syntax
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;CIID;LCRPLORC;;;AU)(A;CIID;CCLCSWRPWPLOCRRCWDWO;;;SA)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;
objectCategory	DN	1	CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;attributeSchema
objectGUID	OctetString	1	{D0E15BBE-8DE4-4A2E-A2C7-4C6D5E3BA4F6}
oMSyntax	Integer	1	6
schemaFlagsEx	Integer	1	1
schemaIDGUID	OctetString	1	{BF967925-0DE6-11D0-A285-00AA003049E2}
searchFlags	Enumeration	1	8
showInAdvancedViewO...	Boolean	1	TRUE
systemFlags	Integer	1	16
systemOnly	Boolean	1	TRUE
uSNChanged	Integer8	1	0x52
uSNCreated	Integer8	1	0x52
whenChanged	GeneralizedTime	1	2013/5/22 0:44:33
whenCreated	GeneralizedTime	1	2013/5/22 0:44:33

如图所示，查看条目 oM-Syntax 的 attributeSyntax 属性和 oMSyntax 属性。



Application Directory Partition

从 Windows Server 2003 开始，微软引入了应用程序目录分区(Application Directory Partition)，其允许用户自定义分区来扩展目录分区。它提供了控制复制范围的能力，并允许以更适合动态数据的方式放置副本。应用程序目录分区会被复制到林中特定的域控中，而不是所有的域控中。管理员可以创建应用程序目录分区，以将数据存储在他们选择的特定域控制器上。

Application Directory Partitions 主要有以下特点:

- 如果用户想要定义一个分区，可以通过 Application Directory Partitions。虽然微软也预置了两个 Application Directory Partitions，但是 Application Directory Partitions 的设计更多是为了让用户可以自定义自己的数据。设计 Application Partitions 最大的用途就是，让用户自己来定义分区。

- Application Directory Partitions 可以存储动态对象。动态对象是具有生存时间(TTL）值的对象，该值确定它们在被 Active Directory 自动删除之前将存在多长时间。也就说 Application Directory Partitions 可以给数据设置个 TTL，时间一到，Active Directory 就删除该数据。

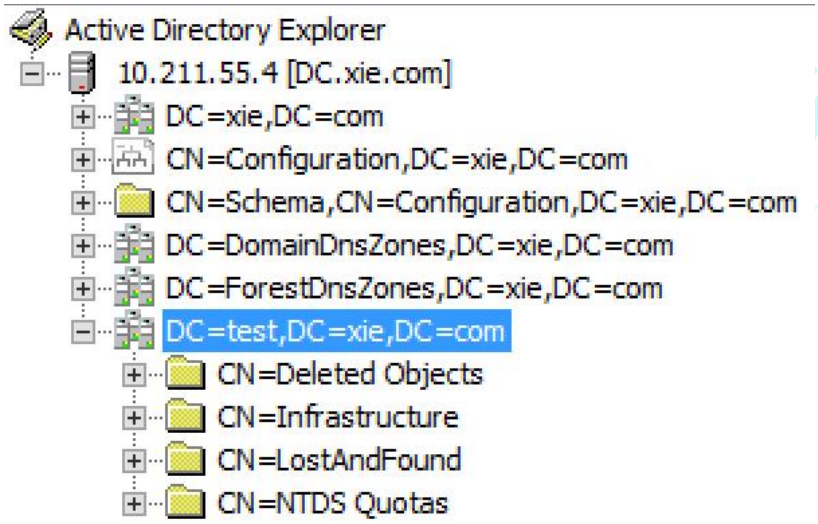
fcmit.cc

fcmit.cc

如图所示，通过 ntdsutil 创建应用程序目录分区 DC=test,DC=xie,DC=com。

```
C:\Users\Administrator>ntdsutil
ntdsutil: partition management
partition management: create nc "dc=test,dc=xie,dc=com" dc.xie.com
adding object dc=test,dc=xie,dc=com
partition management:
```

如图所示，使用 ADExplorer 连接活动目录查看应用程序目录分区，可以看到应用程序目录分区 DC=test,DC=xie,DC=com。



条目属性分析

我们下面具体分析一下条目的一些比较重要的属性。首先看看条目属性的四列分别代表着什么?

- Attribute 代表条目的属性。
- Sytnta 代表条目属性的值的数据类型。
- Count 代表条目属性的值的个数。

fcmit.cc

- Value(s)代表条目属性具体的值。

如图所示，我们就拿默认的域管理员administrator(CN=Administrator,CN=Users,DC=xie,DC=com)为例。

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,DC=xie,DC=com;CN=Enterprise Admins,CN=Users,DC=xie,DC=c...
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf9...
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

1. adminCount

adminCount 属性代表该条目是否是受保护组的对象，如果其值是 1 的话，就是受保护的；如果其值是 0 的话，就是不受保护的。

如图所示，这里我们可以看到 administrator 的 adminCount 属性为 1，说明他是受保护组的对象。具体关于受保护组的对象，我们会在后面的文章中讲解。

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,DC=xie,DC=com;CN=Enterprise Admins,CN=Users,DC=xie,DC=c...
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf9...
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

2. badPasswordTime

badPasswordTime 属性的话很好理解，就是该用户最后一次输错密码的时间。

如图所示，这里我们可以看到 administrator 的 badPasswordTime 属性为 2021/10/16 11:29:34。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f01
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

3. badPwdCount

badPwdCount 属性的话很好理解，就是该用户输错密码的次数。其实可以根据这一属性，来查看哪些用户可能被爆破。

如图所示，administrator 的 badPwdCount 为 0，说明没输错过密码。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,DC=xie,DC=c
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(O
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

4. cn

cn 属性的话就是条目的通用名称，不具有唯一性。默认是对象的 DN 的最后一级子节点的名称。

如图所示，administrator 的 CN 就是为 administrator。

fcmit.cc

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e05
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

5. description

description 属性的话很好理解，就是对该条目的一个描述。

如图所示，域管理员 administrator 的描述为“管理计算机(域)的内置帐户”。

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,DC=xie,DC=cor
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

6. distinguishedName

distinguishedName 属性的话就是该条目的可分辨名称 DN，每个对象拥有的 distinguishedName 属性的值都是唯一的。

如图所示，administrator 用户的 DN 为 CN=Administrator,CN=Users,DC=xie,DC=com。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 25
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=U
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

7. lastLogon

lastLogon 属性代表该用户最后的登录时间。

如图所示，可以看到 administrator 用户最后一次登录时间为 2021/10/26 22:12:01。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 25
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Us
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

8. logonCount

logonCount 属性代表该用户的登录次数。

如图所示，代表 administrator 用户登录过 20 次。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,D
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

9. memberOf

memberOf 属性代表该用户所属的组。

如图所示，可以看到 administrator 所属的组很多，有 Group Policy Creator Owners 、Domain Admins、Enterprise Admins、Schema Admins 和 Administrators。

fcmit.cc

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,DC=xie,DC=com;CN=Enterprise Admins,CN=Users,DC=xie,DC=c...
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;bf9...
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

10. member

member 属性与 memberOf 属性相反，意思是该组内有哪些用户。但是由于 administrator 不是组，因此没有该属性。

我们可以看 Domain Admins 组的 member 属性，如图所示，可以看到有 administrator 用户。

Attribute	Syntax	Count	Value(s)
adminCount	Integer	1	1
cn	DirectoryString	1	Domain Admins
description	DirectoryString	1	指定的域管理员
distinguishedName	DN	1	CN=Domain Admins,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	3	2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/1 7:04:16
groupType	Integer	1	-2147483646
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
member	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
memberOf	DN	2	CN=Denied RODC Password Replication Group,CN=Users,DC=xie,DC=com;CN=Administrators,CN=Builtin,DC=xie,DC=com
name	DirectoryString	1	Domain Admins
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;;RP;4c164200-20c0-11d0-a
objectCategory	DN	1	CN=Group,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	2	top;group
objectGUID	OctetString	1	{67C0B211-BF6B-4214-9028-AA1B86417849}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-512
sAMAccountName	DirectoryString	1	Domain Admins
sAMAccountType	Integer	1	268435456
uSNChanged	Integer8	1	0x31F1
uSNCreated	Integer8	1	0x3039
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:26:55

fcmit.cc

11. name

name 属性就是条目的名字。如图所示，administrator 用户的 name 属性的值就为 administrator。

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,D
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

12. nTSecurityDescriptor

nTSecurityDescriptor 属性的值是这个条目的 ACL。

如图所示，可以看到 nTSecurityDescriptor 属性的值的类型为 NTSecurityDescriptor，其值就是该条目的 ACL，是用 SDDL 语言描述的。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f01
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

其实与用户 ACL 相关的还有一个属性，就是 defaultSecurityDescriptor 属性。defaultSecurityDescriptor 属性是实例默认的 ACL。但是在 administrator 条目这里没看到这个属性，我们可以在 Schema Directory Partition 里面查询一下即可看到 User 类还有一个 defaultSecurityDescriptor 属性。也就是说，当 User 类在实例化的时候，没有指定 ACL 的话，则 nTSecurityDescriptor 属性的值就为 CN=User,CN=Schema,CN=Configuration,DC=xie,DC=com 条目的 defaultSecurityDescriptor 属性的值。如果在实例化的过程中，指定了 ACL 的话，则 nTSecurityDescriptor 属性的值就为指定的 ACL。

13. objectClass

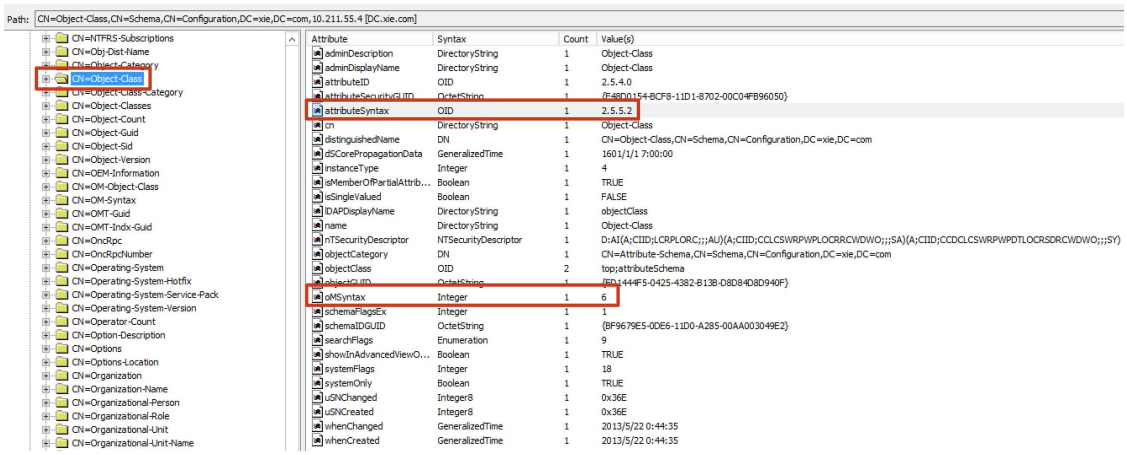
objectClass 属性代表该实例对象继承的类有哪些。

fcmit.cc

如图所示，是 administrator 对象的 objectClass 属性，OID 代表其值数据类型为 OID，4 代表其值有 4 个，而 top;person;organizationalPerson;user 就是其属性的值。

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=User
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f0
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

而 objectClass 这个属性在 Schema Directory Partition 里面就有定义，如图所示：



如图所示，通过定义的语法查表可以得知其值的数据类型为 String(Object-Identifier)，也就是我们看到的 OID。

String(Object-Identifier)	2.5.5.2	6	\x550502	The object identifier

14. objectGUID

objectGUID 属性就是对象的 GUID 属性的值。

如图所示，可以看到 administrator 的 objectGUID 属性为{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Adm
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45b
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

15. objectSid

objectSid 属性代表该条目 SID 的值，域管理员 administrator 的 SID 默认为域 SID+500。

如图所示，可以看到 administrator 的 objectSid 属性 S-1-5-21-域 SID-500。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 2
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,C
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b0
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/10/16 11:29:51
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x31F3
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/10/16 11:42:05
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

16. pwdLastSet

pwdLastSet 属性的值就是该用户最后一次修改密码的时间。

如图所示，可以看到 administrator 的最后一次修改密码时间为 2021/11/8 15:11:28。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=Users,I
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/11/8 15:11:28
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x50BD
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/11/8 15:11:28
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

17. whenChanged

whenChanged 属性就是代表该对象最近一次被改动的时间，比如最近一次密码被修改的时间。

如图所示，可以看到 administrator 的 whenChanged 属性为 2021/11/8 15:11:28。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,CN=
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-a
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/11/8 15:11:28
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x50BD
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/11/8 15:11:28
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

18. whenCreated

whenCreated 属性就是代表该对象被创建的时间。

如图所示，可以看到 administrator 的 whenCreated 属性为 2021/10/16 11:24:44。

fcmit.cc

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	2021/10/16 11:29:34
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	管理计算机(域)的内置帐户
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=xie,DC=com
dSCorePropagationData	GeneralizedTime	4	2021/10/16 11:42:05;2021/10/16 11:42:05;2021/10/16 11:26:55;1601/1/2 1:12:16
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2021/10/26 22:12:01
lastLogonTimestamp	Integer8	1	2021/10/16 11:29:51
logonCount	Integer	1	20
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 25
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=xie,DC=com;CN=Domain Admins,Cl
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=xie,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{7B73B1AA-7830-48F7-9106-0BE3FA003BCE}
objectSid	Sid	1	S-1-5-21-1313979556-3624129433-4055459191-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2021/11/8 15:11:28
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512
uSNChanged	Integer8	1	0x50BD
uSNCreated	Integer8	1	0x2004
whenChanged	GeneralizedTime	1	2021/11/8 15:11:28
whenCreated	GeneralizedTime	1	2021/10/16 11:24:44

非常感谢您读到现在，由于作者的水平有限，编写时间仓促，文章中难免会出现一些错误或者描述不准确的地方，恳请各位师傅们批评指正。如果你想一起学习 AD 域安全攻防的话，可以加入下面的知识星球一起学习交流。

fcmit.cc

fcmit.cc

谢公子

我加入了这个星球，邀你一起学习

域渗透攻防指南

星主：谢公子

60+	30+	306
成员数量	内容数量	运营天数

书籍📚《域渗透攻防指南》官方知识星球。星球讨论与微软AD域相关攻防技术，大家互相交流互相学习，共同进步成长。

现价：¥199

微信扫码加入星球

知识星球

谢公子学安全

fcmit.cc

参考：

https://docs.microsoft.com/en-us/windows/win32/adschema/active-directory-schema-site

https://docs.microsoft.com/en-us/windows/win32/ad/naming-contexts-and-partitions

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/f0f1e85a-3ac2-466a-87bf-2a8a1d18e4b8

https://docs.microsoft.com/en-us/windows/win32/adschema/classes

https://docs.microsoft.com/en-us/windows/win32/adschema/attributes

https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-server-2003/cc773309(v=ws.10)