Active Directory 教程

Active Directory 教程

活动目录（Active Directory）是面向 Windows Standard Server、Windows Enterprise Server 以及 Windows Datacenter Server 的目录服务。Microsoft Active Directory 服务是 Windows 平台的核心组件，它为用户管理网络环境各个组成要素的标识和关系提供了一种有力的手段。在本期技术教程中，我们将介绍 Active Directory 在虚拟化方面的使用技巧。

使用 Active Directory 追踪 VM

随着很多企业部署越来越多的虚拟化平台，如何区分物理服务器和虚拟服务器也变得越来越难。有一种标识服务器对象（无论是虚拟环境还是物理环境）的方法是使用每一台计算机对象 Active Directory 中的 Description 属性。那么具体该如何操作呢？

- **使用 Active Directory 标识和追踪虚拟机**
- **使用脚本进行 Description 查询**
- **添加自定义 Active Directory 计算对象属性定位虚拟机**

Active Directory 快照

Windows Server 2008 允许管理员对 Active Directory 进行快照。在作出任何主要的 Active Directory 修改之前创建快照，以便在需要的时候使用副本数据库恢复。如何使用 Windows Server 2008 里的 Active Directory 快照？

- **使用 Windows Server 2008 里的 Active Directory 快照**

Active Directory 实用技巧

如何创建一个 Windows AD 组？如何在 vSpere 中使用这个组控制虚拟基础架构的管理人员？在 Active Directory 环境里，如何诊断和解决登录性能缓慢的难题？taskpad 是什么？对 Active Directory 数据库有何作用？

- **使用 Windows Active Directory 组控制 vSpere 管理权限**
- **解决在 Active Directory 环境里 Windows 登录性能问题**
- **在 Active Directory 管理里创建 taskpad view**

使用 Active Directory 标识和追踪虚拟机

在本系列文章的第一篇文章中，TechTarget 中国的虚拟化专家 Chris Wolf 将介绍如何使用 Active Directory 跟踪虚拟化资源。

随着很多企业部署越来越多的虚拟化平台，如何区分物理服务器和虚拟服务器也变得越来越难。有些管理员在每台虚拟机的主机名后加上“_vm”以示区别。然而，很多企业不喜欢这种方法，因为任何名字的变化都会影响到用户和应用程序访问虚拟机数据信息的方式。在服务器转变为虚拟机之后，改变服务器的名字可能也会影响到服务器本地安装的应用程序和服务。如果管理员对一台遵循从物理平台到虚拟平台（P2V）迁移的服务器重新命名，他们通常使用 DNS 中的 CNAME 记录，以此来保证名字解析的透明性。但是，这种方法增加了对服务器资源管理的额外复杂度。另外一种标识服务器对象（无论是虚拟环境还是物理环境）的方法是使用每一台计算机对象 Active Directory 中的 Description 属性。已经有一些企业使用 Description 属性来标识一台计算机的位置、部门或者角色。考虑到这一点，使用 Description 属性可能要求用户能够简洁地标识出是物理平台还是虚拟平台。例如，可以使用如下的命名规范：

Ps – Physical server

Vesx – VMware ESX VM

Vms – Microsoft Virtual Server VM

Vxen – Xen VM

Vvi – Virtual Iron VM

Vvz – SWsoft Virtuozzo virtual private server

Vscon – Solaris Container

在所有 Description 属性中，我比较喜欢使用“P”作为物理平台的前缀，“V”作为虚拟平台的前缀。这样做的话可以使用户使用脚本语句对所有的虚拟机做查询操作，例如，仅通过脚本查询每一台计算对象的 Description 属性的第一个字母。
图 1 和图 2 给出了通过计算机对象的 Description 属性标识虚拟机的两种方法：

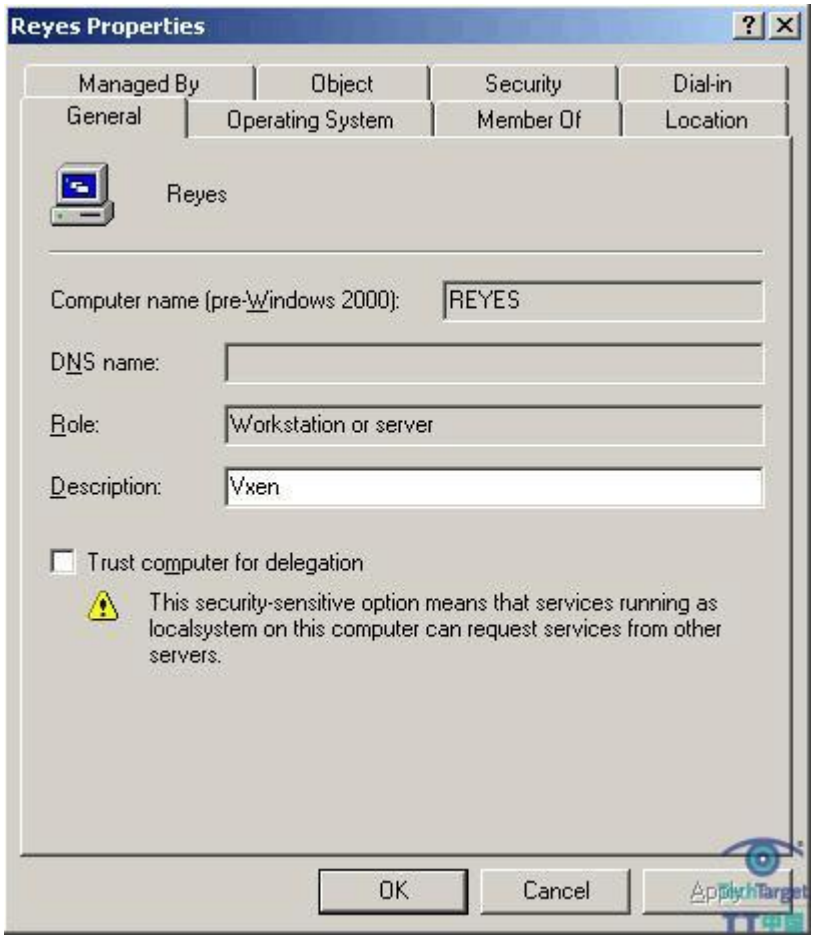


图 1：使用 Description 属性标识一台 Xen 虚拟机

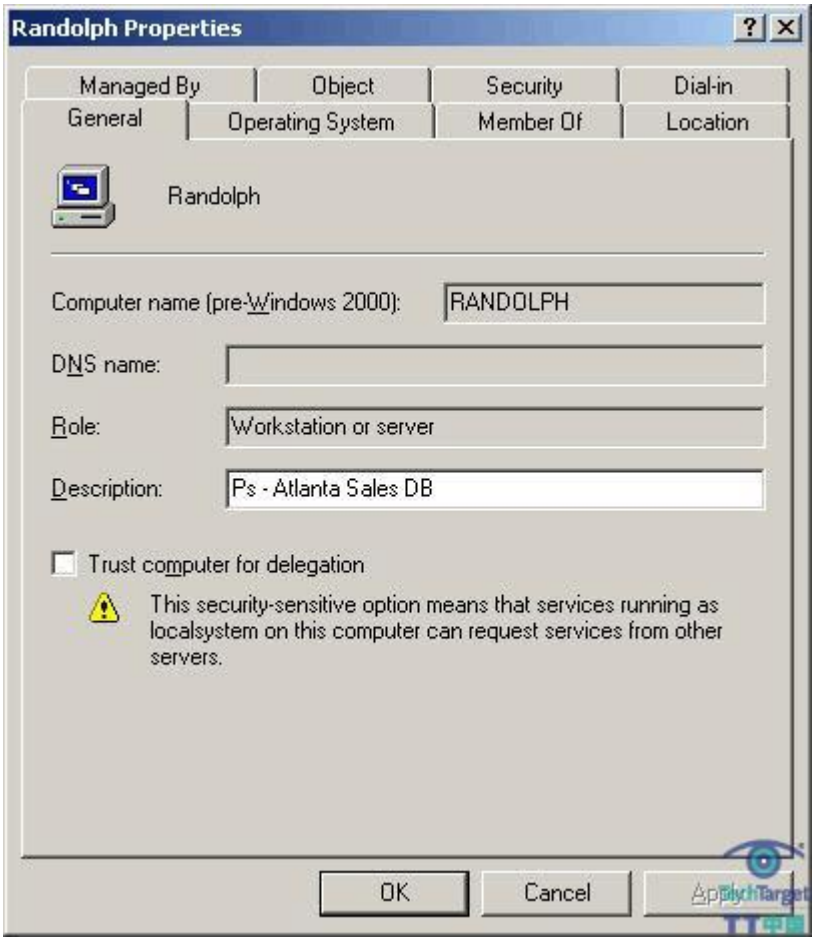


图 2：使用 Description 属性标识一台物理服务器，以及其位置、部门和角色

有了这些合适的命名规范，通过使用 Active Directory Users and Computers 和给这些对象排序（使用 Description 属性），就可以很快地在任何一个 Active Directory 容器中定位到虚拟机对象。点击 Active Directory Users and Computers 中的 Description 列就可以做到这些，双击的话就可以按照降序排序。如图 3 是一个通过 Description 排序计算机对象的例子：

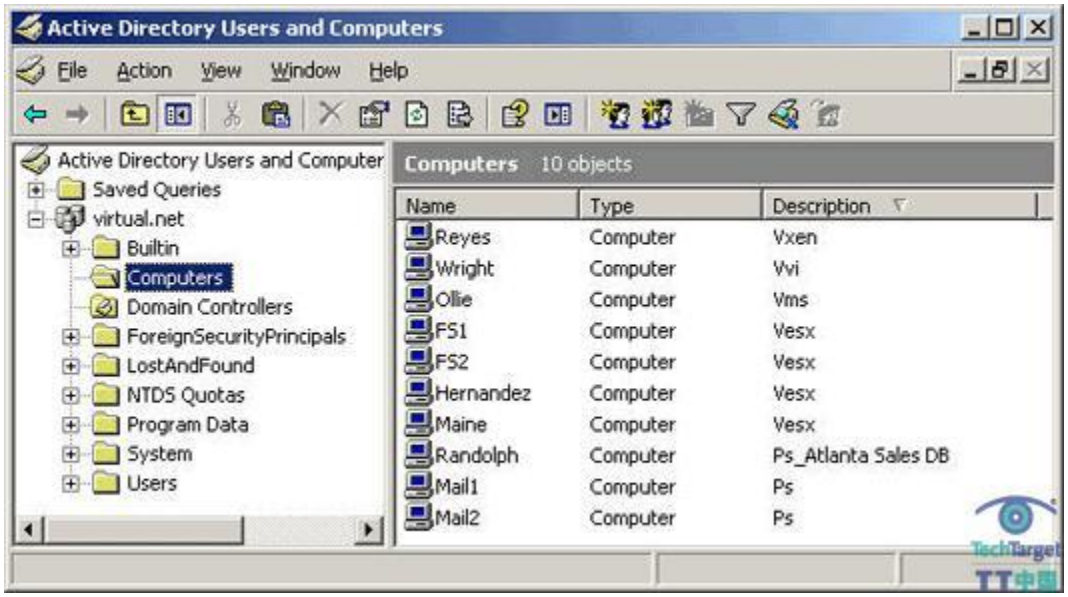


图 3：在 Active Directory Users and Computers 中排序虚拟机计算机对象

在大型企业中，很多管理员发现 Active Directory 查询属性非常有用。例如，为了定位所用域中的成员计算机（这些计算机都是 ESX 虚拟机），以下几个步骤就非常必要：

1. 在 Active Directory Users and Computers 窗口，右键点击“Domain Object”，选择“Find”
2. 在“Find”对话框，点击“Find Drop-down”菜单，选择“Computers”
3. 接下来，点击“Advanced”属性页。在“Advanced”属性页下，点击“Field”按钮，在复合的 drop-down 菜单中选择“Description”
4. 在“Condition Drop-down”菜单中，选择“Starts With”
5. 在“Value”属性中输入“Vesx”，注意如果需要搜索所有虚拟机，只需输入“V”
6. 接下来，点击“Add”按钮
7. 现在可以点击“Start”开始查询（如图 4），就可以显示出那些 Description 属性以“Vesx 开头”的计算机对象

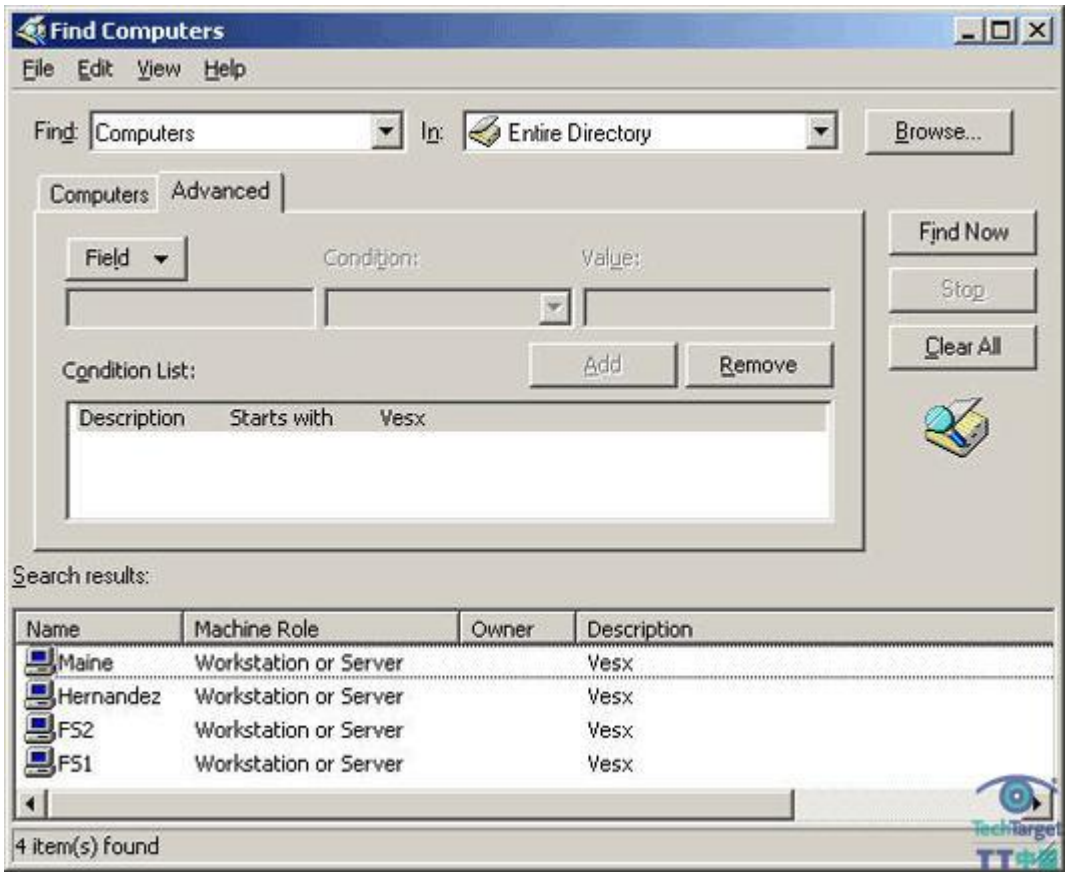


图 4：ESX 虚拟机 Active Directory 查询

当然，使用 Active Directory Users and Computers GUI 只能完成这些工作。在大型环境中，用户可能希望使用脚本语言来填充每一台计算机对象的 Description 属性。下面的 SetDescription.vbs 脚本就可以从一个文本文件中读取一个计算机列表，也可以修改这些已有的 Description 属性，确保其有一个物理或者虚拟的标识符作为前缀。

```
'SetDescription.vbs
'Adds virtual or physical descriptor to
'computer description attribute.

'set variables

'strPrefix -- physical or virtual identifier prefix
' Prefix values:
'  Ps – Physical server
'  Vesx – VMware ESX VM
'  Vms – Microsoft Virtual Server VM
'  Vxen – Xen VM
'  Vvi – Virtual Iron VM
```

```
'  Vvz – SWsoft Virtuozzo virtual private server
'  Vscon – Solaris Container
strPrefix = "Vesx"

'strDomainTarget -- this is the AD container
' where the target computer accounts are located
strDomainTarget = "cn=computers,dc=virtual,dc=net"

'strSourceFile -- file that contains computer
' account list
strSourceFile = "c:\computers.txt"

' Constants
Const ForReading = 1

'Open Source File
Set objFSO = CreateObject("Scripting.FileSystemObject")
set objSourceFile = objFSO.OpenTextFile(strSourceFile,_
    ForReading, True)

'Connect to Directory Service
'Modify computer description for each computer in
' source file list
Do Until objSourceFile.AtEndOfStream
    strcomputer = objSourceFile.Readline
    strADSpath = "LDAP://cn=" & strcomputer & _
      "," & strDomainTarget
    Set objComputer = GetObject(strADSpath)
    strOldDes = objcomputer.description
    If strOldDes = "" then
      strNewDes = strPrefix
    Else
      strNewDes = strPrefix & " - " & strOldDes
    End If
    objcomputer.Put "Description", strNewDes
    objcomputer.SetInfo
Loop
```

注意：在上述脚本中，需要修改如下的三个变量：

- strPrefix
- strDomainTarget
- strSourceFile

strPrefix 标识虚拟机的前缀，用来给每台计算机 Description 属性赋值。例如，对于 ESX 虚拟机，就可以把 strPrefix 赋值为“Vesx”；对于物理服务器，可以给 strPrefix 赋值

为“Ps”。strDomainTarget 必须用来给容器设置不同的名字，在这些容器中包含有目标计算机。例如，如果计算机对象在 TechTarget.com 域的 Computers 容器中，这个 strDomainTarget 变量就应该设置为“cn=computers,dc=techtarget,dc=com”；如果计算机对象在 TechTarget.com 域的 Development OU 中，这个 strDomainTarget 变量的值就应该设置为“ou=development,dc=techtarget,dc=com”。需要注意的是脚本一次只能在一个 Active Directory 容器中运行，因此，如果需要修改多个容器中计算机对象的话，用户就需要在每一个 Active Directory 目标容器中运行一次脚本程序。

strSourceFile 用来标识文本文件，在这些文本文件中是一个需要修改的计算机名列表。文件中的每一行都需要列出一个计算机主机名字。如下的链接中是一个样例：computers.txt。

在每一台计算对象的 Description 属性设定之后，用户就可以使用在本文中前面部分提到的 Active Directory Users and Computers 查询技术来定位虚拟机对象。另外，用户也可以使用一个脚本程序查询 Active Directory 或者输出一个计算机列表，这个列表包含有一个描述前缀符号，如“Vesx”或者“V”。在本系列文章的第二篇文章中，我们将讨论如何使用脚本进行 Active Directory 计算机对象 Description 查询；在第三部分中，我在 Active Directory 范式的基础上做了进一步扩展，其中包括用一个自定义属性来标识计算机是物理平台还是虚拟平台。

(作者：Chris Wolf 译者：王越 来源：TechTarget 中国)

原文标题：使用 Active Directory 标识和追踪虚拟机

原文链接：http://www.searchsv.com.cn/showcontent_19476.htm

使用脚本进行 Description 查询

在这系列文章的第二部分中，TechTarget 中国的虚拟化专家 Chris Wolf 将介绍如何使用脚本查询计算对象描述属性以定位虚拟机。

在这系列第一部分中，我介绍了如何使用计算机对象 Description 属性标识出虚拟平台和物理平台的方法。同时我也阐述了如何使用 vbscript 为大量计算机修改 Description 属性。

在本文中，我将介绍查询 Active Directory 的方法，来查询匹配预定义 Description 属性前缀的计算机对象。例如，如果用户希望查找所有虚拟机，可能就需要找出所有 Description 属性以“V”开始的计算机。如果要查找所有基于 Xen 的虚拟机，就需要查询所有 Description 属性以“Vxen”开始的计算机。

在上一篇文章中我解释了如何使用 Active Directory Users and Computers 执行计算机对象查找，但是有时用户要么是为了和其它管理工具保持完整性，要么是为了长时期保存，也可能希望输出存储在一个文本文件中。考虑到这些的话，可以使用脚本程序 QueryDescription.vbs（在我的个人主页上可以下载到文本格式）。执行这个脚本程序，可以返回一个计算机列表，这些计算机的 Description 属性都是以预定义字符串开始的。

为了在读者的工作环境中使用这个脚本程序，需要编辑三个变量：

- strPrefix
- strDomainTarget
- strLogFile

strPrefix 标识 Description 属性前缀，以包括查询使用。例如，把 strPrefix 设置为“V”将会返回所有虚拟机列表。如果把 strPrefix 设置为“Ps”，将会返回所有物理服务器列表。

strDomainTarget 用来标明用户希望查询域的不同名字，这个变量的设置需要和用户的域名相匹配。因此如果用户管理的是 searchservervirtualization.com 域的话，strDomainTarget 就需要设置为“dc=searchservervirtualization, dc=com”。需要注意的是用户也可以通过新增一个不同的名字限制一个 OU 的连接范围，例如，为了连接 TechTarget.net 域中的“Web”OU，strDomainTarget 就应该设置为“ou=web,dc=techtarget, dc=net”。

最后一个可能需要修改的变量是 strLogFile。strLogFile 标识脚本程序输出的日志文件所存储的位置。默认保存到 C 盘根目录下，下面是一个日志文件的样例：

The following computers have the vesx Description Prefix:
Computer Name
==========
FS1
FS2
Hernandez
Maine
web1
web2
web3

相信读者也看到了，在 Active Directory 中跟踪虚拟机对象没有看起来那么难。使用脚本程序修改 Description 属性来标识计算机是特定的虚拟机类型或者是物理系统，使用该方法可以允许用户更迅速地合理部署一个系统，并且可以更轻松地跟踪整个企业内部系统中的所有虚拟机。在全部现有的物理计算机和虚拟机对象在它们的 Description 属性中都设置合适的前缀之后，用户应该确保所有新加入域的虚拟机也拥有正确的 Description 属性前缀（如 Vesx、Vvi、Vms 等）。企业内部的部署和更改控制流程也需要随之进行更新，以保证这些操作正常进行。

在本系列文章的最后一部分，我将探讨自定义 Active Directory 的一些方法。通过这些自定义 Active Directory，可以使用自定义虚拟机属性。如果使用已有 Description 属性（其它属主的 Description 属性），下一篇文章中给出的解决方案或许正是读者所需要的。

(作者：Chris Wolf 译者：王越　来源：TechTarget 中国)

原文标题：使用脚本进行 Description 查询

原文链接：http://www.searchsv.com.cn/showcontent_19480.htm

添加自定义 Active Directory 计算对象属性定位虚拟机

在这一系列的最后一篇文章中，TechTarget 中国的特约虚拟化专家 Chris Wolf 将介绍如何添加自定义 Active Directory 计算对象属性以定位虚拟机。

在本系列文章的的前两篇中，我描述了一种通过计算机对象 Active Directory 中 Description 属性来标识一个工作环境是物理环境还是虚拟环境的方法。在本文中，我将对 Active Directory Integrity 做进一步介绍，探讨自定义 Active Directory 模式，用来支持新的虚拟化属性。

在本文中，我给出了创建两个自定义 Active Directory 属性（isVirtual 属性和 vmType 属性）的基本步骤。isVirtual 属性是一个布尔变量，用来标识一台计算机是物理计算机还是虚拟计算机。如果 isVirtual 设置为“True”，就说明该计算机对象是虚拟机。如果用户希望以更细的粒度标识虚拟机，就需要增加 vmType 属性。vmType 是一个字符串变量，可以用来标识一台虚拟机的虚拟平台，在此需要使用第一篇文章中所描述的命名规范。

需要注意的是本文所述的过程要求 Active Directory 模式修改，修改后是不可撤消的。如果存在问题，那么你需要评估本系列前两篇文章中所描述的解决方案。对于扩展 Active Directory 模式的技术背景，用户需要看是 TechNet 的一篇文章《Extending the schema》，在这篇文章中，有几个微软文档的链接。微软的这几篇文档解释模式修改的程序及其微小差异。一定要记住本文列出的几个步骤在应用到产品领域之前，一定要先在某个测试环境中进行评估。

在开始之前，如果还没有对象标识符（（OID：Object Identifier））的话，需要为企业申请一个。如果企业没有 OID，就需要在 MSDN 的 Active Directory Naming Registration 网站申请一个。另外，在这篇之外也不失一般性，最好的方案是在通用名字和 LDAP 显示名字中使用企业指定的模式前缀。例如，我的模式前缀是 cwolf。因此不是使用通用名字“isVirtual”，最好的方法是使用“cwolf-isVirtual”，关于模式命名更多的信息，参看 Microsoft Windows Server 2003 应用程序规范。请注意，如果读者希望在一个实验室环境中测试这些流程，可以使用我在本文中给出的 OID 变量。

为了创建新 isVirtual 属性和 vmType 属性，需要注册 Active Directory 模式 MMC 嵌入式管理单元。为了注册这个管理单元，需要登录域控制器，运行命令 regsvr32 schmmgmt.dll。注意：只有用户是模式管理组成员才可以能够对 Active Directory 模式做出改动。
接下来就需要运行 mmc 目录打开一个空 MMC shell，在 shell 上新增 Active Directory 模式管理单元。如果创建一个自定义的虚拟机属性，以下几个步骤是很有必要的：

1. 在“Active Directory Schema MMC”中，右键点击“Attributes Container”，选择“Create Attribute”

2. 查看“Schema Object Creation warning”对话框；点击“Continue”，一定要注意属性增加将会导致 Active Directory 模式的永久性改变

3. 在如图 1 所示的对话框中，输入如下变量：

Common Name: isVirtual
LDAP Display Name: isVirtual
Unique X500 Object ID: Prefix value associated with organization's OID, followed by a unique attribute identifier. For example, 1.2.840.113556.1.8000.2522.2.1.
Description: Identifies a computer as virtual
Syntax: Boolean

4. 在“Create New Attribute”对话框中输入要求的变量之后，点击“OK”就可以创建 Description 属性

5. 接下来，需要创建 vmType 属性；右键点击“Attributes Container”，选择“Create Attribute”

6. 查看“Schema Object Creation warning”对话框；点击“Continue”

7. 在“Create New Attribute”对话框中（如图 2），输入如下变量：

Common Name: vmType
LDAP Display Name: vmType
Unique X500 Object ID: Prefix value associated with organization's OID, followed by a unique attribute identifier. For example, 1.2.840.113556.1.8000.2522.2.2.
Description: Identifies the VM's virtualization platform
Syntax: Case-insensitive string

8. 刷新模式之后就可以看见新增的属性；右键点击“Active Directory Schema object”，选择“Reload the Schema”

9. 接下来，点击“Attributes Container”，定位 isVirtual 属性；看到 isVirtual 属性之后，右键点击选择“Properties”

10. 在“isVirtual Properties”对话框中，检查“Index this Attribute in the Active Directory”复选框，点击“OK”；注意，在此也需要选上 Attribute is Active 框。

11. 如果新增“vmType Attribute”重复第 9 步和第 10 步

12. 需要注意的是所创建的属性必须和计算机类相关联；所以需要扩展类容器并且定位“Computer”类；右键点击“Computer”，选择“Properties”

13. 在“Computer Properties”对话框中，选择“Attributes”属性页，点击“Add”按钮

14. 在“Select Schema Object”对话框中，向下拉选择“isVirtual attribute”，然后选择“OK”

15. 在“Computer Properties”对话框的“Attributes”复选框内，再次点击“Add”按钮

16. 现在可以选择“vmType Attributes”，点击“OK”

17. 在在“Computer Properties”对话框的可选属性中就可以看到 isVirtual 和 vmType；点击“OK”保存更改

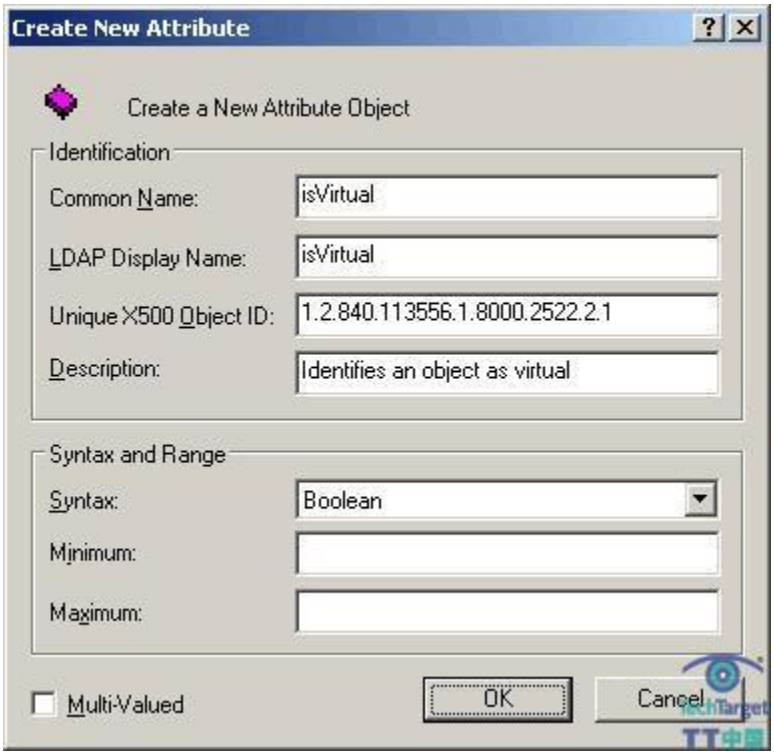


图 1：创建 isVirtual 属性

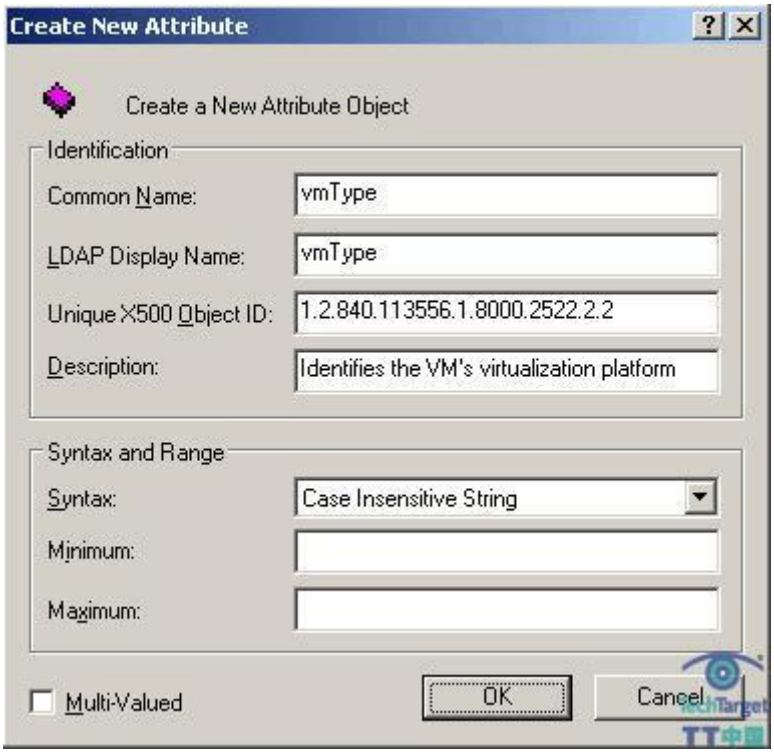


图 2：创建 vmType 属性

注意这些步骤将会改变模式，对 Active Directory 模式的任何改变将会影响到整个集群，所以需要确保在尝试该流程之前，对于这些变化有适当的符号结束指令。

在属性增加到模式之后，就需要配置属性，使用 setvirtual.vbs vbscript 脚本程序设置计算机 isVirtual 属性：

```
strComputerDN = "CN=reyes,CN=Computers,DC=virtual,DC=net"
Set objComputer = GetObject("LDAP://" & strComputerDN)
objComputer.Put "isVirtual" , true
objComputer.SetInfo
```

另外还需要编辑 strComputerDN 变量的名字确保和要编辑的计算机的不同名字保持一致，可以使用如下 queryvirtual.vbs 脚本查询一台计算机的 isVirtual 属性：

```
strComputerDN = "CN=reyes,CN=Computers,DC=virtual,DC=net"
Set objComputer = GetObject("LDAP://" & strComputerDN)
isVirtual = objComputer.get("isVirtual")
wscript.echo(strComputerDN & " isVirtual = " & isVirtual)
```

如果需要为很多计算机设置 isVirtual 和 vmType 属性，我的个人主页上的 setvirtualattributes.vbs 脚本程序可以完成这项工作。

但是需要修改脚本程序中的以下几个变量：

- blnIsVirtual
- strVMtype
- strDomainTarget
- strSourceFile

在使用脚本标识计算机对象为虚拟机的情况下，blnIsVirtual 需要被设置为“True”。

strVMtype 标识虚拟机类型代码，用来自定义每台计算的 vmType 属性。例如，设置 ESX 虚拟机的 strVMtype 为“Vesx”。

strDomainTarget 必须用来给容器设置不同的名字，在这些容器中包含有目标计算机。例如，如果计算机对象在 TechTarget.com 域的 Computers 容器中，这个 strDomainTarget 变量就应该设置为“cn=computers,dc=techtarget,dc=com”；如果计算机对象在 TechTarget.com 域的 Development OU 中，这个 strDomainTarget 变量的值就应该设置为“ou=development,dc=techtarget,dc=com”。需要注意的是脚本一次只能在一个 Active Directory 容器中运行，因此，如果需要修改多个容器中计算机对象的话，用户就需要在每一个 Active Directory 目标容器中运行一次脚本程序。

strSourceFile 用来标识文本文件，在这些文本文件中是一个需要修改的计算机名列表。文件中的每一行都需要列出一个计算机主机名字。如下的链接中是一个样例：computers.txt。

最后，为了定位一个特定域内的所有虚拟机，需要运行 QueryVirtualAttributes.vbs 脚本，该脚本程序可以在我的个人主页上下载到文本格式。为了在读者的工作环境中运行该脚本，需要修改三个变量：

- strVMtype
- strDomainTarget
- strLogFile

strVMtype 标识用户可能查询的虚拟机平台类型。例如，设置 strVMtype 为“Vxen”将会输出一个所有基于 Xen 的虚拟机列表；使用“V”作为 vmType 变量将会输出 isVirtual 属性都是“True”的计算机列表，同时还有 vmType 属性的值。

strDomainTarget 用来标明用户希望查询域的不同名字，这个变量的设置需要和用户的域名相匹配。因此如果用户管理的是 searchservervirtualization.com 域的话，strDomainTarget 就需要设置为“dc=searchservervirtualization, dc=com”。需要注意的是用户也可以通过新增一个不同的名字限制一个 OU 的连接范围，例如，为了连接 TechTarget.net 域中的“Web”OU，strDomainTarget 就应该设置为“ou=web,dc=techtarget, dc=net”。

最后一个可能需要修改的变量是 strLogFile。strLogFile 标识脚本程序输出的日志文件所存储的位置。默认保存到 C 盘根目录下，下面是一个日志文件的样例：

```
The following computers have the Vesx vmType attribute
Name VM Type
==== =======
Reyes Vesx
Maine Vesx
Wagner Vesx
WS86 Vesx
```

从本系列文章的第一部分和第二部分中提到的技术可以看到，每次一台新计算机对象创建时，为 isVirtual 和 vmType 自定义 AD 属性值是非常重要的。

整合虚拟化管理和 Active Directory 可以给用户对于审计和管理整个企业内部所有虚拟机更大控制权。令人振奋的消息是，本系列文章中提到的一个解决方案可以提供 AD 整合和管理，这或许正是各位读者正在寻找的。如果不是的话，请告知我还需要那些技术来简化虚拟化工作环境的管理工作。

(作者：Chris Wolf 译者：王越 来源：TechTarget 中国)

原文标题：添加自定义 Active Directory 计算对象属性定位虚拟机
原文链接：http://www.searchsv.com.cn/showcontent_19482.htm

使用 Windows Server 2008 里的 Active Directory 快照

Windows Server 2008 允许管理员对 Active Directory 进行快照。顾名思义，快照就是对数据库在线、只读的备份。

在作出任何主要的 Active Directory 修改之前创建快照，以便在需要的时候使用副本数据库恢复。这样你可以比较在运行的数据库与副本里包含的设置。甚至可以从快照输出数据，输入到活动着的 Active Directory 数据库。

创建 Active Directory 快照

可能有点奇怪，在 AD 快照过程的第一步实际上是创建快照本身。打开高级命令提示符窗口并输入下面命令：

NTDSUTIL "Activate Instance NTDS" snapshot create quit quit

如图 A 所示，尽管我们输入了单个命令，Windows 实际上作为独立命令解释了单个部分。你应该能从这些命令执行输出执行创建的快照。

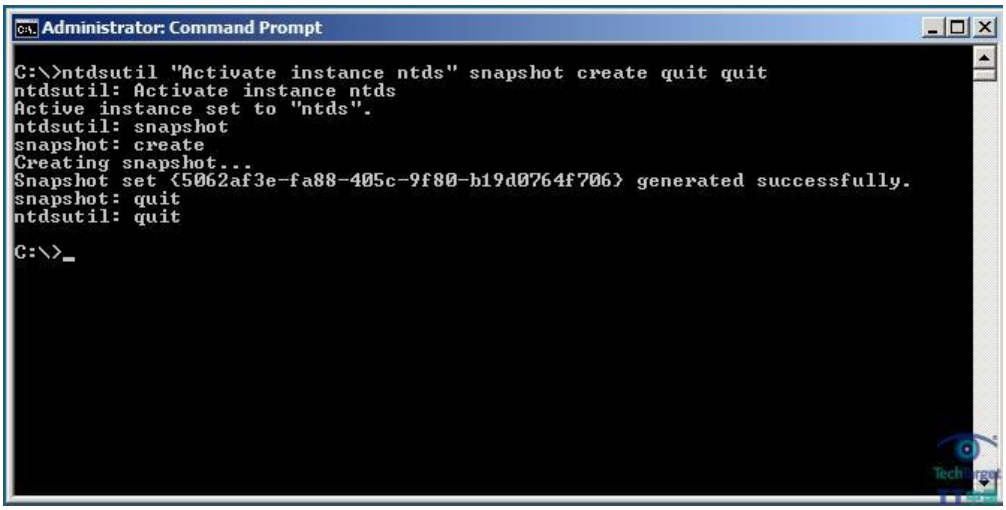


图 A（点击图片本身就能放大）

启动快照

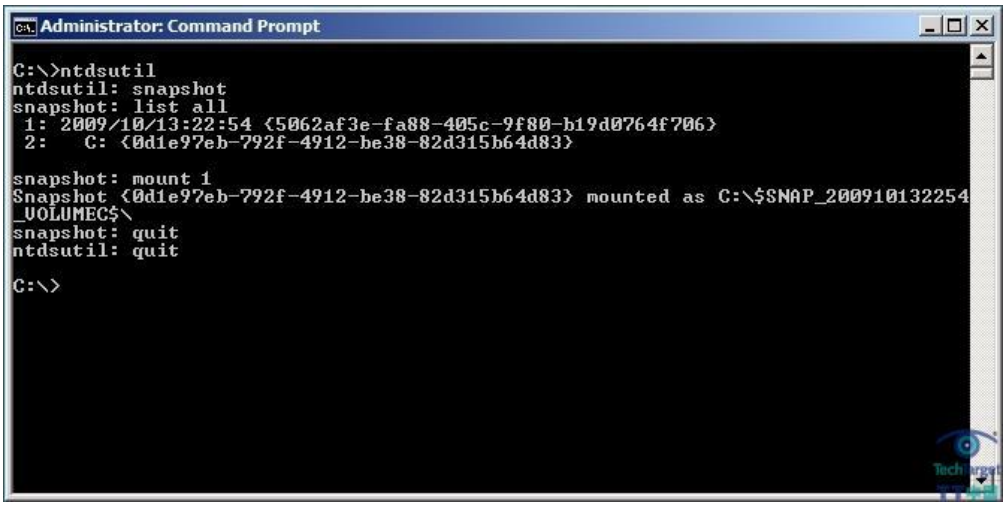
创建快照后，仍然必须在使用之前启动它。从你的高级命令提示符输入下面命令：

NTDSUTIL
Snapshot
List all

一般说来，在你输入这些命令时能看见两个列出的 Active Directory 快照。第一个快照显示的是目前的数据和时间。这是你刚刚创建的快照。如果你再看图 A，会发现有一行文本：Snapshot Set {5062af3e-fa88-405c-9f80-b19d0764f706} generated successfully。这与快照 1 上日期后面的数字相同。因此，我们需要告诉 Windows 启动快照 1，输入下面命令：

Mount 1

如图 B 所示。



连接 Active Directory 快照

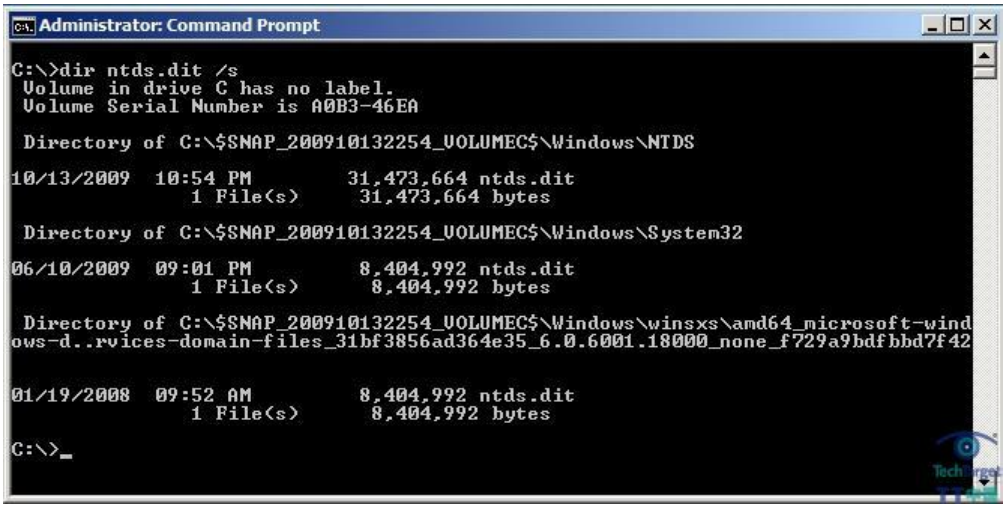
现在我们已经启动了快照，我们必须将其连到一个端口号以浏览快照。通常，LDAP（轻量目录访问协议）查询通过 Port 389 制作到 Active Directory。我们能使用任何未使用的端口号。实际上，你需要四个空闲的连续端口号。我推荐使用端口 30,000，这会让 Windows 作出如下的端口分配：

30,000 LDAP
30,001 LDAP / SSL
30,002 Global Catalog
30,003 Global Catalog / SSL

在我们能分配端口号之前，我们需要找到快照里 Ntds.dit 文件的位置。尽管这个文件通常位于 C:\Windows\NTDS，你仍然应该输入下面命令：

C:
CD\
Dir ntds.dit /s

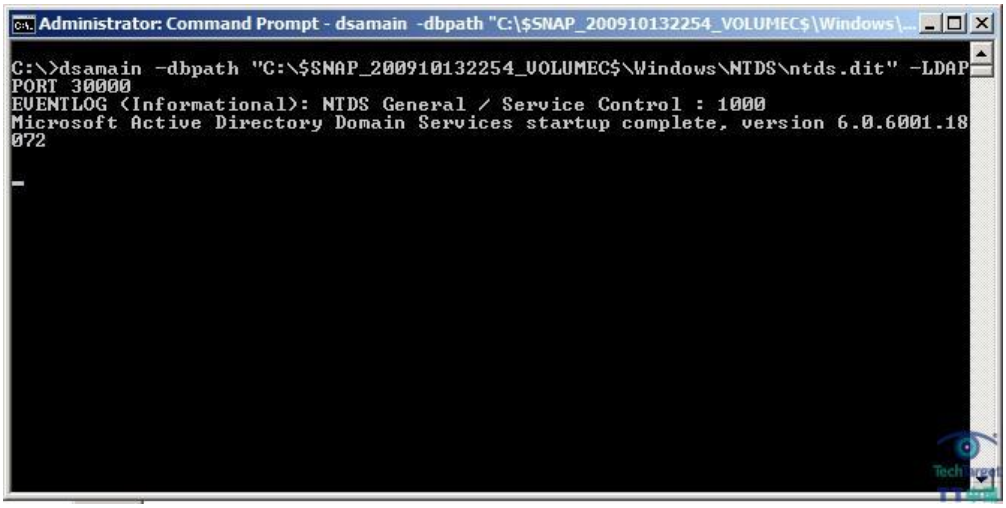
如果你查看图 C，你将看到返回到 C:\Windows\NTDS\ntds.dit 的第一个结果。你也注意到路径包括代码 C:\$SNAP_200910132254_VOLUMEC$。你必须注意路径这部分，它在每台服务器上都不同。



知道到 Ntds.dit（包括启动代码）的路径之后，你已经选择了一个端口号，通过使用下面命令启动快照：

DSAdmin –dbpath "C:\SNAP_200910132554_VOLUMEC$\Windows\NTDS\ntds.dit" –LDAPport 30000

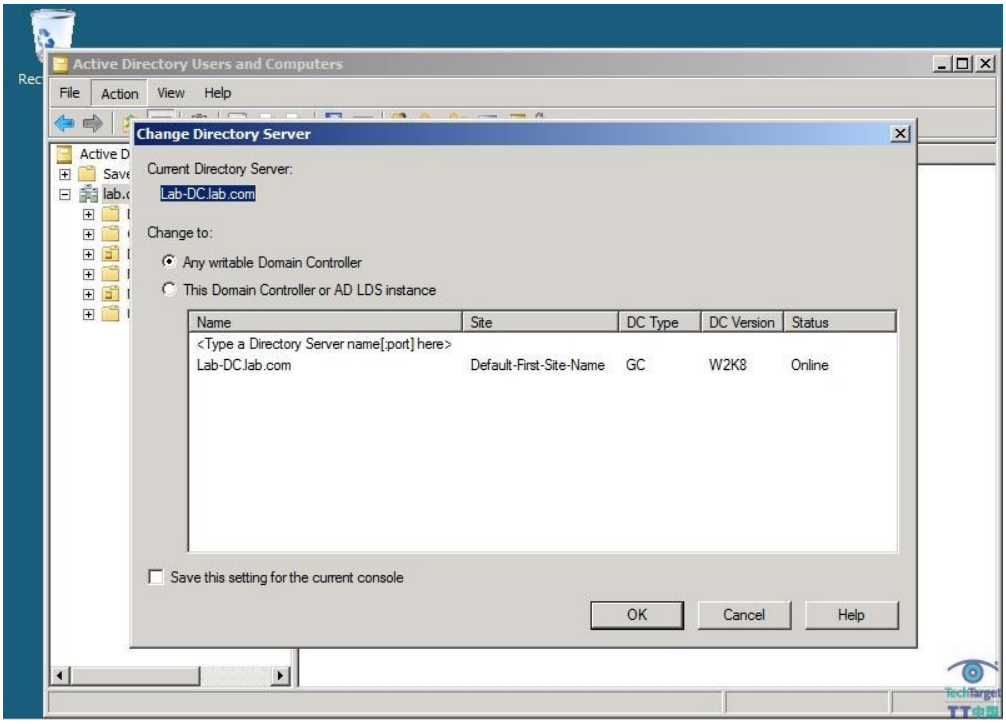
如图 D 所示，我们将收到来自 Active Directory Domain Services 启动的确认，不过稍后窗口看起来是锁定的。然而窗口实际上没有锁定，让它保持打开状态很重要。



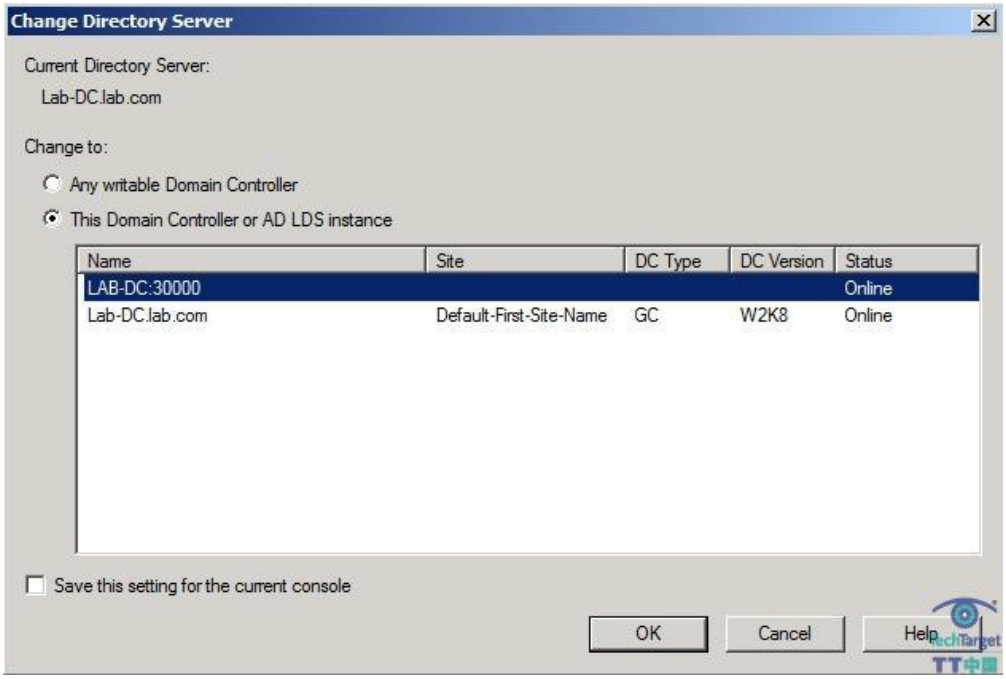
使用 Active Directory 信息

在你最后完成启动 Active Directory 快照后，能用所有标准的 Active Directory 工具使用快照。要理解快照如何工作，我们来看看如何使用 Active Directory Users 和 Computers 控制台使用快照。

打开控制台后，从 Actions 菜单选择 Change Domain Controller 命令。现在能看见 Change Directory Server 对话框，如图 E 所示。选择选项 This Domain Controller or AD LDS Instance，然后点击选项 Type a Directory Server Name [port] Here。



接下来，输入域控制器的名称，一路点击确定并选择你所选的端口号。例如，在图 F 你能看见我已经输入 Lab-DC:30000。点击 OK，控制台将指向使用 Active Directory 快照。



断开快照

当你使用完快照后，关闭控制台窗口并退回到高级命令提示符窗口。按下 Ctrl+C 键，快照就断开了。

接下来，你必须关掉并删除快照。首先输入以下命令：

NTDSUTIL
Snapshot
List mounted

一旦验证分配给快照的数字，通过以下命令删除快照：

Unmount 2
Delete 2
Quit
Quit

Active Directory 快照提供了与在线 AD 副本轻松工作的方式。记住，虽然从快照输出 Active Directory 设置是可能的，但是快照本身是只读的。

(作者：Brien M. Posey 译者：唐琼瑶 来源：TechTarget 中国)

原文标题：添加自定义 Active Directory 计算对象属性定位虚拟机

原文链接：http://www.searchsv.com.cn/showcontent_28325.htm

使用 Windows Active Directory 组控制 vSpere 管理权限

Windows 管理员在实际操作中发现最好能够在安装服务器之后配置该服务器，从而可以使用户以非 Windows 管理员的身份登录。在 VMware vSpere 管理过程中也会遇到同样的问题：在 vCente 服务器设置、运行，并且合理配置之后，用户应该可以不以 Windows 管理员登录那样登录到 vSpere 客户端。但是为了达到这个目的，就需要使用 Windows Active Directory（AD）连接 vSpere。在本文中，TechTarget 中国的特约虚拟化专家 David Davis 将会介绍如何创建一个 Windows AD 组，以及如何在 vSpere 中使用这个组控制虚拟基础架构的管理人员。

为什么不能够使用管理员账号管理 vSpere？

和用户不希望每一个人都可以以“域管理员”或者甚至是“本地管理员”身份登录到自己的 Windows PC 机一样，用户也同样不希望所有 VMware 管理员以域管理员身份（或者是用户所创建的其他具有完全访问权限的管理员账号）登录到 vSpere。下面列出的是若干个真正原因：

- **可追踪性**：每个用户使用相同的用户名，那么如果虚拟基础架构出问题的话，怎么定位该有谁来负责？如果每个用户都以自己的账号登录，这样就可以在账号身份下记录该用户做的所有更改，而不是记录在一个统一的账号下。
- **认证**：如果每个用户都以管理员身份登录，如何定位知道网络上的恶意攻击者。因为每个用户看起来都一样。
- **授权**：需要限制对虚拟基础架构的访问，读者是否听说过最小特权原则？根据该原则，应该是只给员工授权对完成其自身任务所必需的公司资源的访问权限。这样的话，每个用户都应该以其自身的身份登录到系统，并且可以限制在虚拟基础架构中特定区域和任务，这是其完成工作所必需的。

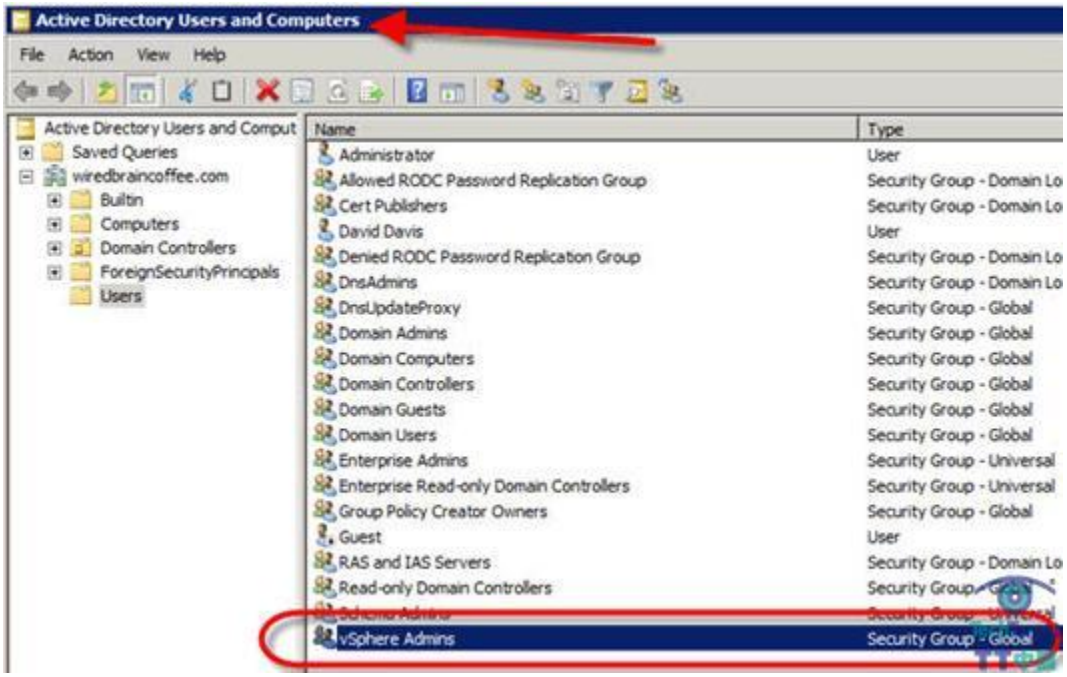
为 vSpere 管理工作创建一个 Windows AD 组

Windows Active Directory 很可能是网络上认证信息（用户名和口令）的一个单独存储池。用户希望使用 Windows AD 而同时又不需要再另外创建一个认证信息存储池。幸运的是，VMware 内置了这项功能，并且也可以很方便地使 AD 和 VMware 协调工作。

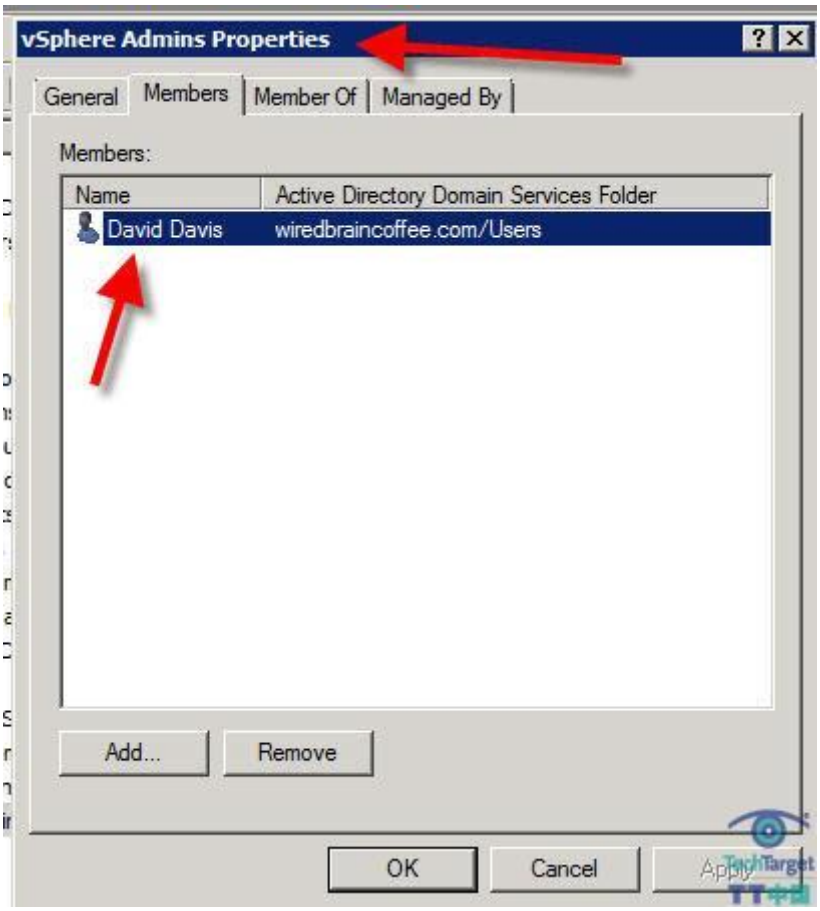
即使在网络上只有一个 VMware 管理员，还是需要首先创建一个名字为“vSpere Admins”的 Windows 组。最初该组可能只有一个账户，但是之后可以新增其他账户。也可以创建其他组，然后为其命名，如“vSphere Desktop VM admins”或者“vSphere Web Server admins”。这些组内的账户没有完全控制权限，但是可以管理该区域内的特定 VMware 虚拟机。也可以更具体点，如创建一个命名为“vSphere Support Techs”的组，只给该组内的账户对特定虚拟机开机和关机权限。

下面创建“vSphere Admins”组：首先需要进入 Windows DC 界面，运行 Active Directory Users and Computer（或者远程运行）。

Active Directory Users and Computer 运行之后，在 Windows AD 内创建一个新的全局安全组，命名为“vSphere Admins”，如下图所示：



下一步，把自己和其他 vSpere 管理员账户添加到这个组内，如下图所示：

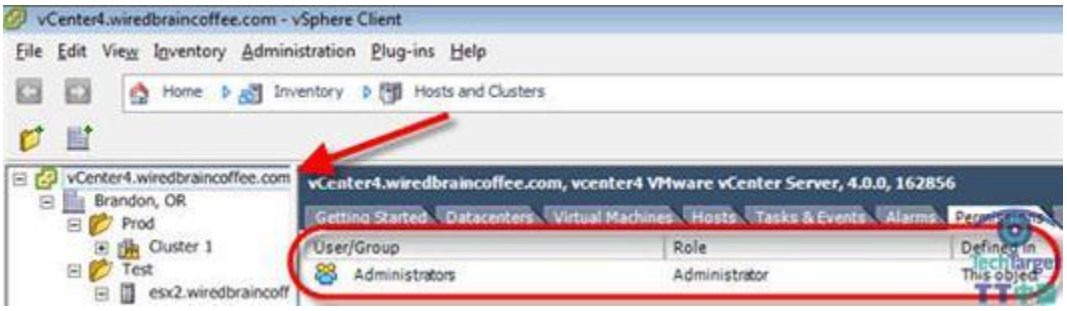


上面都是从 Windows AD 的角度看，下面介绍一下在 vSpere 内需要做的工作。

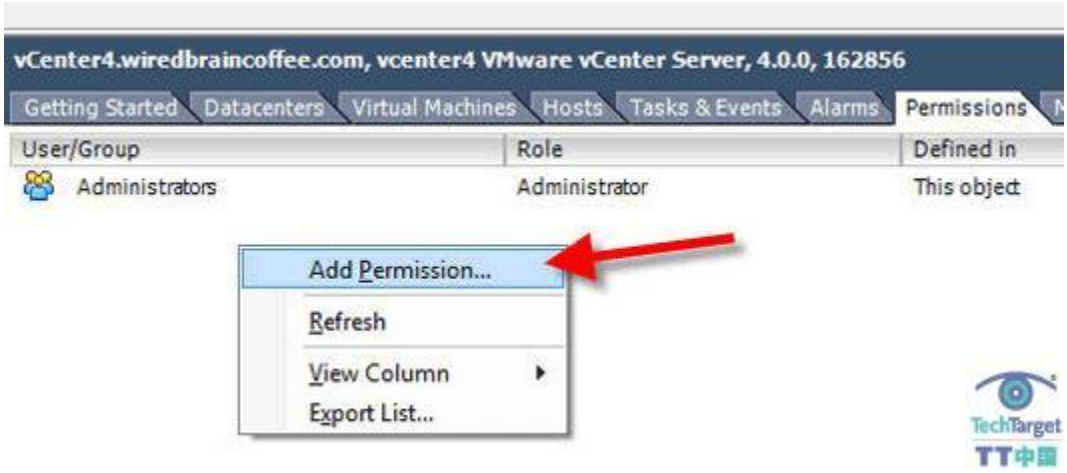
配置 vSpere 可以使其使用 Windows 组控制管理权限

创建 Windows AD 组并且把用户账号加入该组后，需要告诉 vSpere 使用这个 Windows 组。假定计划给予这些组内的用户完全的 vSpere 管理员权限，点击“主机和集群目录”中目录树的最高级别就可以了，这个应该是虚拟基础架构的 vCenter 服务器。

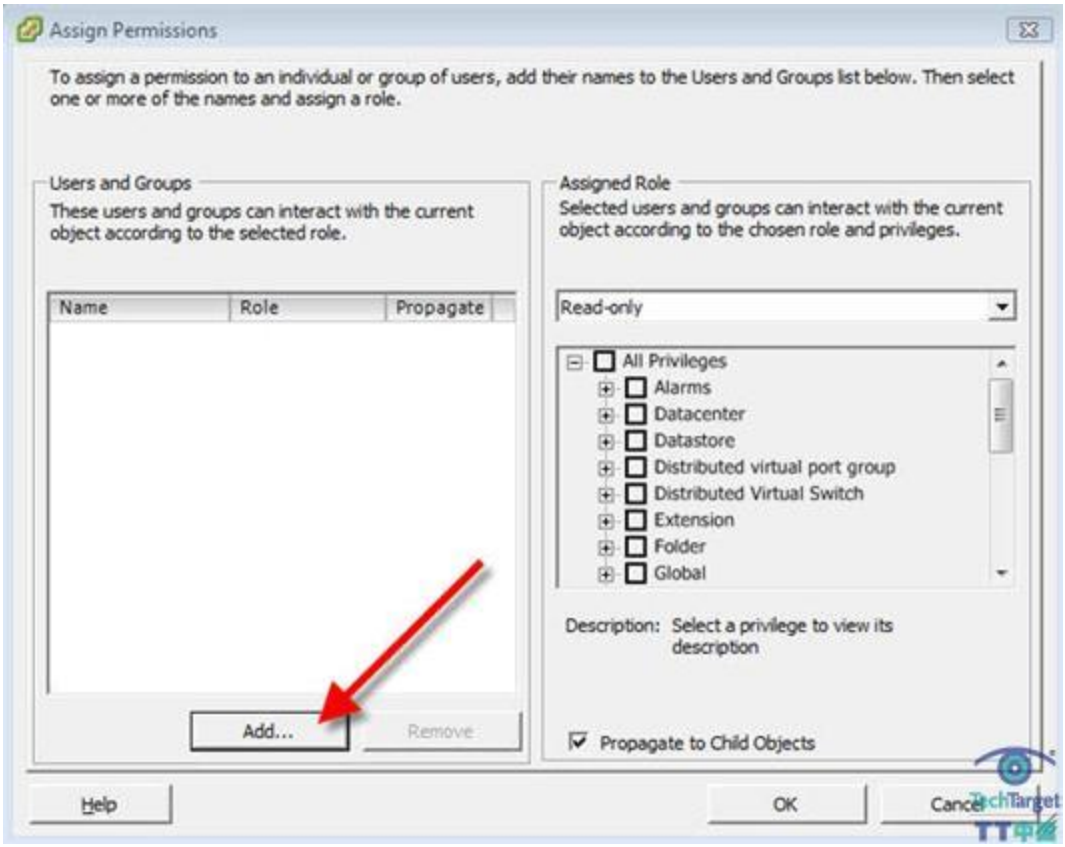
点击 vCenter 服务器，然后点击“权限许可（Permission）”标签页。可以看到管理员组拥有完全访问权限，如下图所示：



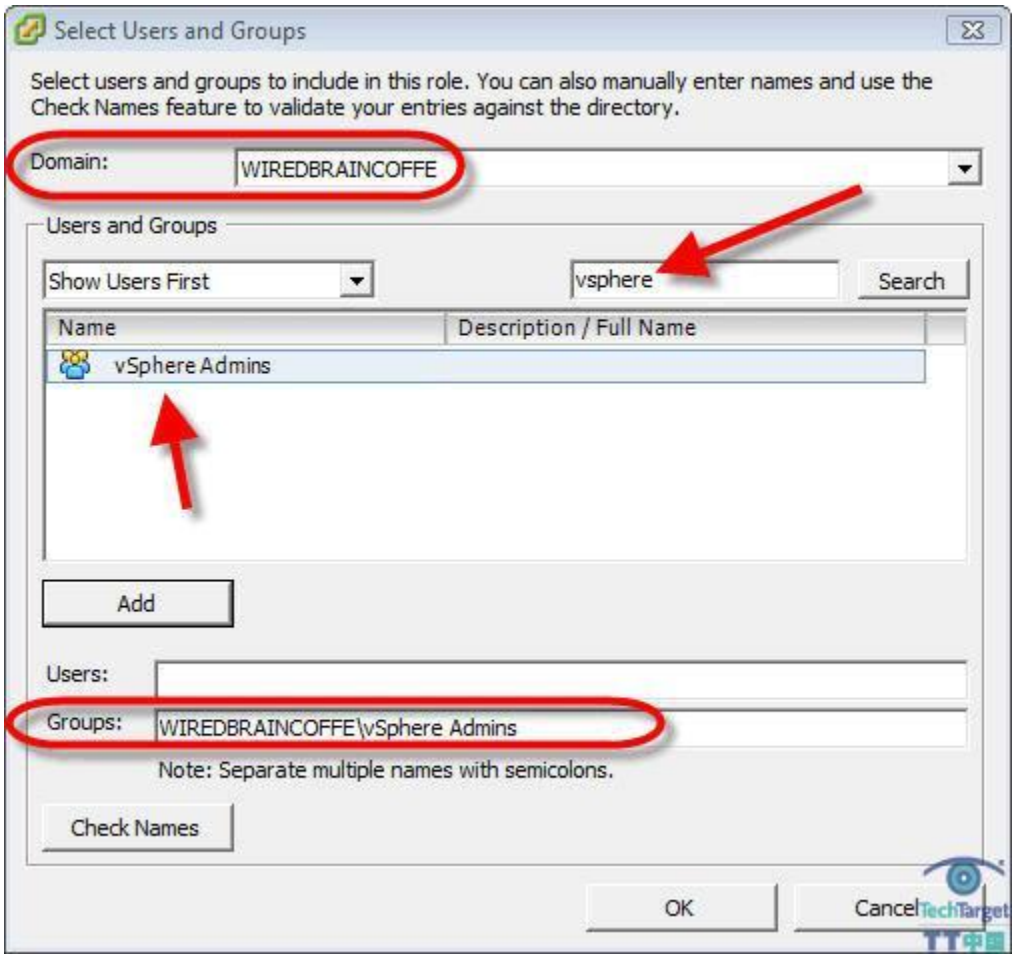
接下来需要做的是创建一个新 vSpere 管理组，移除当前组。当然在增加新组之前用户不希望移除当前组，否则就会失去任何访问权限。为了增加新组，在权限许可标签页的空白处单击右键，选择“新增权限许可（Add Permissions）”，如下图所示：



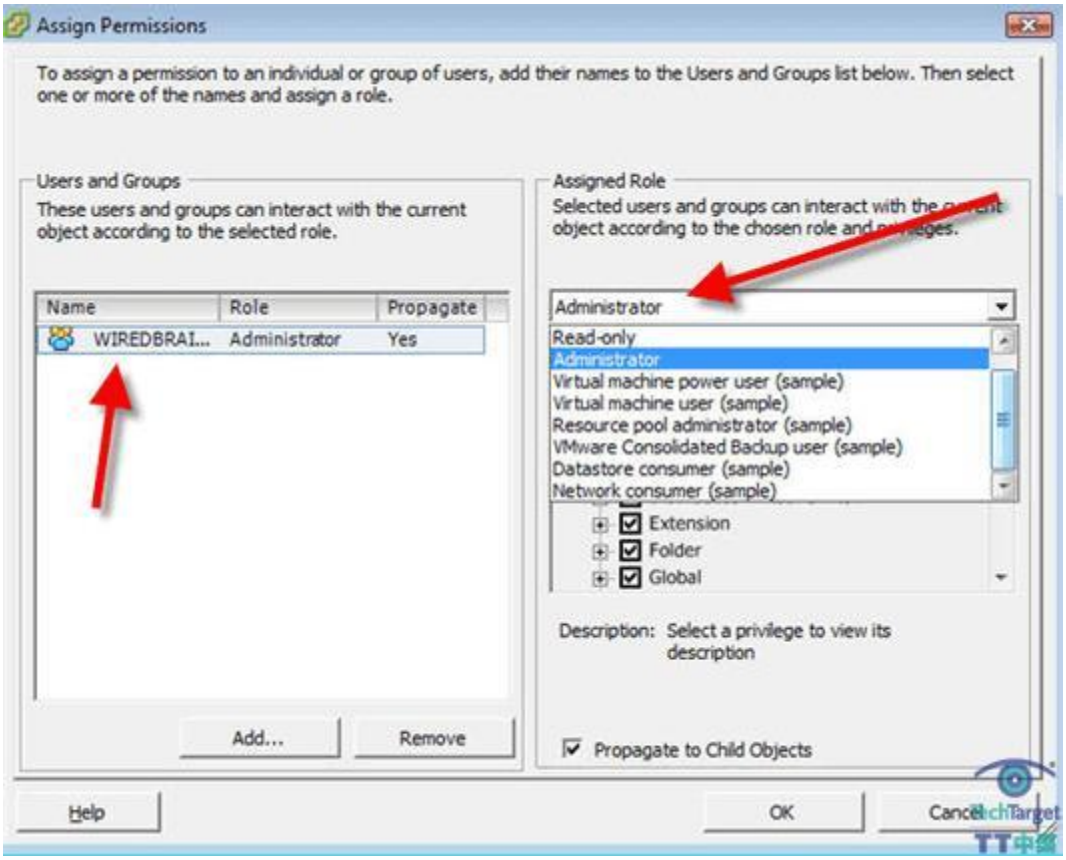
然后就可以看到“指定权限许可”窗口，在这个对话框上，点击“添加”就可以增加新用户和组，如下图所示：



此时出现的是“选择用户和组”对话框。选择将要用来覆盖用户和组的域。在实施过程中，我们选择了“WIREDBRAINCOFFEE”域，因为有很多用户和组都在这个列表中，因此我使用搜索选项寻找 vSpere。在此仅仅看到新创建的 vSpere 管理组，所以选择这个组，然后点击“添加”，如下图所示：



现在点击“完成”就可以了。回到“指定许可权限”对话框就可以看到新增的 vSpere 管理组，但是该组在默认状态下只有只读权限。在右边，我使用“指定角色”的下拉菜单，找到“管理员”选项，如下图所示：



接下来，点击“完成”使这个管理员角色指定到 vSe 管理组操作生效。现在就拥有两个不同的组，这两个组都可以对 vSpere 做管理性的修改。

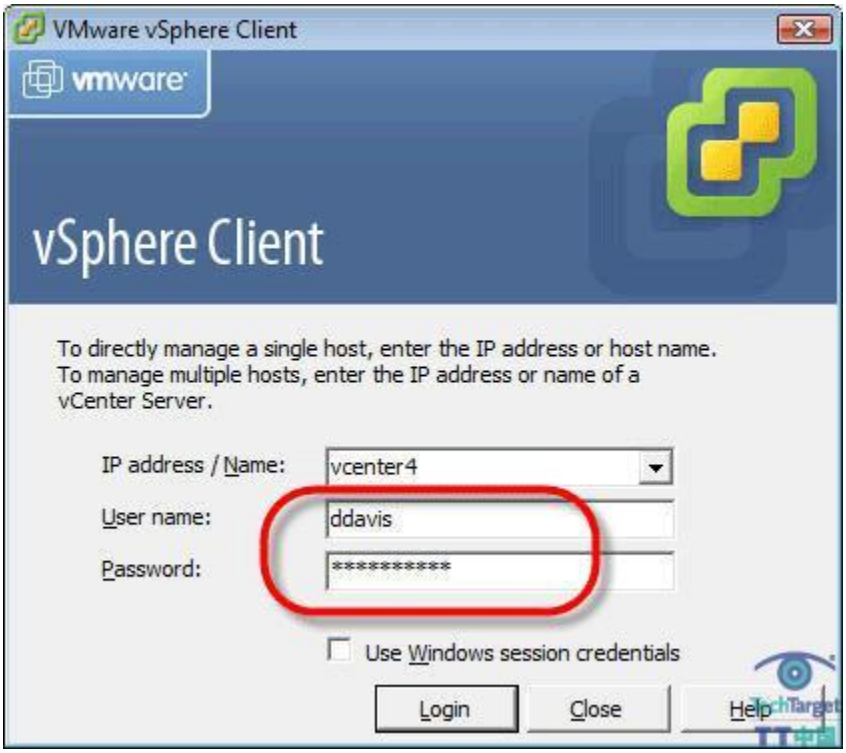
现在需要移除默认的管理员组，右键点击该组，选择“删除”。在弹出的确认删除的消息框中，点击“是”。然后需要立刻取消 vSpere 客户端，因为此时是以管理员身份登录的，对吧？

测试新 Windows AD 和 vSpere 安全配置

为了充分测试，需要连接到 vSpere 客户端。以自己的身份登录到系统，可以使用在 Windows AD 中为自己定义的任何用户名和口令。如果已经使用 Windows AD 登录到 PC

机中，该登录和新 vSpere 管理组中的 Windows AD 登录相同。点击“使用 Windows 会话认证信息”，看来并不是必须输入用户名或者口令才可以建立连接。

如果在 PC 机上没有登录到该域中，输入 Windows 的域名和口令，如下图所示：



成功了！

成功地以“ddavis”（那个是我的用户名）身份登录到 vSpere 客户端，而不用必须以 Windows 域管理员的身份登录。

最后回到 vSpere vCenter 服务器的权限许可标签页，验证名字为“vSphere Admins”的 WiredBrainCoffee.com 域用户是否能够登录和控制该虚拟基础架构。

(作者：David Davis 译者：王越　来源：TechTarget 中国)

原文标题：使用 Windows Active Directory 组控制 vSpere 管理权限

原文链接：http://www.searchsv.com.cn/showcontent_23938.htm

解决在 Active Directory 环境里 Windows 登录性能问题

与性能相关的问题通常是最难解决的，主要由于要考虑许多变数。在本文中，TechTarget 中国的特约专家 Gary Olsen 介绍当用户登录到域账户时，如何诊断和解决登录性能缓慢的难题。

在解决任何性能问题时，你必须首先定义能接受的延迟范围。我见过一些环境，用户经历 5 到 10 分钟的登录时间也不抱怨，因为他们习惯了。我也见过其他情形，就算一分钟的延迟也是不可接受的。这就是为什么先要定义可接受范围的原因，以便你知道如何解决问题。

Windows 登录性能因素

当查找登录性能问题的原因时，考虑大量因素很重要。一些因素包括：

- 域控制器太接近用户
- 网络连接与可用的带宽
- 数据中心上的硬件资源（x64 vs.x86、内存等）
- 应用于用户和计算机的组策略（GPO，会直接影响带宽）数量
- 用户和计算机所在安全组的数量（也直接影响带宽）
- 需要额外处理时间的 GPO 包含设置，如：环回处理、WMI 过滤器和 ACL 过滤
- 繁重的载入域控制器由以下因素造成：需要认证的应用、来自用户脚本或应用的无效 LDAP 查询、宿主其他应用，如 Exchange、IIS、SQL Server 等的数据中心
- 客户端配置：内存、磁盘、处理器等、网络接口（10 个、100 或 1000 个）、到站点的合适子网映射和 DNS 配置

定义范围

为了定义问题的实际范围，我通常花时间询问简单的问题。这需要一些精力，因为这些问题通常由抱怨问题的用户定义。下面是需要询问的重要问题：

- 这些问题定义为单个站点、安全组、OU、部门、客户端的类型（笔记本还是桌面）还是操作系统？
- 问题在每天某个时刻发生吗？
- 当你在办公室或者跨 VPN 连接就发生问题吗？
- 描述症状：延迟每次发生在某个点吗？（例如发生在登录屏幕的“Network Settings”上）、在登录页面之前还是之后发生？
- 什么时候开始发生的？

工具和数据收集

我使用一些基本的工具收集数据。对于性能问题，我喜欢广撒网，收集所有能收集的信息。如下面例子：

在客户端和他们的验证数据中心运行微软产品支持报道（MPSreports）。这是个常用的工具，收集所有事件日志、MSINFO32、NetDiag、PConfig、驱动与 hotfixes 等的数据。Hewlett-Packard 自身也有叫做 HPS Reports 的版本，在我看来，它比微软的工具更高级，如果运行在数据中心上，可以收集具体的 Active Directory 数据。它也收集与硬件相关的多余信息，甚至不是 HP 的硬件也可以收集。

在客户端，使用 Microsoft KB article 221833 为 Winlogon 系统进程设置冗长的登录。这将在%Systemroot%\Debug\UserMode\Userenv.log 文件里提供精确的细节。注意，这个日志不包括数据日期，因此你必须：

1. 从客户端删除现有的 userenv.log
2. 启动 verbose 登录为每 KB 221833
3. 注销、登录并保存 userenv.log 到新地点，以在登录期间限制数据收集

注意，userenv.log 在下面的 GPO 和配置文件进程很精确，并且通常你能明显看见哪里发生了登陆延迟。

启用 Net Logon 登录。Netlogon 日志位于%systemroot%\debug，如果没有启用登录就是空的。例如，它会显示子网里的哪个客户端没有映射到站点。这会导致客户端在数据中心之外验证，需要的登录时间比预想的长。

运行来自 Sysinternals 的 Process Monitor。在启用启动日志上的 Help 部分查看细节。你能在缓慢启动期间捕获进程信息查看哪个处理器在影响性能。

解决客户端登录缓慢的其他技巧

你还能查看下面的一些事情，看是否由已知的问题导致登录性能。

首先，在客户端上检查 GPResult.exe 和 LOGONSERVER 环境变量，MPSreports 和 HPS Reports 将为已登录的用户收集 GPResult，它们不收集指向验证数据中心的 LOGONSERVER 变量。这很重要，因为每次用户登录，都会下载 GPO 到客户端。SYSVOL（包含 GPO）是 DFS 根，不服从客户端站点警告。相反，它以随机命令收集数据中心（宿主 SYVOL DFS 根），然后可以从列表里的第一个数据中心下载 GPO。

我遇到过这样的情况，在主服务站点的客户端将跨过缓慢的 WAN 连接到数据中心外，以获得 GPO，导致了非常缓慢的登录时间。由于这可能在每个登录上发生，所以这个问题是间歇性的。

为下载 GPO 的数据中心检查 GPResult，并查看 GPO 是否来自数据中心外面。同样，比较 LOGONSERVER 变量，查看客户端是否在数据中心外验证。使用已知的缓慢或繁忙连接，登录延迟能解释为“通常”行为。

另一个好测试是使用网络启动安全模式，查看是否发生延迟。如果没有，那么进行 Net Start 并列出所有启动的服务。然后以正常模式启动并运行 Net Start，再次列出所有服务。这个不同就能证明是哪个服务有嫌疑，一次消除一个能帮助你识别问题。你也能尝试禁止启动时开始的应用，查看该应用是否是原因所在。

最后一种技术是使用 Netmon、Wireshark 或其他网络捕获工具进行网络追踪。由于你尝试捕获登录进程，将 dumb hub 连接到网络线缆，然后从 hub 连接线缆到有问题的 PC，然后连接另一个线缆到安装了 Netmon 或 WireShark 的另一个 PC 或笔记本。在混合模式里运行捕获工具并复制登录。这样的设置将确保捕获工具收集客户端内外的流量，并消除网络噪声。

上面所述的是你要掌握的基础。只需要记住没有任何偷懒的情况——需要花费时间和精力找到问题。在下一篇文章里，我将介绍解决问题的一些方法。

(作者：Gary Olsen 译者：唐琼瑶　来源：TechTarget 中国)
原文标题：解决在 Active Directory 环境里 Windows 登录性能问题
原文链接：http://www.searchsv.com.cn/showcontent_29247.htm

在 Active Directory 管理里创建 taskpad view

组织越大，管理员管理整个 Active Directory 数据库就越难。Windows 允许你分配管理任务给其他管理员，你可以给他们指定一个执行管理任务的管理控制台。其中包括创建 taskpad。

taskpads 是管理控制台的一个要素，显示控制台结构的某部分，提供到各种管理功能的链接。

要创建 taskpads，你必须打开 Microsoft Management Console（MMC）里的 Active Directory Users 和 Computers snap-in，因为直接打开是不起作用的。在服务器的 Run 提示符里输入 MMC 命令，从文件菜单选择 Add / Remove Snap-In 命令。当 Windows 在对话框显示 Add / Remove Snap-In，点击 Add 按钮，然后从 snap-ins 列表的 Active Directory Users and Computers 选项选择 Active Directory Users and Computers。点击 Add，然后点击 Close 和 OK。

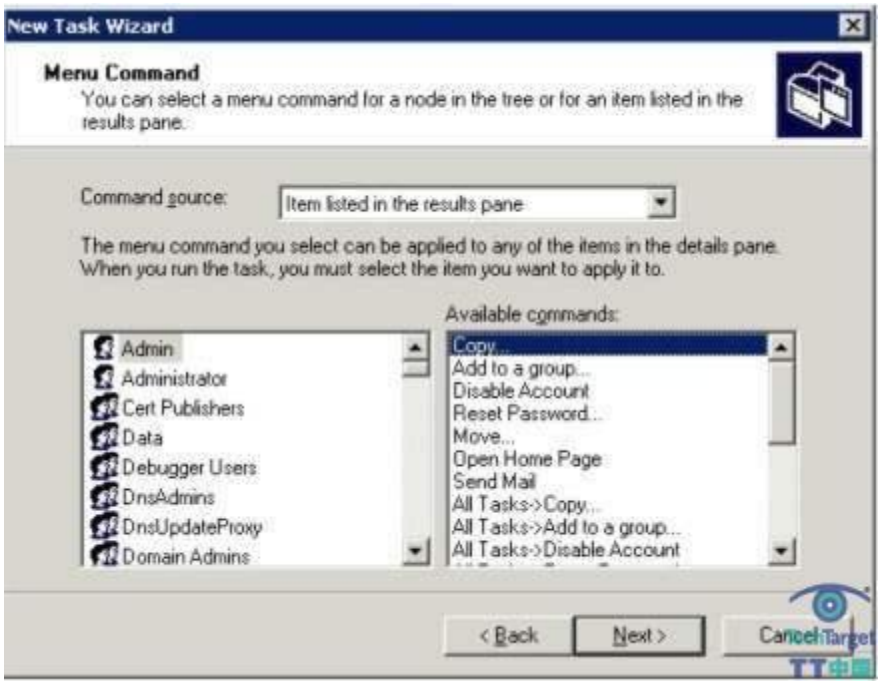
既然必要的 snap-in 已经添加到控制台，展开 Active Directory Users 和 Computers container，并选择你想要宿主 taskpad 的容器。右击容器，并从 resulting shortcut 菜单选择 New Taskpad View 命令。Windows 将启动 New Taskpad View Wizard。

点击 Next 绕开向导的欢迎界面，将出现询问你使用何种类型的界面。你可以创建水平列表、垂直列表，或者不选。我推荐使用默认设置并点击 Next。

下一屏将询问 taskpad view 属于当前结构还是这个类型所有条目。我再次推荐使用默认设置并点击 Next。

然后需要为 taskpad 输入名称和描述。如果你的 taskpad 基于一个组织机构，那么向导将使用这个机构的名称作为 taskpad 的名称。

点击 Next 和 Finish 创建新的 taskpad view。当向导完成后， Windows 将自动启动新的 New Task Wizard。确保选择 Menu Command，点击 Next。参见图 A：



左列包含用户列表，右列包含可用的命令列表。值得注意的是，给用户一个可用命令不是给他或她执行这个命令的权限。

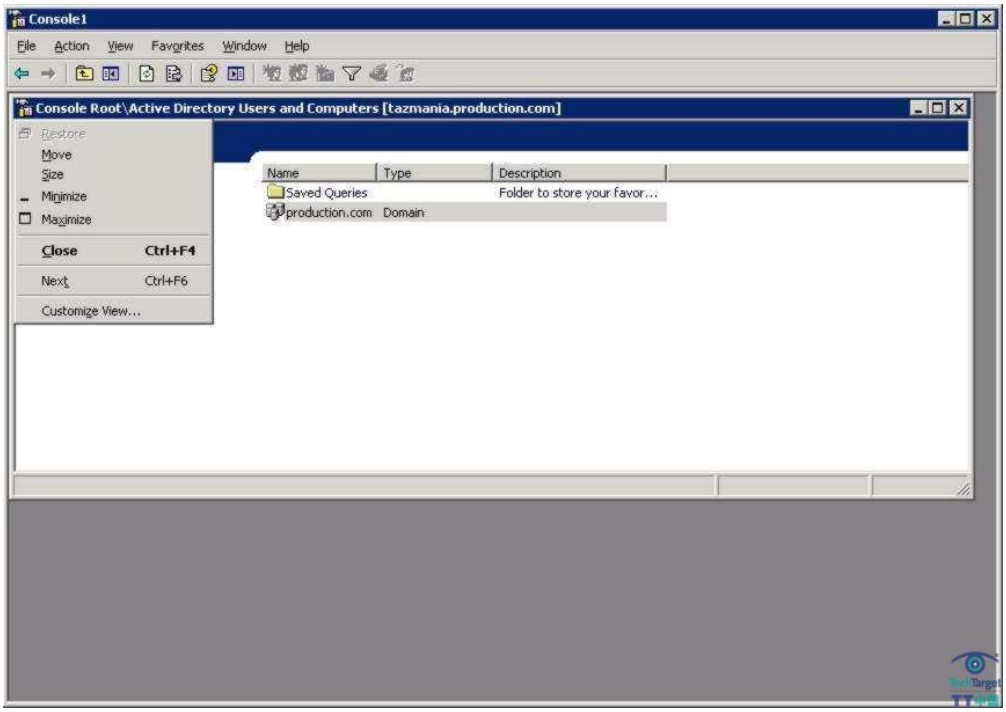
选择一个用户账户和一个命令，点击 Next。属于你输入你创建的命令的名称和描述。这些选项都是默认的，因此你可以直接到下一屏。

你现在必须选择代表任务的图标。你能使用向导所显示的某个图标或者提供自定义图标。选好后点击 Next。

这时候，你能看见关于你创建的命令的描述。点击 Finish 完成向导。如果想往 taskpad 里添加额外的命令，那么在完成之前选择 When I Finish Run This Wizard Again 对话框。

锁定控制台

创建好 taskpad view 后，你需要配置控制台。点击（工具栏下面的）控制台图标，选择 resulting 菜单上的 Customize View，参见图 B。然后移除你不想通过控制台访问的任务。



移除后，从 File 菜单选择 Save As 命令，保存自定义控制台。

记住，只是移除控制台选项是不够的。控制台的主要工作是通过移除任何不被允许的功能选项使得管理任务更容易。还是要依靠你以某种方式分配控制权限，在阻止任务时允许其他人执行管理动作。

(作者：Brien M. Posey 译者：唐琼瑶　来源：TechTarget 中国)

原文标题：在 Active Directory 管理里创建 taskpad view

原文链接：http://www.searchsv.com.cn/showcontent_28801.htm