



中国矿业大学计算机学院

2019 级本科生课程作业

课程名称 操作系统安全——作业一

报告时间 2022 年 5 月 1 日

学生姓名 许万鹏

学 号 05191643

专 业 信息安全

任课教师 张爱娟



目 录

1	作业环境	1
2	配置 Active Directory	1
2.1	Server-No1	1
2.2	Server-No2	11
2.3	Server-No3	21
2.4	一次尝试：使用 Windows Admin Center 配置 AD	30
3	创建用户	34
4	登录客户机	41
4.1	配置	41
4.2	登录 xuwp-No1	45
4.3	登录 xuwp-No2	47
4.4	登录 xuwp-No3	48
5	共享资源	52
5.1	设置共享文件夹	52
5.2	查看共享文件夹	57
6	作业展示截图	65
6.1	域和信任关系的展示截图	65
6.2	连通性测试截图	67
6.3	林中不同域计算机用户登录客户机的截图	71
6.4	可查询共享资源截图	72



1 作业环境

服务器:

Windows Server 2022: Server-No1

Windows Server 2022: Server-No2

Windows Server 2022: Server-No3

客户端:

Windows 10 1909: Client-No1

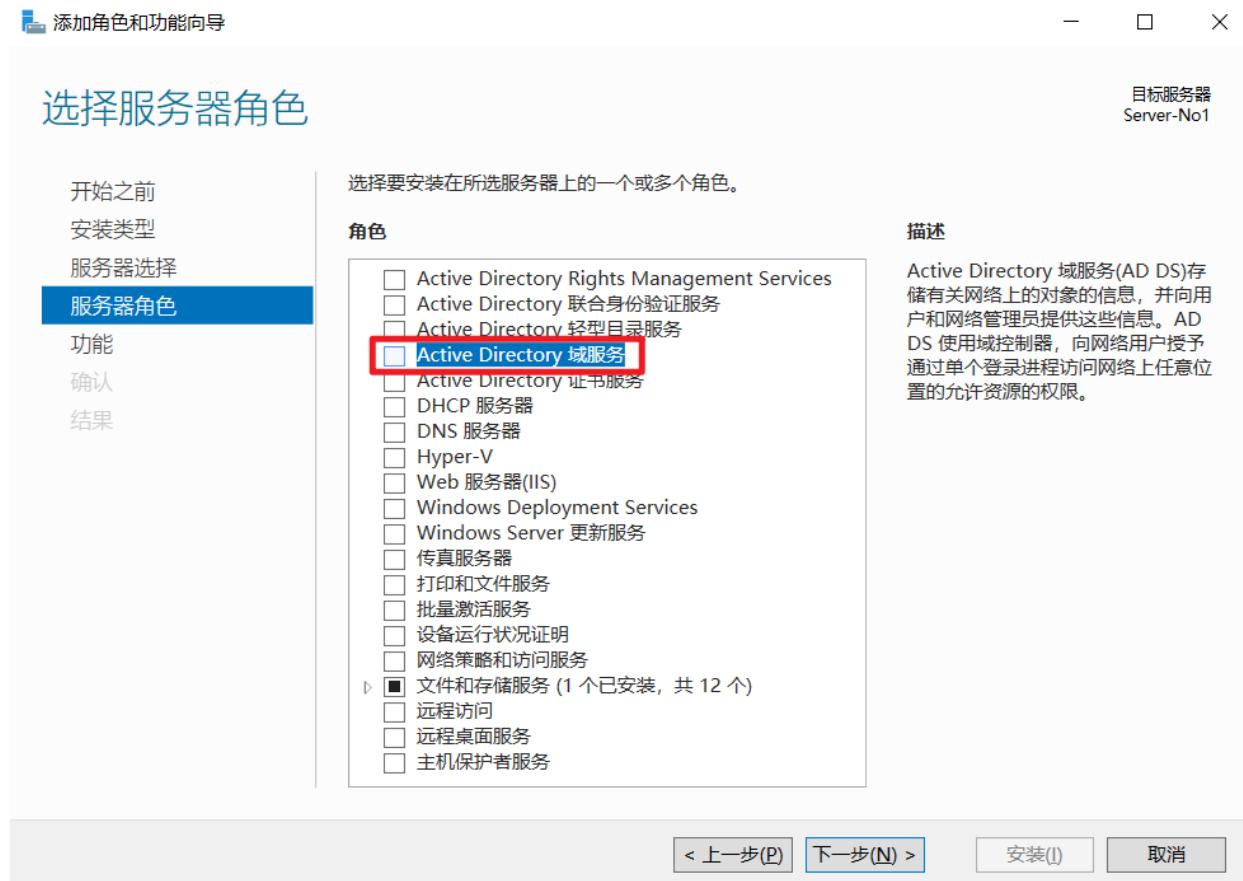
2 配置 Active Directory

2.1 Server-No1

2.1.1 安装

进入 Windows Server Manager，点击“添加角色和功能”。

连续“下一步”，直到到达“服务器角色”。



选中“Active Directory 域服务”。



添加角色和功能向导 X

添加 Active Directory 域服务 所需的功能?

只有在安装了以下角色服务或功能的前提下，才能安装 Active Directory 域服务。

- ▲ 远程服务器管理工具
- ▲ 角色管理工具
- ▲ AD DS 和 AD LDS 工具
 - Windows PowerShell 的 Active Directory 模块
- ▲ AD DS 工具
 - [工具] Active Directory 管理中心
 - [工具] AD DS 管理单元和命令行工具
 - [工具] 组策略管理

包括管理工具(如果适用)

添加功能 取消

点击“添加功能”。

点击“下一步”，可以看到 AD DS 的说明。



添加角色和功能向导

- □ ×

Active Directory 域服务

目标服务器
Server-No1

开始之前
安装类型
服务器选择
服务器角色
功能
AD DS
确认
结果

Active Directory 域服务(AD DS)存储有关网络上的用户、计算机和其他设备的信息。AD DS 有助于管理员安全地管理该信息，并有助于用户间的资源共享和协作。

注意事项:

- 若要有助于确保在某台服务器中断的情况下用户仍然可以登录到网络，请至少为域安装两个域控制器。
- AD DS 要求将 DNS 服务器安装在网络上。如果未安装 DNS 服务器，系统会提示你在该计算机上安装 DNS 服务器角色。



Azure Active Directory 是一个单独的在线服务，可以提供简化的标识和访问管理、安全报告，并允许通过单一登录登录到云和本地的 Web 应用。

[了解有关 Azure Active Directory 的详细信息](#)

[为 Office 365 配置 Azure Active Directory Connect](#)

< 上一步(P) 下一步(N) >

安装(I)

取消

连续“下一步”。



添加角色和功能向导

安装进度

目标服务器
Server-No1

开始之前
安装类型
服务器选择
服务器角色
功能
AD DS
确认
结果

查看安装进度

功能安装

需要配置。已在 Server-No1 上安装成功。

Active Directory 域服务
使此计算机成为域控制器需要执行其他步骤。
将此服务器提升为域控制器

远程服务器管理工具
角色管理工具
AD DS 和 AD LDS 工具
Windows PowerShell 的 Active Directory 模块
AD DS 工具
Active Directory 管理中心
AD DS 管理单元和命令行工具

组策略管理

你可以关闭此向导而不中断正在运行的任务。请依次单击命令栏中的“通知”和“任务详细信息”，以查看任务进度或再次打开此页面。

导出配置设置

< 上一步(P) 下一步(N) > 关闭 取消

点击“将此服务器提升为域控制器”，当然也可以以后配置。

这些可视化的点击步骤也可以导出为 XML 文件，此后使用 PowerShell 安装。

导出配置设置

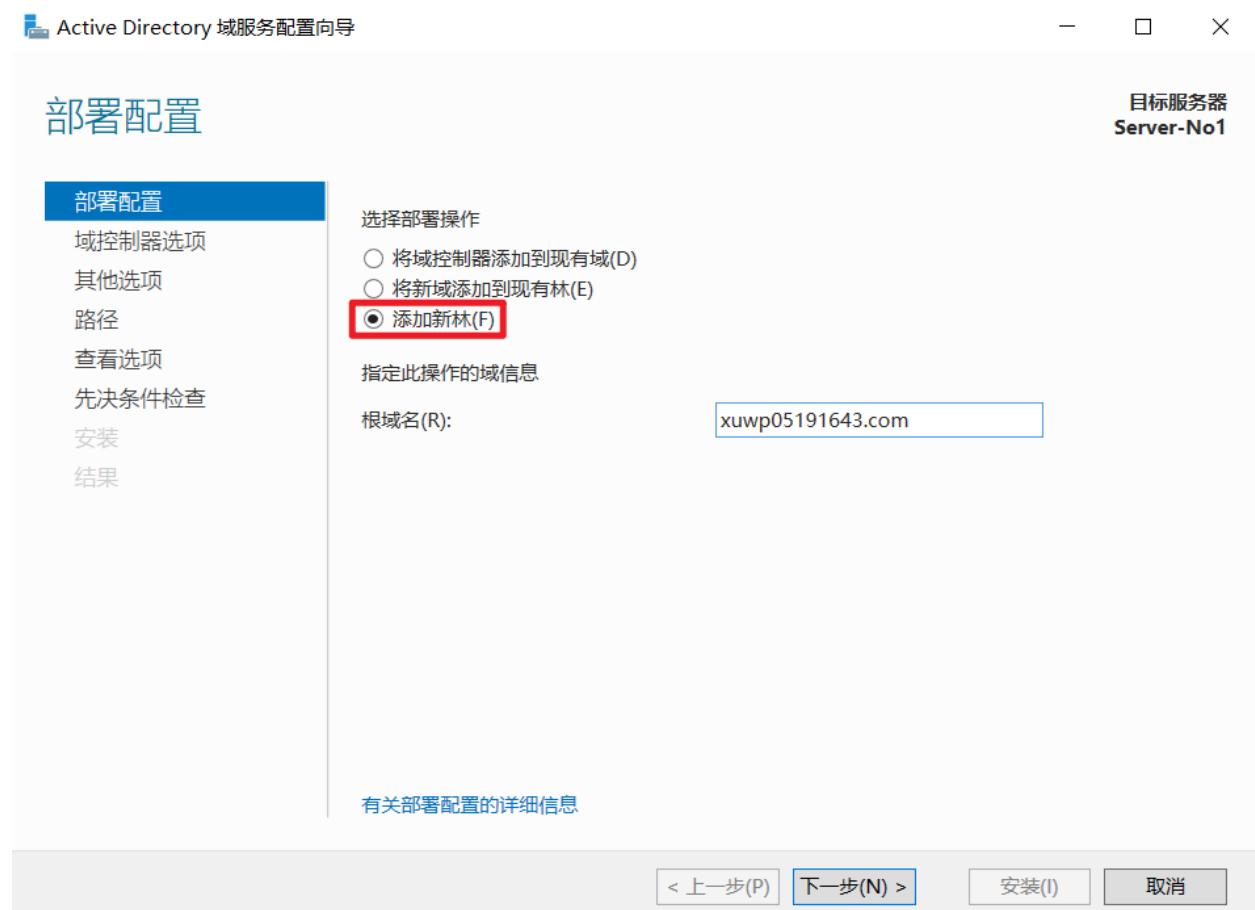
将配置设置和安装选项导出到 XML 文件。

Windows PowerShell 中的用法:
Install-WindowsFeature -ConfigurationFilePath <ExportedConfig.xml>

这样，你就可以在其他服务器上自动完成相同的安装。



2.1.2 配置



点击“添加新林”，输入根域名为“xuwp05191643.com”。

点击“下一步”



Active Directory 域服务配置向导

域控制器选项

目标服务器
Server-No1

部署配置

域控制器选项

DNS 选项

其他选项

路径

查看选项

先决条件检查

安装

结果

选择新林和根域的功能级别

林功能级别: Windows Server 2016

域功能级别: Windows Server 2016

指定域控制器功能

域名系统(DNS)服务器(O)

全局编录(GC)(G)

只读域控制器(RODC)(R)

键入目录服务还原模式(DSRM)密码

密码(D):

确认密码(C):

有关域控制器选项的详细信息

< 上一步(P) 下一步(N) > 安装(I) 取消

在这里输入 DSRM 密码，点击“下一步”。

注：这里的林/域功能级别最高就是 Windows Server 2016。

连续“下一步”，全部使用默认值。



Active Directory 域服务配置向导

查看选项

目标服务器
Server-No1

部署配置
域控制器选项
DNS 选项
其他选项
路径
查看选项
先决条件检查
安装
结果

检查你的选择:
将该服务器配置为新林中的第一个 Active Directory 域控制器。
新域名为“xuwp05191643.com”。这也是新林的名称。
该域的 NetBIOS 名称: XUWP05191643
林功能级别: Windows Server 2016
域功能级别: Windows Server 2016
其他选项:
全局编录: 是
DNS 服务器: 是
创建 DNS 委派: 否
数据库文件夹: C:\Windows\NTDS

可以将这些设置导出到 Windows PowerShell 脚本以自动执行其他安装 [查看脚本\(V\)](#)

[有关安装选项的详细信息](#)

< 上一步(P) [下一步\(N\) >](#) 安装(I) 取消

我们需要留意的是这个界面，我们可以通过和此后两个服务器对比这个界面来明确概念。

这里可以生成 Power Shell 脚本

```
config_Server_No1
#
# 用于 AD DS 部署的 Windows PowerShell 脚本
#
Import-Module ADDSDeployment
Install-ADDSForest
-CreateDnsDelegation:$false
-DatabasePath "C:\Windows\NTDS"
-DomainMode "WinThreshold"
-DomainName "xuwp05191643.com"
-DomainNetbiosName "XUWP05191643"
-ForestMode "WinThreshold"
-InstallDns:$true
-LogPath "C:\Windows\NTDS"
-NoRebootOnCompletion:$false
-SysvolPath "C:\Windows\SYSVOL"
```



-Force:\$true

config_Server_No1

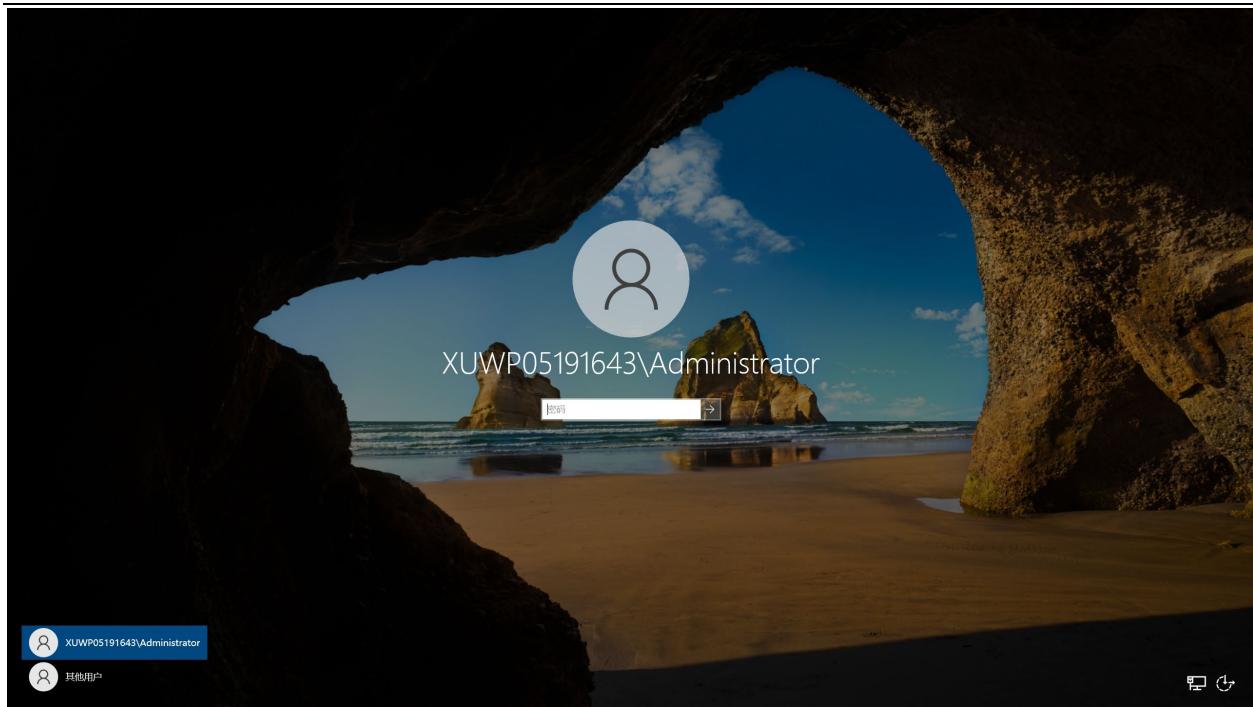
点击“下一步”。



点击“下一步”。



点击“关闭”，等待重启。



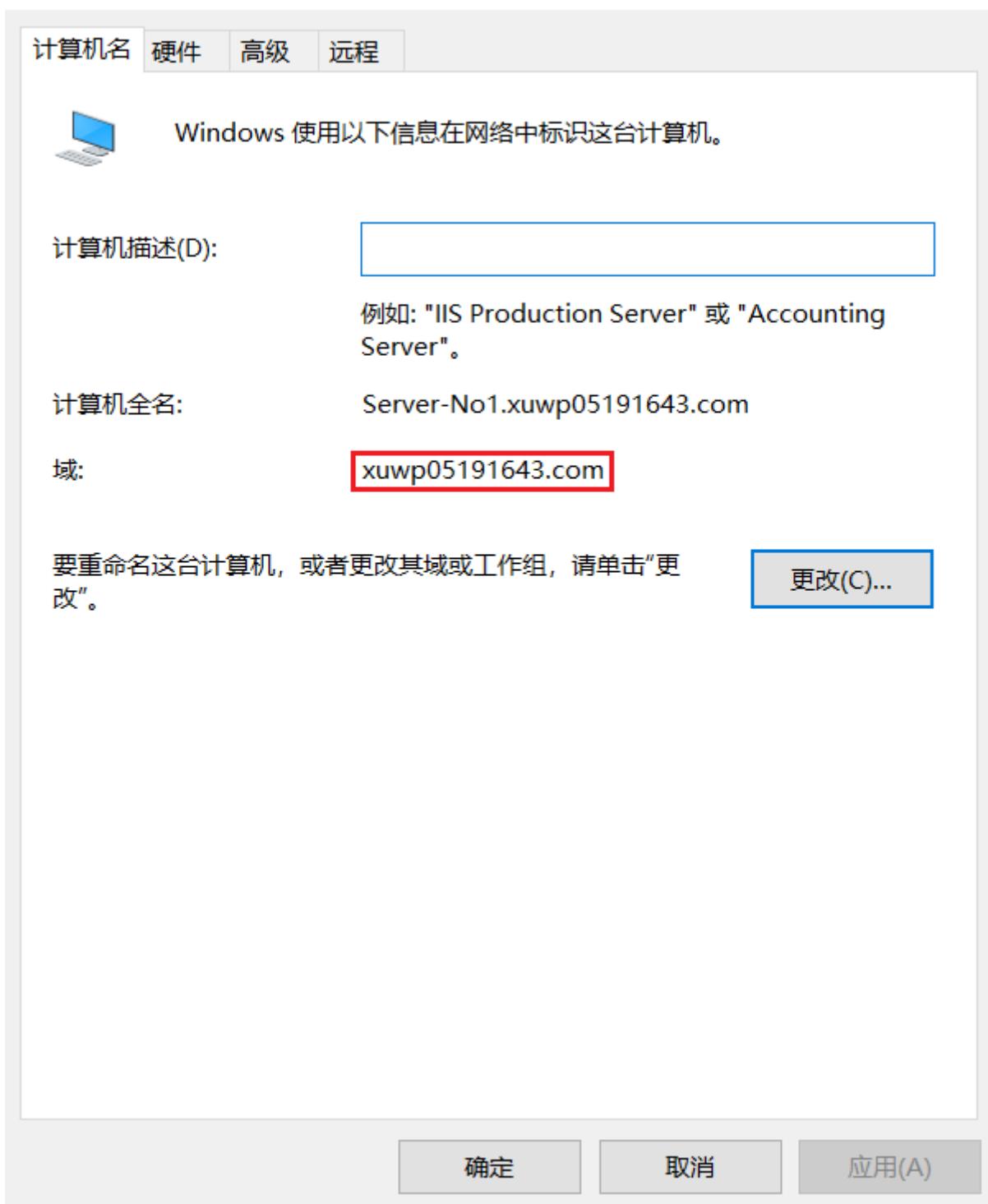
可以发现我们的 Administrator 用户前面增加了域“XUWP05191643”。

进入系统后，查看系统属性。



系统属性

X



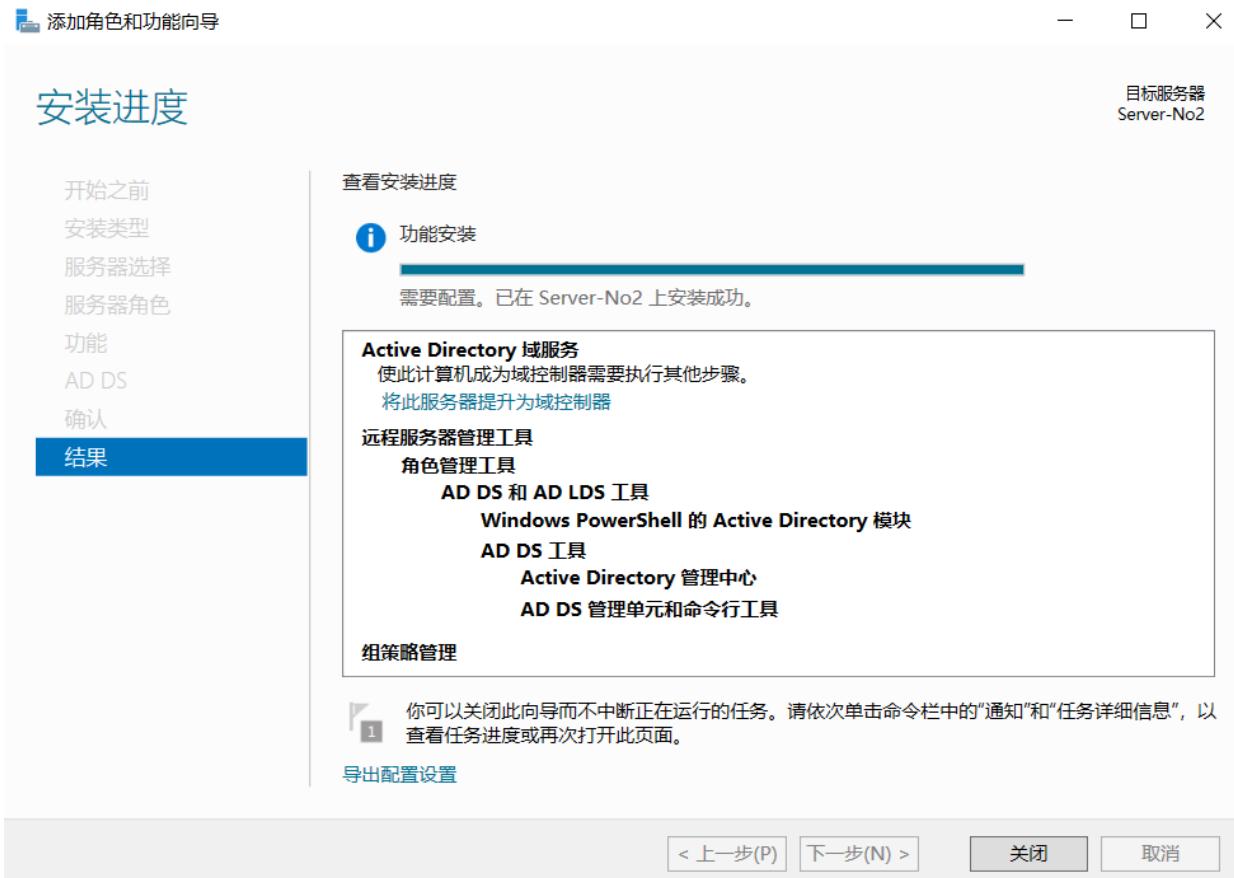
这表明成功创建了父域 xuwp05191643.com，同时服务器 Server-No1 属于 xuwp05191643.com



2.2 Server-No2

2.2.1 安装

同 Server-No1



点击“将此服务器提升为域控制器”。

2.2.2 配置

“将新域添加到现有林” - “更改”。



Active Directory 域服务配置向导

部署配置

目标服务器
Server-No2

部署配置

域控制器选项

其他选项

路径

查看选项

先决条件检查

安装

结果

选择部署操作

将域控制器添加到现有域(D)

将新域添加到现有林(E)

添加新林(F)

指定此操作的域信息

选择域类型(T): 子域

父域名(M): * 选择(S)...

新域名(W): *

提供执行此操作所需的凭据

<未提供凭据> 更改(C)...

有关部署配置的详细信息

< 上一步(P) 下一步(N) > 安装(I) 取消

输入父域的账号密码

Windows 安全中心

X

部署操作的凭据

为此部署操作提供凭据

XUWP05191643\Administrator

*****|



确定

取消

但是发现无法连接，点击“查看详细信息”看一下原因。



计算机名/域更改

×



无法与域“xuwp05191643.com”的 Active Directory 域控制器
(AD DC)连接。

确定

请确保键入的域名正确。

<< 详细信息(D)

如果名称正确, 请单击“详细信息”了解疑难解答信息。

此错误的常见原因包括:

- 查找此域的 AD DC 所需的 DNS SRV 记录未在 DNS 中注册。向域中添加 AD DC 时, 会自动通过 DNS 服务器注册这些记录。AD DC 将根据设置的时间间隔对其进行更新。此计算机配置为使用如下 IP 地址的 DNS 服务器:

192.168.36.2

- 下列一个或多个区域未包括对其子区域的委派:

xuwp05191643.com
com
. (根目录区域)

原来是 DNS 服务器找不到父域, 那直接把 DNS 服务器改成父域的服务器就好了。

我们把 Server-No2 的 DNS 服务器改成 Server-No1。

先设置 Server-No1 的 IP 和 DNS。



Internet 协议版本 4 (TCP/IPv4) 属性

X

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

 自动获得 IP 地址(O) 使用下面的 IP 地址(S):

IP 地址(I):

192 . 168 . 36 . 128

子网掩码(U):

255 . 255 . 255 . 0

默认网关(D):

. . .

 自动获得 DNS 服务器地址(B) 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

192 . 168 . 36 . 128

备用 DNS 服务器(A):

. . .

 退出时验证设置(L)

高级(V)...

确定

取消

然后把 Server-No2 的 DNS 服务器改成 Server-No1。



Internet 协议版本 4 (TCP/IPv4) 属性

X

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

 自动获得 IP 地址(O) 使用下面的 IP 地址(S):

IP 地址(I):

192 . 168 . 36 . 129

子网掩码(U):

255 . 255 . 255 . 0

默认网关(D):

192 . 168 . 36 . 2

 自动获得 DNS 服务器地址(B) 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

192 . 168 . 36 . 128

备用 DNS 服务器(A):

. . .

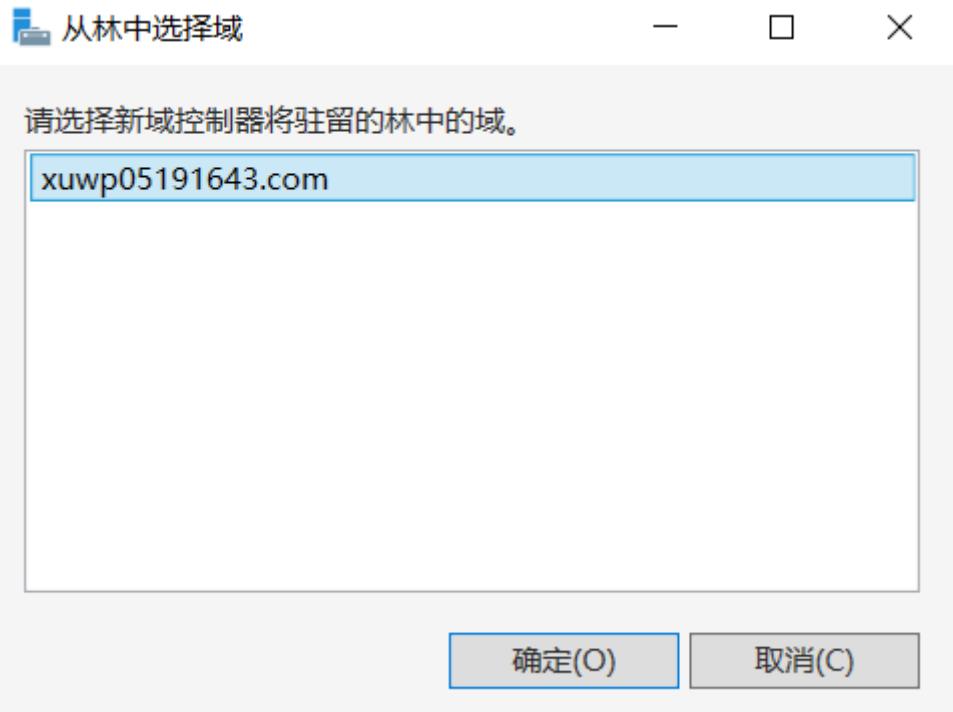
 退出时验证设置(L)

高级(V)...

确定

取消

点击“选择”，发现这次能搜索到了。



选择“xuwp05191643.com”（父域） - “确定”。

将新域名设置为 a

Active Directory 域服务配置向导

部署配置 目标服务器
Server-No2

部署配置

域控制器选项

其他选项

路径

查看选项

先决条件检查

安装

结果

选择部署操作

将域控制器添加到现有域(D)
 将新域添加到现有林(E)
 添加新林(F)

指定此操作的域信息

选择域类型(T): 子域

父域名(M): xuwp05191643.com 选择(S)...

新域名(W): a

提供执行此操作所需的凭据

XUWP05191643\Administrator 更改(C)...

有关部署配置的详细信息

< 上一步(P) 下一步(N) > 安装(I) 取消



连续“下一步”，直到“查看选项”。

部署配置
域控制器选项
DNS 选项
其他选项
路径
查看选项
先决条件检查
安装
结果

目标服务器
Server-No2

检查你的选择:
将此服务器配置为新子域中的第一个 Active Directory 域控制器。

新域名: a
该域的 NetBIOS 名称: A
该新域是以下域的子域: xuwp05191643.com
域功能级别: Windows Server 2016
站点名称: Default-First-Site-Name
其他选项:
全局编录: 是
DNS 服务器: 是
创建 DNS 委派: 是

可以将这些设置导出到 Windows PowerShell 脚本以自动执行其他安装 **查看脚本(V)**

有关安装选项的详细信息

< 上一步(P) **下一步(N) >** 安装(I) 取消

a.xuwp05191643.com 的 PowerShell 脚本。

config_Server_No2

```
#  
# 用于 AD DS 部署的 Windows PowerShell 脚本  
#  
  
Import-Module ADDSDeployment  
Install-ADDSDomain  
-NoGlobalCatalog:$false  
-CreateDnsDelegation:$true  
-Credential (Get-Credential)  
-DatabasePath "C:\Windows\NTDS"  
-DomainMode "WinThreshold"  
-DomainType "ChildDomain"  
-InstallDns:$true  
-LogPath "C:\Windows\NTDS"  
-NewDomainName "a"  
-NewDomainNetbiosName "A"  
-ParentDomainName "xuwp05191643.com"
```



```
-NoRebootOnCompletion:$false  
-SiteName "Default-First-Site-Name"  
-SysvolPath "C:\Windows\SYSVOL"  
-Force:$true
```

———— config_Server_No2

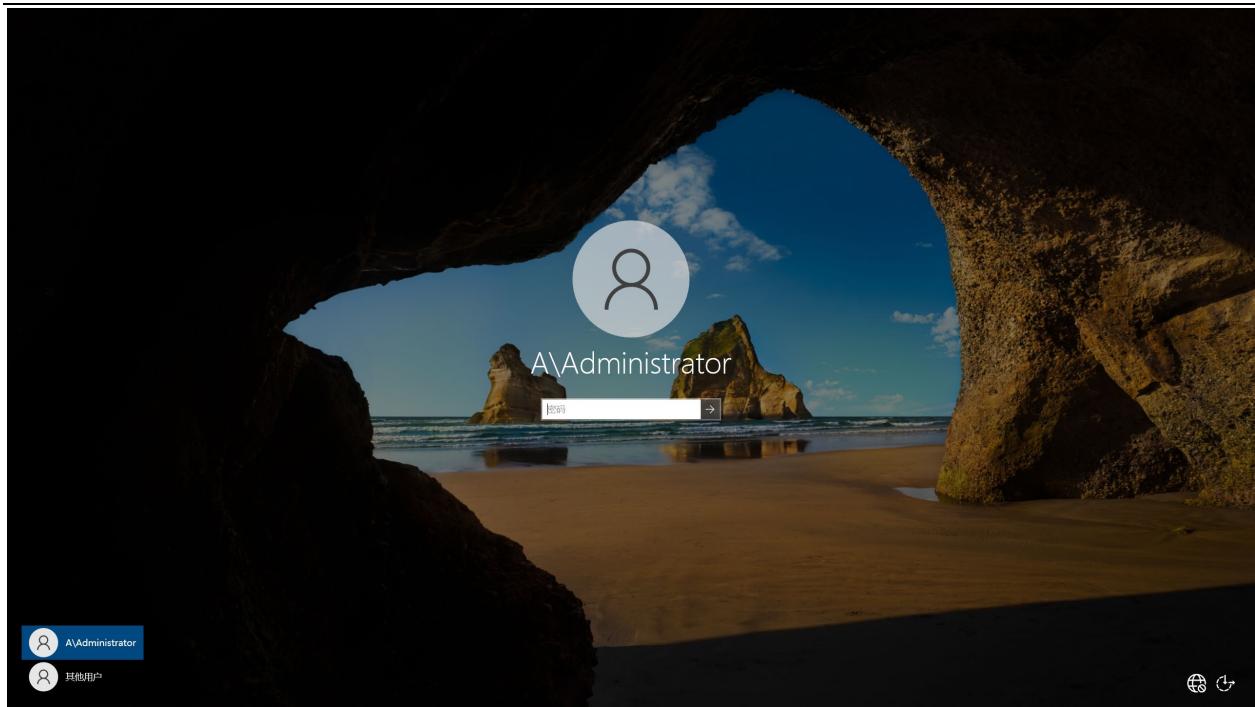
点击“下一步”。



点击“下一步”。



点击“关闭”，等待重启。

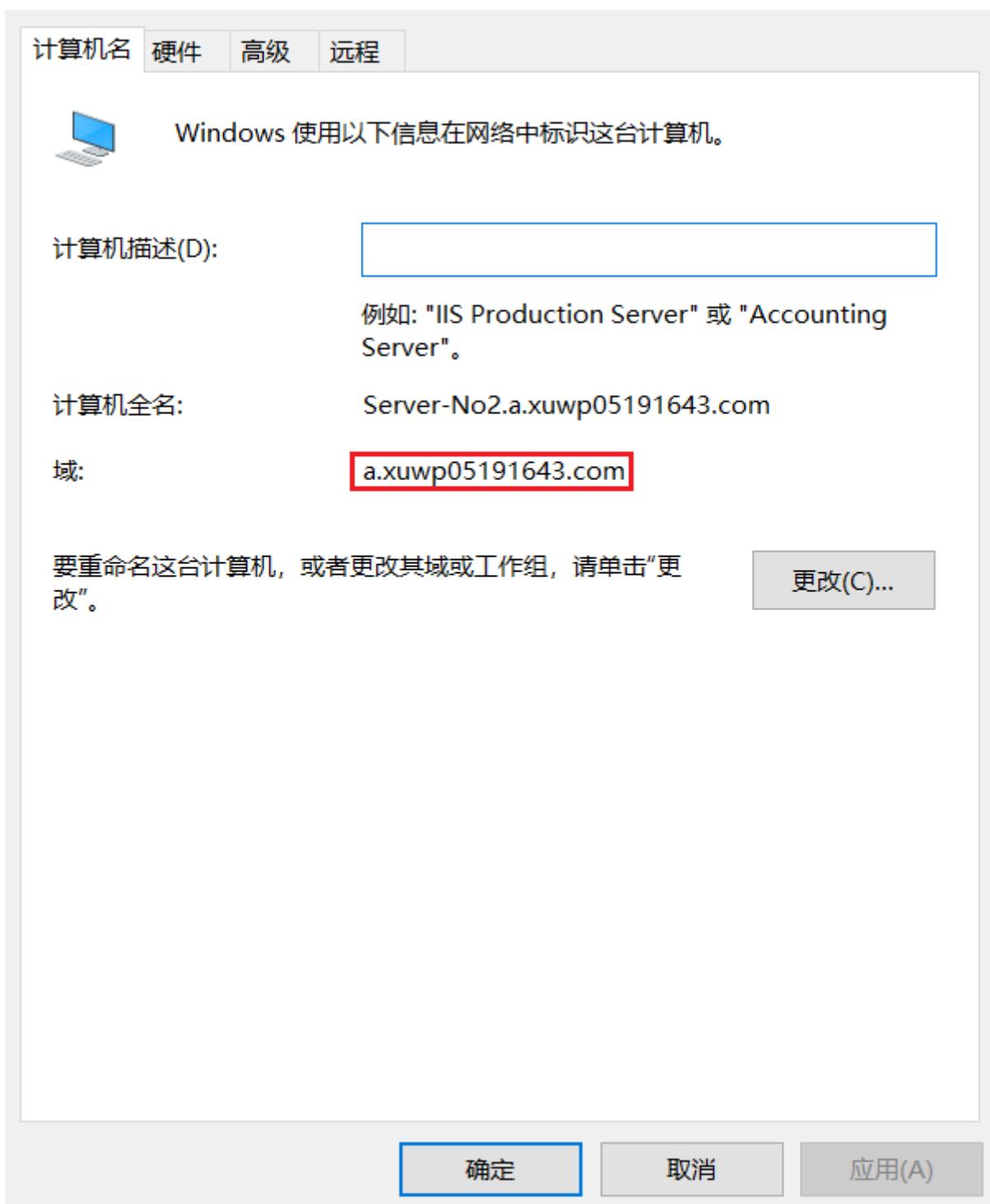


基本上可以看出来配置 AD 成功了，再看一下系统属性。



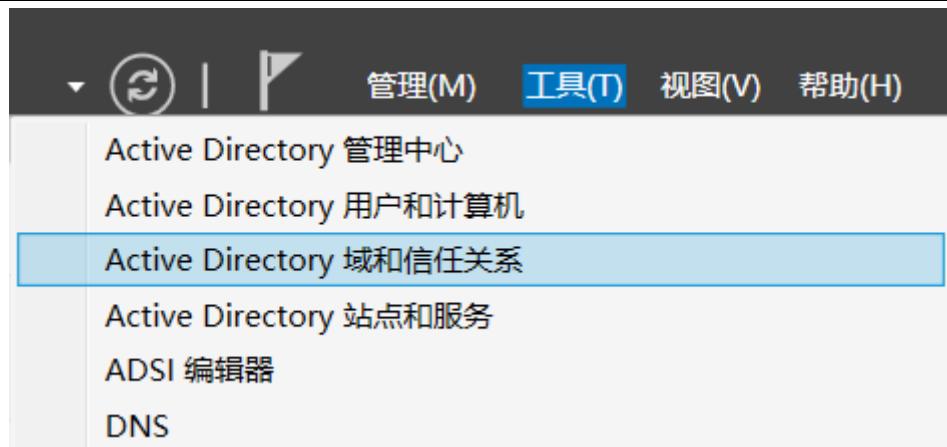
系统属性

X



这表明成功创建了 xuwp05191643.com 的子域 a.xuwp05191643.com，同时服务器 Server-No2 属于 a.xuwp05191643.com。

查看一下目前的 AD 域。



点击“Active Directory 域和信任关系”

This screenshot shows the 'Active Directory 域和信任关系' (Active Directory Domains and Trust Relationships) console window. The title bar reads 'Active Directory 域和信任关系 [Server-No1.xuwp05191643.com]'. The left pane shows a tree structure with 'xuwp05191643.com' expanded, showing its sub-node 'a.xuwp05191643.com'. The right pane displays a table with one row:

名称	类型	操作
xuwp05191643.com	domainDNS	Active Directory 域和信任关系 [Server-No1.xuwp05191643.com] 更多操作

在 Server-No2 中查看也是同样的结果，符合预期，配置完成。

2.3 Server-No3

2.3.1 安装

略

2.3.2 配置

这次我们先修改 DNS



Internet 协议版本 4 (TCP/IPv4) 属性

X

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

 自动获得 IP 地址(O) 使用下面的 IP 地址(S):

IP 地址(I):

192 . 168 . 36 . 130

子网掩码(U):

255 . 255 . 255 . 0

默认网关(D):

. . .

 自动获得 DNS 服务器地址(B) 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

192 . 168 . 36 . 128

备用 DNS 服务器(A):

. . .

 退出时验证设置(L)

高级(V)...

确定

取消

点击“将此服务器提升为域控制器”后出现配置向导。



Active Directory 域服务配置向导

部署配置

目标服务器
Server-No3

部署配置

域控制器选项

DNS 选项

其他选项

路径

查看选项

先决条件检查

安装

结果

选择部署操作

将域控制器添加到现有域(D)

将新域添加到现有林(E)

添加新林(F)

指定此操作的域信息

选择域类型(T): 树域

林名称(M): xuwp05191643.com

新域名(W): xuwp05191643.org

提供执行此操作所需的凭据

XUWP05191643\Administrator

更改(C)...

有关部署配置的详细信息

< 上一步(P) 下一步(N) > 安装(I) 取消

点击“将新域添加到现有林” - “树域”。

“更改”处仍使用xuwp05191643.com的凭据。

连续“下一步”，直到“其他选项”。



Active Directory 域服务配置向导

其他选项

目标服务器
Server-No3

NetBIOS 域名的默认值已使用，建议了一个备用值。

部署配置 确保为域分配了 NetBIOS 名称，并在必要时更改该名称

域控制器选项

DNS 选项

其他选项

路径

查看选项

先决条件检查

安装

结果

有关其他选项的详细信息

< 上一步(P) 下一步(N) > 安装(I) 取消

这里的 NetBIOS 域名和 xuwp05191643.com 的 NetBIOS 域名重复了，所以向导在后面加了个 0 (这里最好还是换个名字，因为改起来很麻烦)。

连续“下一步”，直到“查看选项”。



Active Directory 域服务配置向导

查看选项

目标服务器
Server-No3

部署配置
域控制器选项
DNS 选项
其他选项
路径
查看选项
先决条件检查
安装
结果

检查你的选择:
将该服务器配置为新域树中的第一个 Active Directory 域控制器。
新域的名称: xuwp05191643.org
该域的 NetBIOS 名称: XUWP051916430
新域与以下域具有信任链接: xuwp05191643.com
域功能级别: Windows Server 2016
站点名称: Default-First-Site-Name
其他选项:
全局编录: 是
DNS 服务器: 是
创建 DNS 委派: 否

可以将这些设置导出到 Windows PowerShell 脚本以自动执行其他安装 [查看脚本\(V\)](#)

有关安装选项的详细信息

< 上一步(P) [下一步\(N\) >](#) 安装(I) 取消

xuwp05191643.org 的 PowerShell 脚本。

config_Server_No3

```
#  
# 用于 AD DS 部署的 Windows PowerShell 脚本  
#  
  
Import-Module ADDSDeployment  
Install-ADDSDomain  
-NoGlobalCatalog:$false  
-CreateDnsDelegation:$false  
-Credential (Get-Credential)  
-DatabasePath "C:\Windows\NTDS"  
-DomainMode "WinThreshold"  
-DomainType "TreeDomain"  
-InstallDns:$true  
-LogPath "C:\Windows\NTDS"  
-NewDomainName "xuwp05191643.org"  
-NewDomainNetbiosName "XUWP051916430"  
-ParentDomainName "xuwp05191643.com"  
-NoRebootOnCompletion:$false
```



```
-SiteName "Default-First-Site-Name"
-SysvolPath "C:\Windows\SYSVOL"
-Force:$true
```

config_Server_No3

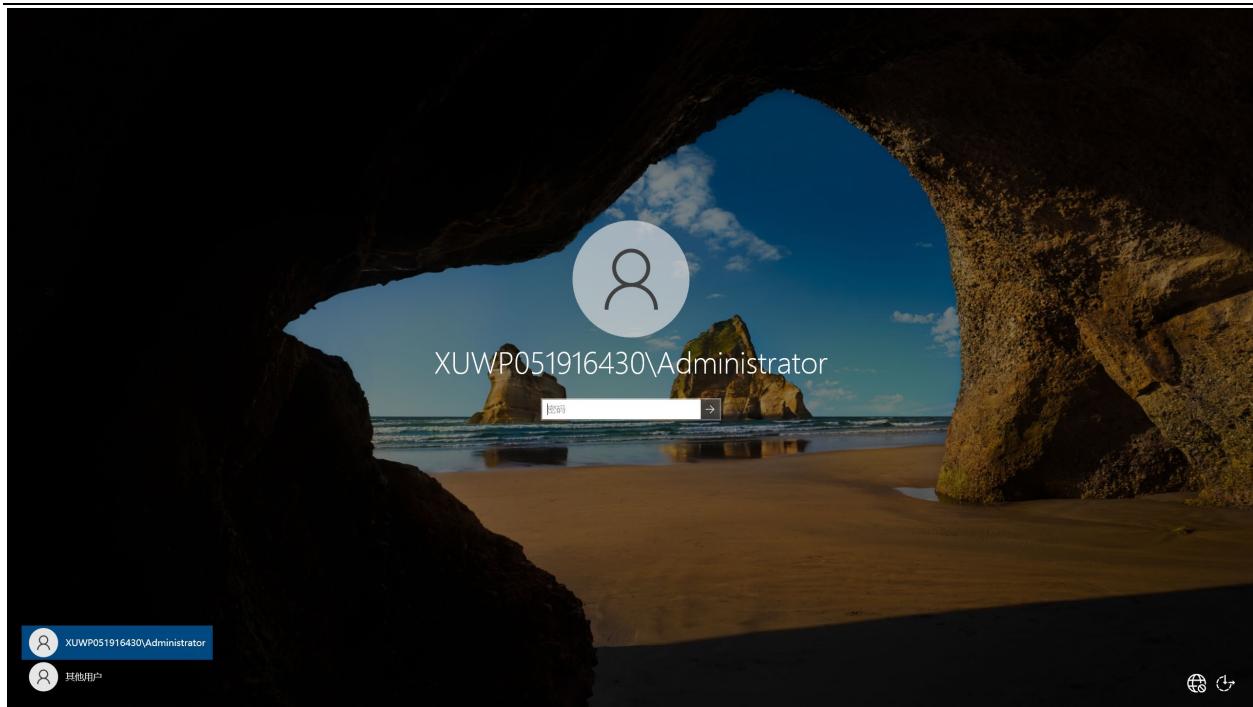
点击“下一步”。



点击“安装”。



点击“关闭”，等待重启。

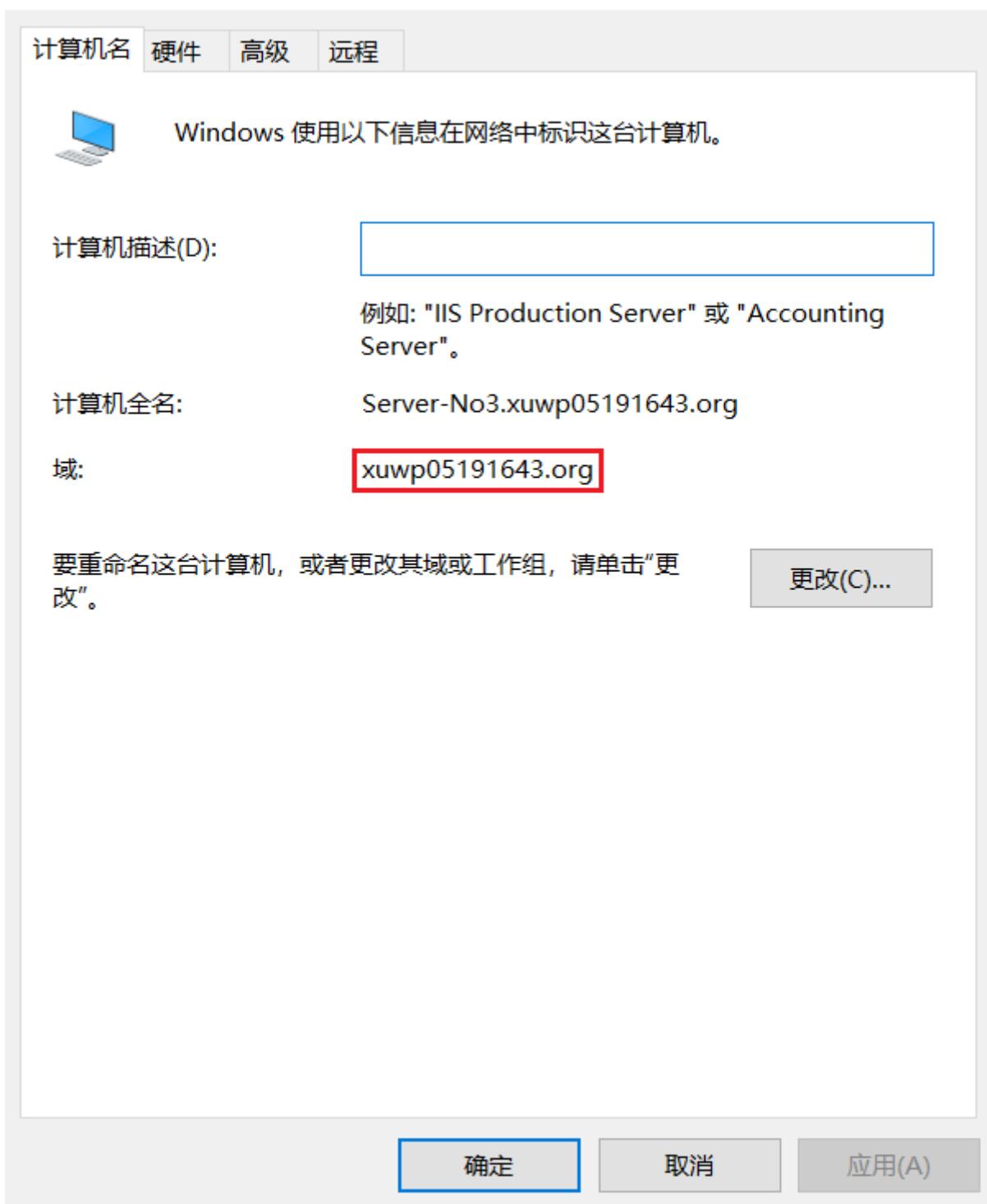


登录界面



系统属性

X



系统属性



《操作系统安全》作业一

The screenshot shows the Windows Server Management Console for Active Directory. The title bar reads "Active Directory 域和信任关系 [Server-No1.xuwp05191643.com]". The left pane displays a tree view with the root node "xuwp05191643.com" expanded, showing its child nodes "a.xuwp05191643.com" and "xuwp05191643.org". The right pane is a table with three columns: "名称" (Name), "类型" (Type), and "操作" (Operations). It lists two entries: "xuwp05191643.com" (domainDNS) and "xuwp05191643.org" (domainDNS). A "更多操作" (More Operations) button is located at the bottom of the table.

名称	类型	操作
xuwp05191643.com	domainDNS	Active Directory 域和信任关系 [Server-No1.xuwp05191643.com]
xuwp05191643.org	domainDNS	更多操作

AD 域和信任关系。

查看一下 xuwp05191643.com 的属性。



xuwp05191643.com 属性

常规 信任 管理者

受此域信任的域(外向信任)(M):

域名	信任类型	可传递
a.xuwp05191643.com	子	是
xuwp05191643.org	树根	是

属性(P)...
删除(R)

信任此域的域(内向信任)(O):

域名	信任类型	可传递
a.xuwp05191643.com	子	是
xuwp05191643.org	树根	是

属性(T)...
删除(V)

新建信任(N)...

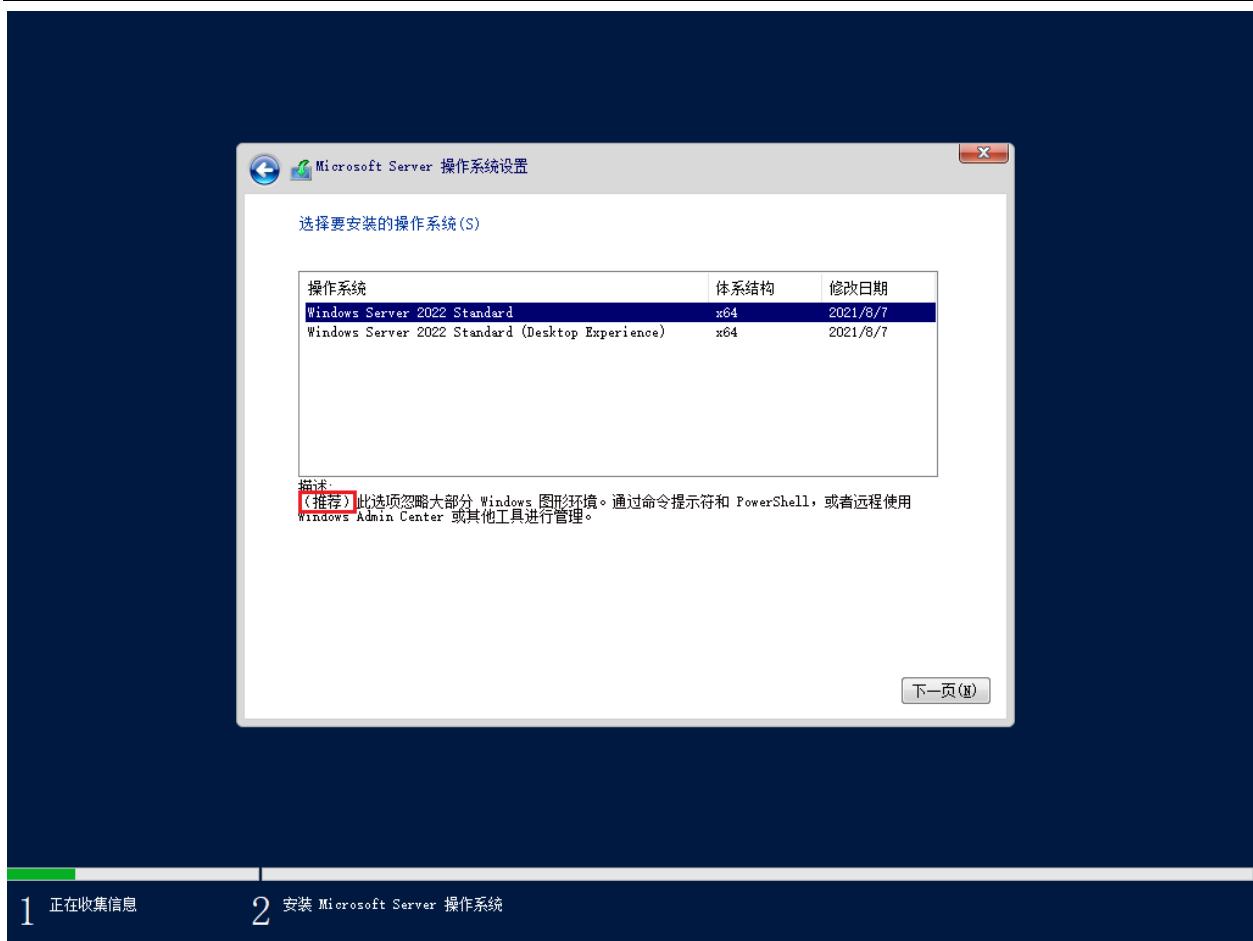
确定 取消 应用(A) 帮助

配置完成。

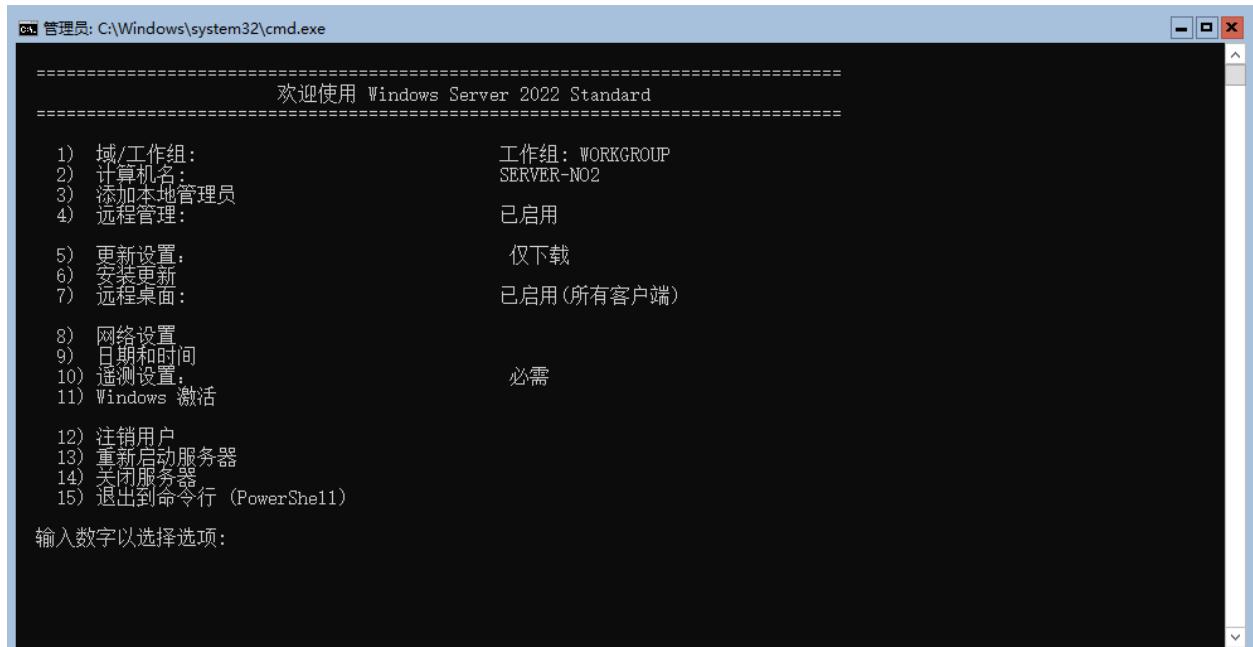
2.4一次尝试：使用 Windows Admin Center 配置 AD

Microsoft 于 2018 年推出了 Windows Admin Center，这款正在开发的程序正在成为主流的服务器管理方式。

最初我尝试着使用这款全新的工具，按照 Microsoft 的推荐在 Server-No2 和 Server-No3 上安装了无 GUI 的 Windows Server。



安装完成后可以发现无 GUI 的 Windows Server 2022 只有一个 PowerShell 窗口，该版本开机后会自动进入 SConfig 程序，如下图。



在 Server-No1 中打开 Windows Admin Center，输入服务器名 Server-No2 即可轻松地与



其建立连接。同样地，点击“角色和功能”，可以在其中安装 Active Directory 域服务。

The screenshot shows the Windows Admin Center interface for Server-No2. The left sidebar has 'Server-No2' selected under 'Tools'. Under 'Roles and Features', the 'Install' tab is active. The 'Roles' section lists several roles: '打印和文件服务' (Installed), '批量数据服务' (Available), '设备运行状况证明' (Available), '文件和存储服务' (Installed), '远程访问' (Available), '远程桌面服务' (Available), '主机保护服务' (Available), 'Active Directory 联合身份验证服务' (Available), 'Active Directory 轻型目录服务' (Available), 'Active Directory 域服务' (Available), 'Active Directory 证书服务' (Available), 'Active Directory Rights Management Services' (Available), 'DHCP 服务器' (Available), 'DNS 服务器' (Available), 'Hyper-V' (Available), 'Web 服务器(IIS)' (Available), 'Windows Deployment Services' (Available), and 'Windows Server 更新服务' (Available). The 'Features' section lists '功能' (Available). On the right, a 'Install Roles and Features' button is shown with a checkbox for '如果需要, 自动重新启动服务器' (Automatically restart server if needed) and a 'Continue' (继续) button.

另外，还可以使用远程桌面连接 Server-No2。

The screenshot shows the Windows Admin Center interface for Server-No2. The left sidebar has 'Server-No2' selected under 'Tools'. Under 'Remote Desktop', the 'Connect' tab is active. A command prompt window is displayed, showing the Windows Server 2022 Standard welcome screen. The screen lists 15 configuration options: 1) 工作组: WORKGROUP, 工作组: WORKGROUP SERVER-NO2; 2) 计算机名: SERVER-NO2; 3) 添加本地管理员; 4) 远程管理: 已启用; 5) 更新设置; 6) 客户端更新: 仅下载; 7) 远程桌面: 已启用 (所有客户端); 8) 网络设置; 9) 日期和时间; 10) 电源设置; 11) Windows 激活: 必需; 12) 注销用户; 13) 重新启动服务器; 14) 关闭服务器; 15) 退出到命令行 (PowerShell)。Input number to select option: -

但是 Windows Admin Center 目前还没有集成对其的配置功能，该功能目前仍作为一个扩展插件被开发，我们可以手动安装它。



可用扩展	已安装的扩展	源
安装		
名称	版本	
Active Directory	0.86.0	
Azure Cloud Shell (Preview)	1.10.0	
Azure Extended Network	2.2.0	
Azure IoT Edge (preview)	2.5.0	
BittOps Changes	2.0.25	
Configuration Manager Client (Preview)	1.2.1	
Containers	1.150.0	
DataON MUST Pro	3.0.0	
DataON MUST Visibility, Monitoring, and Management...	3.4.0	
Dell EMC OpenManage Integration	2.2.1	
Dell EMC PowerPath	1.1.0	
Dell PowerStore Manager	1.0.1	
DHCP (Preview)	0.9.3	
DNS (Preview)	0.9.5	

但遗憾的是这个插件目前只能在作为域控制器的服务器上查看。

server-no1.xuwp05191643.com

工具 < Active Directory 域服务 预览 ⓘ

概述 浏览

域名: xuwp05191643

搜索 Active Directory 搜索

+ 创建 ⓘ 启用 ⓘ 禁用 ⓘ 删除 ⓘ 重置密码 ⓘ 属性

名称 ↴ 若要开始, 请执行搜索或创建新项目

事件
数据包监视
网络
文件和文件共享
系统见解
性能监视器
已安装的应用
远程桌面
证书
注册表
Active Directory

因为 AD 配置功能仍在开发, Windows Admin Center 目前还没有像 Windows Server



Manager 一样强大的功能，但我相信这样的集大成者在不久后定会成为主流，不负安装系统时的推荐二字。

3 创建用户

先试一下 Desktop 版添加用户的方式，打开本地用户和组。



行不通，按它说的在“Active Directory 用户和计算机”中添加试试。

名称	类型	描述
Administrator	用户	管理计算机(域)的内置帐户
Allowed RODC Password Replication Group	安全组 - 本地域	允许将此组中成员的密码复制到域中的所有只读域控制器
Cert Publishers	安全组 - 本地域	此组的成员被允许发布证书到目录
Cloneable Domain Controllers	安全组 - 全局	可以克隆此组中作为域控制器的成员。
Denied RODC Password Replication Group	安全组 - 本地域	不允许将此组中成员的密码复制到域中的所有只读域控制器
DnsAdmins	安全组 - 本地域	DNS Administrators 组
DnsUpdateProxy	安全组 - 全局	允许替其他客户端(如 DHCP 服务器)执行动态更新的 DNS 客户端。
Domain Admins	安全组 - 全局	指定的域管理员
Domain Computers	安全组 - 全局	加入到域中的所有工作站和服务器
Domain Controllers	安全组 - 全局	域中所有域控制器
Domain Guests	安全组 - 全局	域的所有来宾
Domain Users	安全组 - 全局	所有域用户
Enterprise Admins	安全组 - 通用	企业的指定系统管理员
Enterprise Key Admins	安全组 - 通用	此组的成员可以对林中的密钥对象执行管理操作。
Enterprise Read-only Domain Controllers	安全组 - 通用	该组的成员是企业中的只读域控制器
Group Policy Creator Owners	安全组 - 全局	这个组中的成员可以修改域的组策略
Guest	用户	供来宾访问计算机或访问域的内置帐户
Key Admins	安全组 - 全局	此组的成员可以对域中的密钥对象执行管理操作。
Protected Users	安全组 - 全局	此组的成员将受到针对身份验证安全威胁的额外保护。有关详细信息，...
RAS and IAS Servers	安全组 - 本地域	这个组中的服务器可以访问用户的远程访问属性
Read-only Domain Controllers	安全组 - 全局	此组中的成员是域中只读域控制器
Schema Admins	安全组 - 通用	架构的指定系统管理员
Windows Admin Center CredSSP Administrators	安全组 - 本地域	允许用户执行 Windows Admin Center CredSSP 操作

右击“xuwp05191643.com”，点击“新建” - “组织单元”。



新建对象 - 组织单位

X



创建于: xuwp05191643.com/

名称(A):

Client Users

防止容器被意外删除(P)

确定

取消

帮助

右击“Client Users”，点击“新建” - “组”。



新建对象 - 组

X



创建于: xuwp05191643.com/Client Users

组名(A):

Server Users

组名(Windows 2000 以前版本)(W):

Server Users

组作用域

- 本地域(O)
- 全局(G)
- 通用(U)

组类型

- 安全组(S)
- 通讯组(D)

确定

取消

右击“Client Users”，点击“新建” - “用户”。



新建对象 - 用户

X



创建于: xuwp05191643.com/Client Users

姓(L):

Xu

名(F):

Wanpeng

英文缩写(I):

-No1

姓名(A):

XuWanpeng-No1

用户登录名(U):

xuwp-No1

@xuwp05191643.com

用户登录名(Windows 2000 以前版本)(W):

XUWP05191643\

xuwp-No1

< 上一步(B)

下一步(N) >

取消



新建对象 - 用户

X



创建于: xuwp05191643.com/Client Users

密码(P):

••••••••••

确认密码(C):

••••••••••

- 用户下次登录时须更改密码(M)
- 用户不能更改密码(S)
- 密码永不过期(W)
- 帐户已禁用(O)

< 上一步(B)

下一步(N) >

取消



新建对象 - 用户

X



创建于: xuwp05191643.com/Client Users

你单击“完成”后，下列对象将被创建:

全名: XuWanpeng-No1

用户登录名: xuwp-No1@xuwp05191643.com

用户下次登录时须更改密码。

< 上一步(B)

完成

取消

这里为了区分各 Server 的用户，我在“英文缩写”处做了一个标识“-Nox”。

注：在实际生产环境中最好勾选“用户下次登录时须更改密码”，这里我勾选了，后面可以看到需要更改密码才能登录进去，后两个用户就不勾了。

同样的步骤，在 Server-No2 和 Server-No3 中操作一遍，有：



新建对象 - 用户

X



创建于: a.xuwp05191643.com/Client Users

你单击“完成”后，下列对象将被创建:

全名: XuWanPeng-No2

用户登录名: xuwp-No2@a.xuwp05191643.com

< 上一步(B)

完成

取消



新建对象 - 用户

X



创建于: xuwp05191643.org/Client Users

你单击“完成”后，下列对象将被创建:

全名: XuWanpeng-No3

用户登录名: xuwp-No3@xuwp05191643.org

< 上一步(B)

完成

取消

4 登录客户机

4.1 配置

首先要将客户机加入到我们创建的 AD 林中。

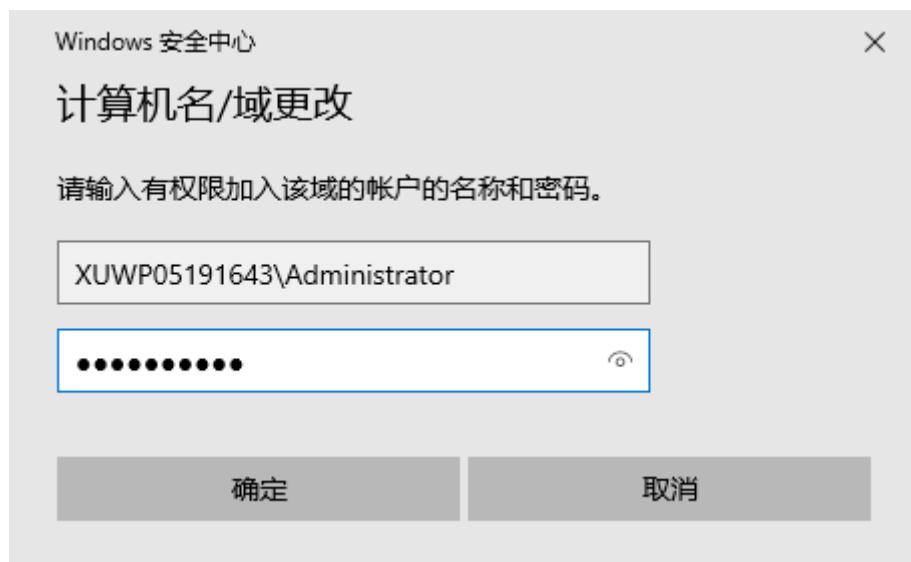
首先改 DNS



在“系统属性”中加入域即可。



输入 xuwp05191643.com 的凭据





计算机名/域更改

×

i 欢迎加入 xuwp05191643.com 域。

确定

加入成功。

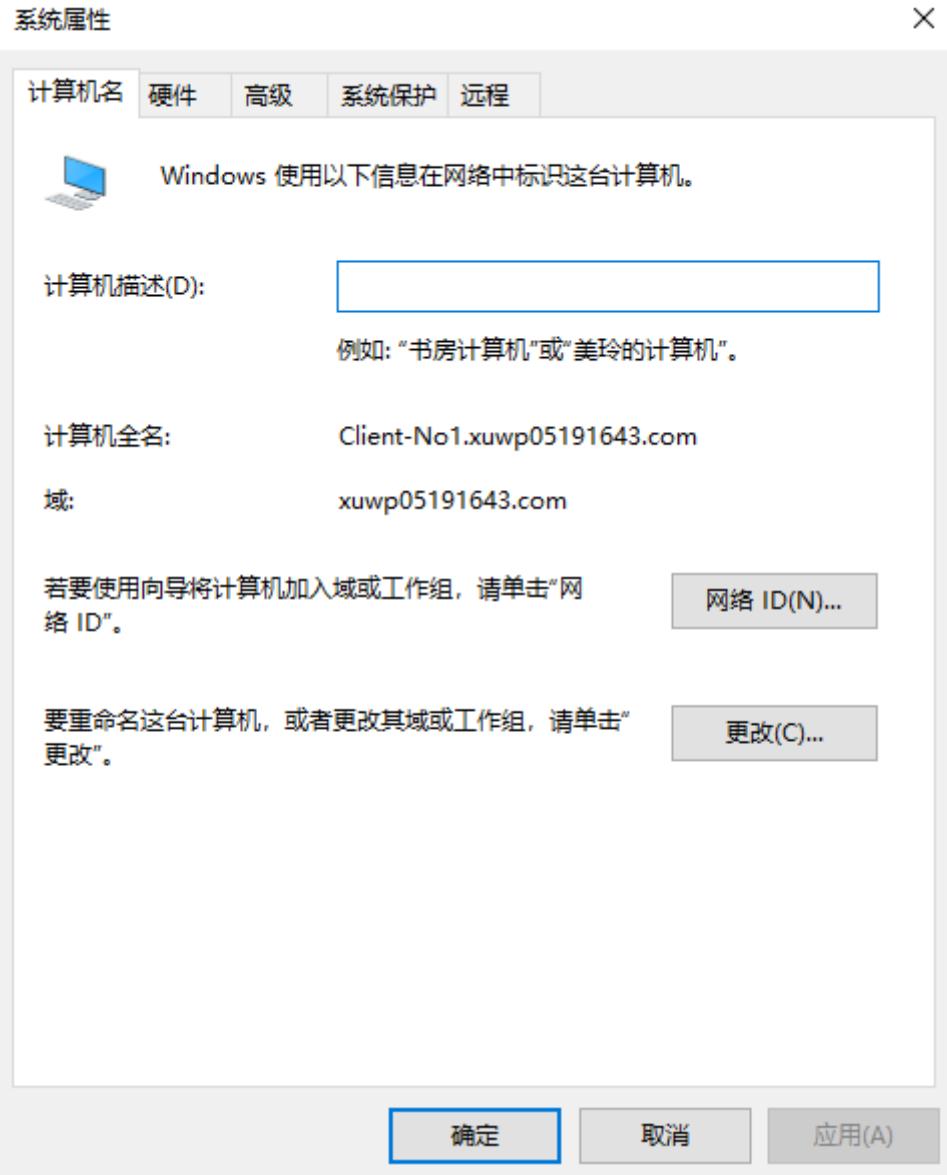
计算机名/域更改

i 必须重新启动计算机才能应用这些更改

重新启动之前, 请保存所有打开的文件并关闭所有程序。

确定

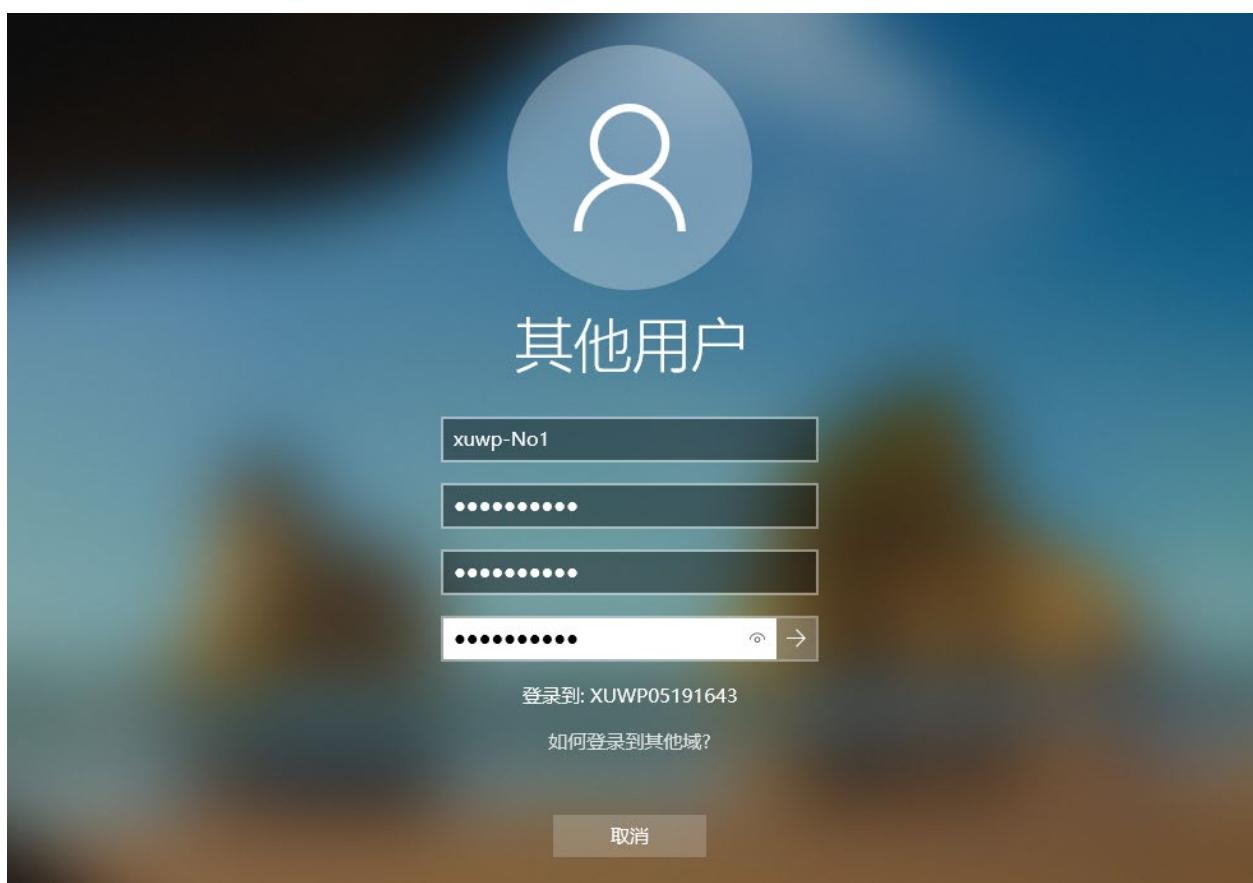
重启后查看“系统属性”。



4.2 登录 xuwp-No1



因为我们之前勾选了“用户下次登录时须更改密码”，所以这里系统要求我们更改密码后进入。



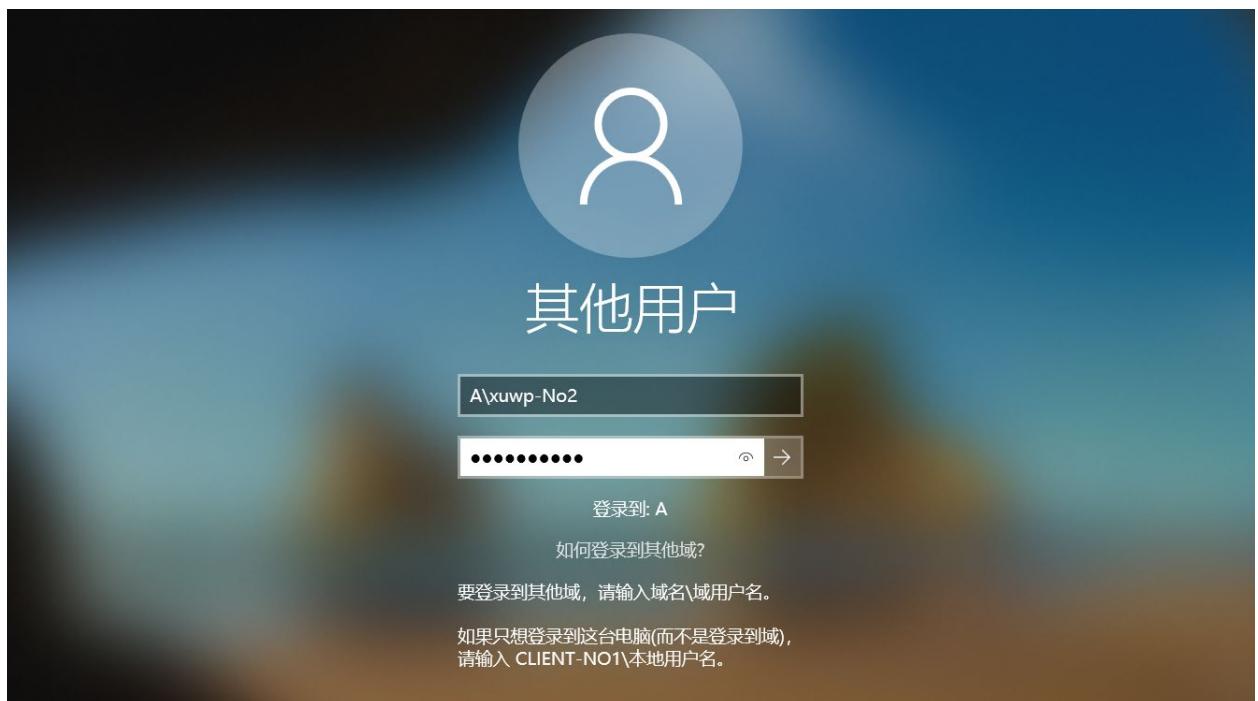


使用新密码登录系统后，出现和初始化系统相同的界面。

最后，使用 whoami 命令确定域和用户。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.18363.418]
(c) 2019 Microsoft Corporation。保留所有权利。
C:\Users\xuwp-No1>whoami
xuwp05191643\xuwp-no1
```

4.3 登录 xuwp-No2



根据下面“如何登录到其他域？”的提示，我们使用域名\域用户名的格式登录。(这



实际上是 Windows 2000 以前版本的登录方式，目前应该使用域用户名@域名)。

这里不需要更改密码，等待初始化系统后使用 whoami 确定域和用户。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.18363.418]
(c) 2019 Microsoft Corporation。保留所有权利。
C:\Users\xuwp-No2>whoami
a\xuwp-no2
```

4.4 登录 xuwp-No3



发现登录不上，我们 ping 一下 Server-No3 试试。

```
C:\Users\xuwp-No1>ping 192.168.36.130

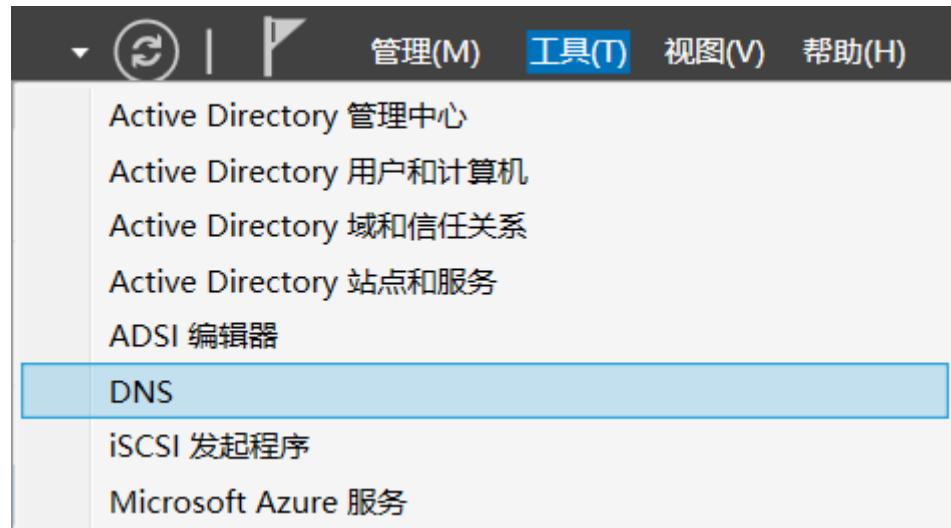
正在 Ping 192.168.36.130 具有 32 字节的数据:
来自 192.168.36.130 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128

192.168.36.130 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 2ms, 平均 = 0ms

C:\Users\xuwp-No1>ping xuwp05191643.org
Ping 请求找不到主机 xuwp05191643.org。请检查该名称, 然后重试。
```



发现 DNS 无法解析，那就对 xuwp05191643.com 设置一个 xuwp05191643.org 的 IP 转发。



点击“工具” - “DNS”。



显示当前所选内容的帮助。

右击“条件转发器” - “新建条件转发器”。



新建条件转发器

X

DNS 域:

xuwp05191643.org

主服务器的 IP 地址(S):

IP 地址	服务器 FQDN	已验证
<单击此处添加 IP 地址或 DNS 名称>		
192.168.36.130	SERVER-NO3	验证服务器时出现了一个未知错误。

删除(D)

上移(U)

下移(O)

 在 Active Directory 中存储此条件转发器，并按如下方式复制它(S):

此林中的所有 DNS 服务器

在转发查询超时之前的秒数:

如果未配置相应的反向查找区域和条目，则服务器 FQDN 将不可用。

确定

取消

输入“DNS 域”和“主服务器的 IP 地址”，点击“确定”。

注：这里虽然提示了一个“验证服务器时出现了一个未知错误”，但其实并无大碍。

再试着 ping 一下 Server-No3。



```
C:\Users\xuwp-No1>ping 192.168.36.130
```

正在 Ping 192.168.36.130 具有 32 字节的数据：
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128

192.168.36.130 的 Ping 统计信息：
数据包：已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位)：
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```
C:\Users\xuwp-No1>ping xuwp05191643.org
```

正在 Ping xuwp05191643.org [192.168.36.130] 具有 32 字节的数据：
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128

192.168.36.130 的 Ping 统计信息：
数据包：已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位)：
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

可以解析了，再次登录一下。



这次可以登录成功了，使用 whoami 确定域和用户。



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.18363.418]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\xuwp-No3>whoami
xuwp051916430\xuwp-no3
```

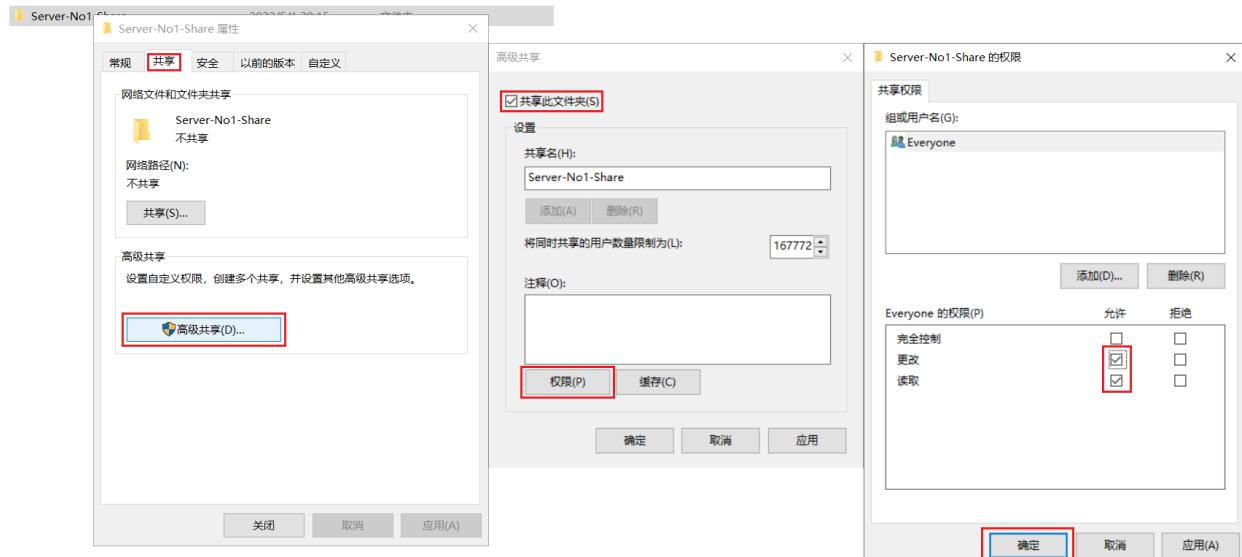
5 共享资源

共享资源有几种方式，但都差不太多。

5.1 设置共享文件夹

5.1.1 高级共享

右击想要共享的文件夹-“属性”-“共享”-“高级共享”-“共享此文件夹”-“权限”-允许读取/更改-“确定”。



注意这种方式是共享给“Everyone”的，林中的所有用户都可以发现共享文件夹。

5.1.2 共享

右击想要共享的文件夹-“属性”-“共享”-下拉箭头-“查找个人”-“位置”



位置

X

选择你想进行搜索的位置。

位置(L):

The screenshot shows a Windows-style search interface. At the top left is a text input field labeled "位置(L):". Below it is a tree view of directory contents under "整个目录". The tree includes the root domain "xuwp05191643.com" and its subfolders: "a.xuwp05191643.com", "Builtin", "Client Users", "Computers", "Domain Controllers", "ForeignSecurityPrincipals", "LostAndFound", "Managed Service Accounts", and "Program Data". The "整个目录" option is selected. At the bottom right are two buttons: "确定" (Confirm) and "取消" (Cancel).

选中“整个目录”。

然后我们就可以搜索我们的 3 个 Administrator 和 3 个 XuWanpeng-Nox 了。



选择用户或组

X

选择此对象类型(S):

用户、组或内置安全主体

对象类型(O)...

查找位置(F):

整个目录

位置(L)...

一般性查询

名称(A):

起始为

Xu

列(C)...

描述(D):

起始为

立即查找(N)

 禁用的帐户(B) 不过期密码(X)

自上次登录后的天数(I):

停止(T)



搜索结果(U):

确定

取消

名称	电子邮件地址	描述	所在文件夹
XuWanpeng-No1			xuwp05191643.com/Client Users
XuWanPeng-No2			a.xuwp05191643.com/Client Users
XuWanpeng-No3			xuwp05191643.org/Client Users

选中他们，点击“确定”。

将 6 个用户全部加入后如图。



选择用户或组

X

选择此对象类型(S):

用户、组或内置安全主体

对象类型(O)...

查找位置(F):

整个目录

位置(L)...

输入对象名称来选择(示例)(E):

Administrator; Administrator; Administrator;
XuWanpeng-No1 (xuwp-No1@xuwp05191643.com);
XuWanPeng-No2 (xuwp-No2@a.xuwp05191643.com);
XuWanpeng-No3 (xuwp-No3@xuwp05191643.org)

检查名称(C)

高级(A)...

确定

取消

点击“确定”。



X

[← 网络访问](#)

选择要与其共享的网络上的用户

键入名称，然后单击“添加”，或者单击箭头查找用户。

名称	权限级别
Administrator	读取/写入 ▼
Administrator	读取/写入 ▼
Administrator	读取/写入 ▼
Administrators	所有者
XuWanpeng-No1	读取/写入 ▼
XuWanPeng-No2	读取/写入 ▼
XuWanpeng-No3	读取 ▼

共享时有问题

添加(A)

共享(H) 取消

最后将他们权限级别全部改为“读取/写入”。

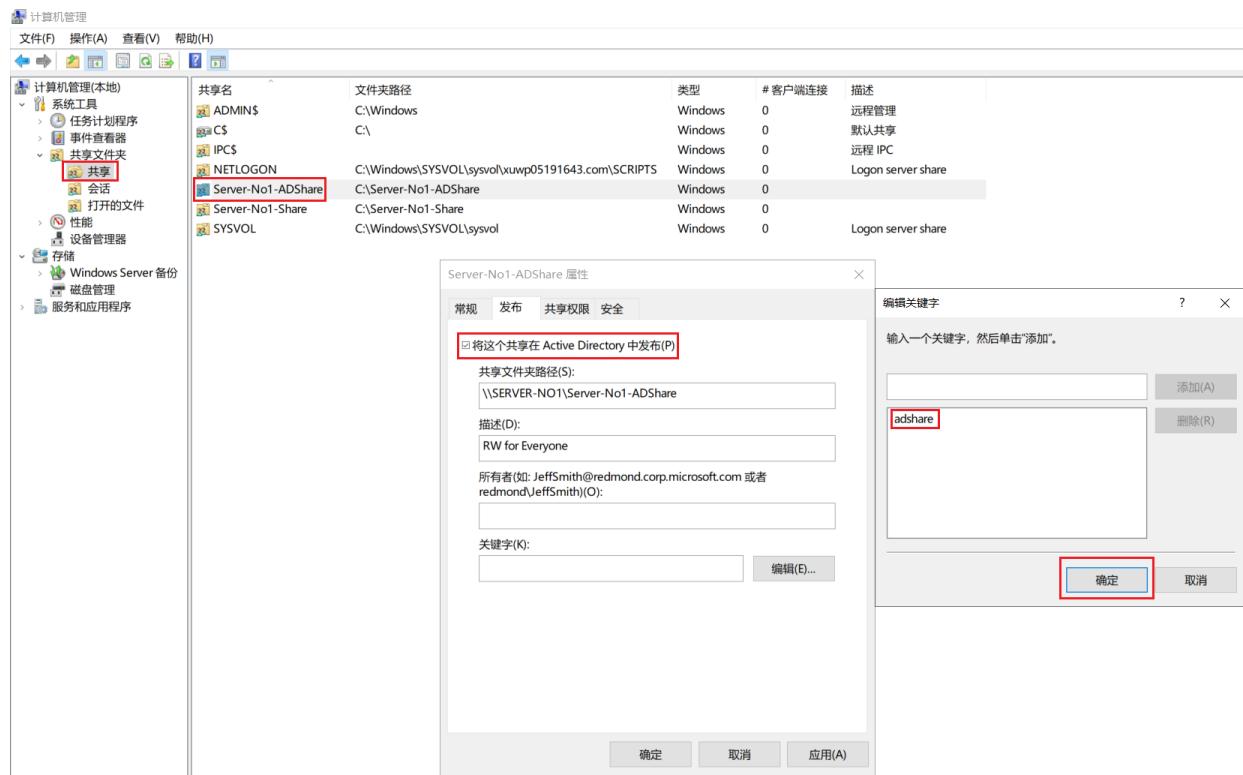
注：这种方式也可以实现对“Everyone”的共享，这个选项也在下拉菜单中。

5.1.3 在 Active Directory 上发布共享文件夹

有的时候我们不希望整个网络的主机都发现我们的共享文件夹，我们现在试着将文件夹发布到自己所在的 AD 上。

首先，使用前两节的方法将其设置为共享文件夹。

接着，打开“计算机管理”(compmgmt.msc) - “共享文件夹” - “共享” - 右击“Server-No1-ADShare” - “属性”。



点击“将这个共享在 Active Directory 中发布”，并为其设置一个关键字即可发布到主机所在 AD 上，我们在 5.2.2 节演示怎样使用这些共享文件夹。

5.2 查看共享文件夹

5.2.1 在网络中发现共享文件

设置好共享文件夹后，系统会生成一个网络路径，如



林中的计算机使用这个路径后都可以查看共享文件夹。但是我们并不能发现它，这要怎么办呢？

一个朴素的想法就是在“控制面板” - “网络和 Internet” - “网络和共享中心” - “高级共享设置”中“启用网络发现”。



域 (当前配置文件)

网络发现

如果已启用网络发现，则这台计算机可以发现网络上的其他计算机和设备，而且其他网络计算机也可以发现这台计算机。

- 启用网络发现
 关闭网络发现

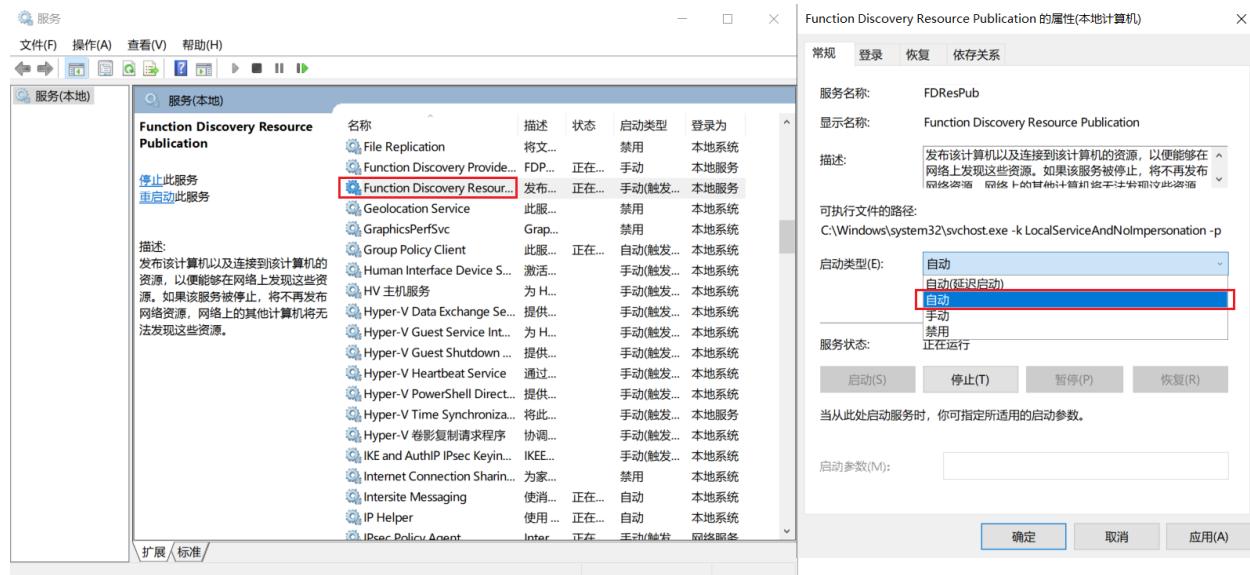
文件和打印机共享

启用文件和打印机共享时，网络上的用户可以访问通过此计算机共享的文件和打印机。

- 启用文件和打印机共享
 关闭文件和打印机共享

但我们发现这个选项点不开，关闭页面后又会变回去。

更简单的方法是在“服务”(services.msc)中把“Function Discovery Resource Publication”服务打开。



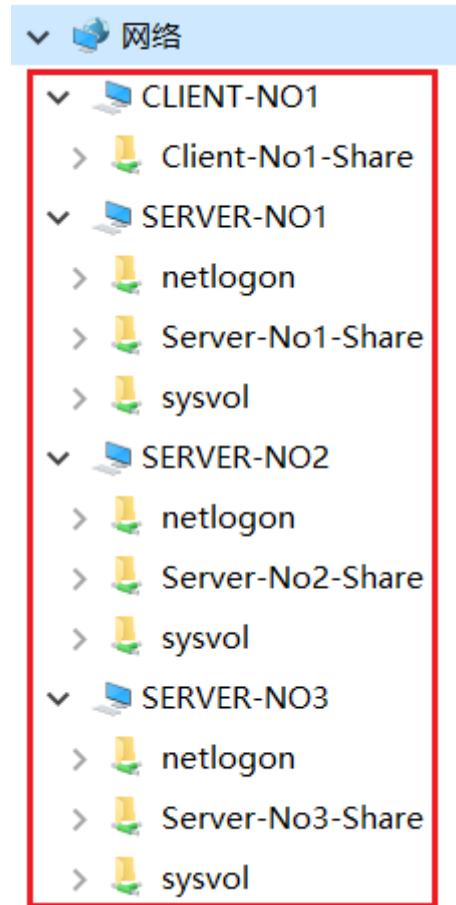


Function Discovery Resource Publication		发布...	自动(触发...)	本地服务
Geolocation Service	此服务	启动(S)	系统	
GraphicsPerfSvc	Graphics Performance Monitor	停止(O)	系统	
Group Policy Client	此服务	暂停(U)	系统	
Human Interface Device Service	激活(I)	恢复(M)	系统	
HV 主机服务	为 Hyper-V 提供支持	重新启动(E)	系统	
Hyper-V Data Exchange Service	提供数据交换服务	所有任务(K)	系统	
Hyper-V Guest Service Interface	为 Hyper-V 客户机提供服务	刷新(F)	系统	
Hyper-V Guest Shutdown Service	提供来宾关机服务	属性(R)	系统	
Hyper-V Heartbeat Service	通过心跳检测来宾状态	帮助(H)	系统	
Hyper-V PowerShell Direct	提供 PowerShell 直接访问			
Hyper-V Time Synchronization Service	将此计算机设置为网络时间同步			服务

FDResPub 服务的作用是：发布该计算机以及连接到该计算机的资源，以便能够在网络上发现这些资源。如果该服务被停止，将不再发布网络资源，网络上的其他计算机将无法发现这些资源。

然后我们就可以在“网络”中发现共享文件夹了。

事实上“启用网络发现”这个选项也是可以打开的，需要用上述方式打开“Function Discovery Resource Publication”服务、“SSDP Discovery”服务、“UPnP Device Host”服务，然后这个选项就永久打开了（推荐这种方式）。



至此，我们随便选择 3 个 Administrator 和 3 个 xuwp-Nox 中的任何 1 个都可以查看到这些共享文件夹。

5.2.2 在 Active Directory 上查找共享文件夹

点击“网络” - “搜索 Active Directory”。

将“查找”处改为“共享文件夹”。

输入关键字，点击“开始查找”即可找到我们在 AD 上发布的共享文件夹 Server-No1-ADShare。

这里我使用通配符*，但并没有发现此前那些共享文件夹，说明这里只能搜索到在 AD 上发布的共享文件夹。

事实上，“启用网络发现”的主机也可以看见共享文件夹 Server-No1-ADShare，这是不安全的，所以尽量使用 Active Directory 共享文件夹。

注：关键字缺省代表搜索所有共享文件夹。



The screenshot shows the Windows Network interface. In the top navigation bar, the 'Network' tab is selected. A red box highlights the '搜索Active Directory' button. Below the navigation bar, there's a list of network resources under '计算机 (4)', showing three servers: SERVER-NO1, SERVER-NO2, and SERVER-NO3.

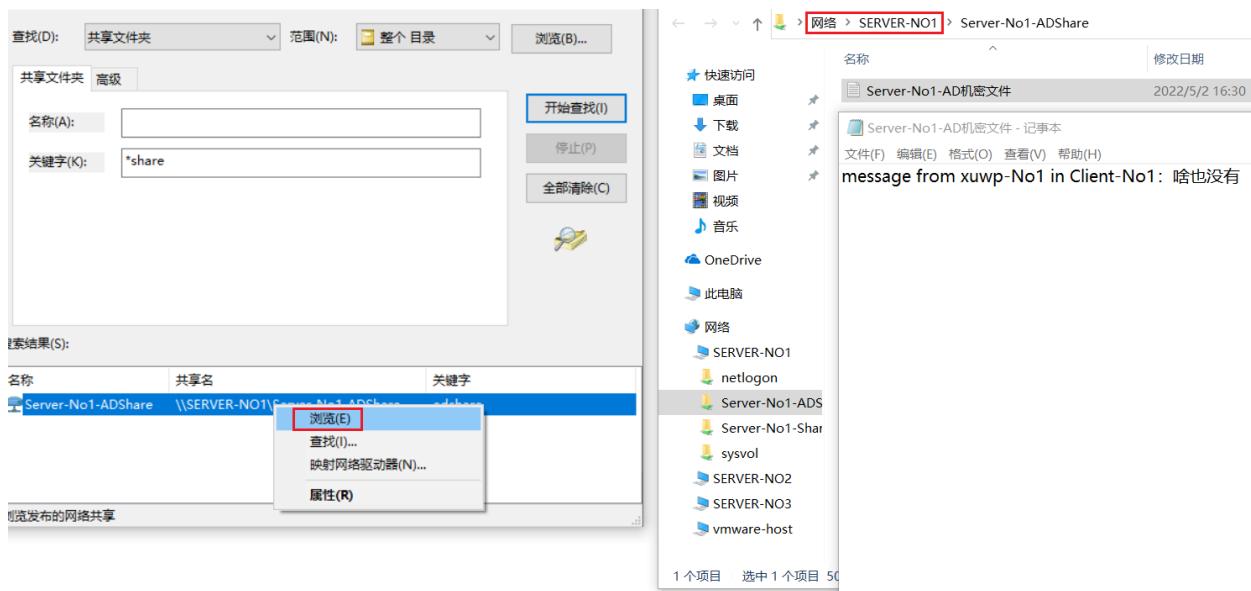
A search dialog box is open, also with a red box around the '搜索Active Directory' button. The search criteria are set to '共享文件夹' in the '查找(D):' field and '*share' in the '关键字(K):' field. The '开始查找(I)' button is also highlighted with a red box.

The search results table shows one entry:

名称	共享名	关键字
Server-No1-ADShare	\SERVER-NO1\Server-No1-ADShare	adshare

A red box highlights the entire row for 'Server-No1-ADShare'. At the bottom of the search results, it says '找到了 1 个项目'.

右击“Server-No1-ADShare”行，点击“浏览”即可正常读写文件夹。



我们在这个共享文件夹中写入一个文件，测试其他主机是否能看到这个文件。

进入任意一个林中的主机（这里我选用了发布该共享文件的主机），打开文件。



刷新后即可发现这个新增的文件。

有时我们需要经常用到某个共享文件夹，我们可以将其映射到网络驱动器。

右击“Server-No1-ADShare”行，点击“映射网络驱动器”。



X

[← 映射网络驱动器](#)

要映射的网络文件夹:

请为连接指定驱动器号，以及你要连接的文件夹:

驱动器(D): A:

文件夹(O): \\SERVER-NO1\Server-No1-ADShare

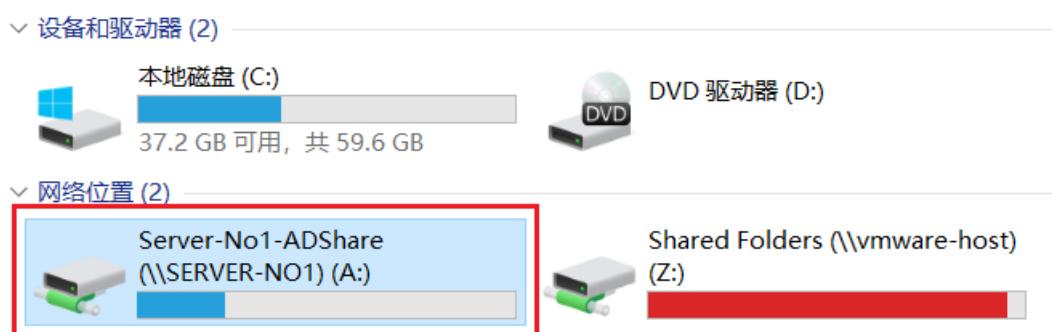
示例: \\server\share

登录时重新连接(R)

使用其他凭据连接(C)

[连接到可用于存储文档和图片的网站。](#)

在“驱动器”处选择一个喜欢的盘符。



回到资源管理器即可发现这个网络驱动器。

最后附一张位于多个域的共享文件夹查询。



查找 共享文件夹

文件(F) 编辑(E) 查看(V)

查找(D): 共享文件夹 范围(N): 整个目录 浏览(B)...

共享文件夹 高级

名称(A):
关键字(K):

开始查找(I) 停止(P) 全部清除(C)

搜索结果(S):

名称	共享名	关键字
Server-No3-ADShare	\SERVER-NO3\Server-No3-ADShare	adshare
Server-No2-ADShare	\SERVER-NO2\Server-No2-ADShare	adshare
Server-No1-ADShare	\SERVER-NO1\Server-No1-ADShare	adshare

找到了 3 个项目



6 作业展示截图

6.1 域和信任关系的展示截图

The screenshot shows the 'Active Directory Domains and Trust Relationships' window. The title bar reads 'Active Directory 域和信任关系 [Server-No1.xuwp05191643.com]'. The menu bar includes '文件(F)', '操作(A)', '查看(V)', and '帮助(H)'. Below the menu is a toolbar with icons for back, forward, search, and other functions. The left pane displays a tree view of domains: 'xuwp05191643.com' (selected), 'a.xuwp05191643.com', and 'xuwp05191643.org'. The right pane is a table with three columns: '名称' (Name), '类型' (Type), and '操作' (Operations). It lists two entries: 'xuwp05191643.com' (domainDNS) and 'xuwp05191643.org' (domainDNS). The '操作' column shows a link 'Active Directory 域和信任关系 [Server-No1.xuwp05191643.com]' and a '更多操作' (More Operations) button.

Active Directory 域和共享关系



xuwp05191643.com 属性

? X

常规 信任 管理者

受此域信任的域(外向信任)(M):

域名	信任类型	可传递
a.xuwp05191643.com	子	是
xuwp05191643.org	树根	是

属性(P)...

删除(R)

信任此域的域(内向信任)(O):

域名	信任类型	可传递
a.xuwp05191643.com	子	是
xuwp05191643.org	树根	是

属性(T)...

删除(V)

新建信任(N)...

确定

取消

应用(A)

帮助

xuwp05191643.com 属性



6.2 连通性测试截图

```
C:\Users\Administrator>whoami  
xuwp05191643\administrator  
  
C:\Users\Administrator>ping a.xuwp05191643.com  
  
正在 Ping a.xuwp05191643.com [192.168.36.129] 具有 32 字节的数据：  
来自 192.168.36.129 的回复：字节=32 时间=1ms TTL=128  
来自 192.168.36.129 的回复：字节=32 时间<1ms TTL=128  
来自 192.168.36.129 的回复：字节=32 时间<1ms TTL=128  
来自 192.168.36.129 的回复：字节=32 时间<1ms TTL=128  
  
192.168.36.129 的 Ping 统计信息：  
数据包：已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位)：  
最短 = 0ms, 最长 = 1ms, 平均 = 0ms  
  
C:\Users\Administrator>ping xuwp05191643.org  
  
正在 Ping xuwp05191643.org [192.168.36.130] 具有 32 字节的数据：  
来自 192.168.36.130 的回复：字节=32 时间=1ms TTL=128  
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128  
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128  
来自 192.168.36.130 的回复：字节=32 时间<1ms TTL=128  
  
192.168.36.130 的 Ping 统计信息：  
数据包：已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位)：  
最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

Server-No1 ping Server-No2 和 Server-No3



```
C:\Users\Administrator>whoami  
a\administrator
```

```
C:\Users\Administrator>ping xuwp05191643.com
```

正在 Ping xuwp05191643.com [192.168.36.128] 具有 32 字节的数据:
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128

192.168.36.128 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```
C:\Users\Administrator>ping xuwp05191643.org
```

正在 Ping xuwp05191643.org [192.168.36.130] 具有 32 字节的数据:
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128

192.168.36.130 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

Server-No2 ping Server-No1 和 Server-No3



```
C:\Users\Administrator>whoami  
xuwp051916430\administrator
```

```
C:\Users\Administrator>ping xuwp05191643.com
```

正在 Ping xuwp05191643.com [192.168.36.128] 具有 32 字节的数据:

来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128

192.168.36.128 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```
C:\Users\Administrator>ping a.xuwp05191643.com
```

正在 Ping a.xuwp05191643.com [192.168.36.129] 具有 32 字节的数据:

来自 192.168.36.129 的回复: 字节=32 时间<1ms TTL=128

192.168.36.129 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 0ms, 最长 = 0ms, 平均 = 0ms

Server-No3 ping Server-No1 和 Server-No2



```
C:\Users\XuWanpeng>whoami  
client-no1\xuwanpeng
```

```
C:\Users\XuWanpeng>ping xuwp05191643.com
```

正在 Ping xuwp05191643.com [192.168.36.128] 具有 32 字节的数据:
来自 192.168.36.128 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.128 的回复: 字节=32 时间<1ms TTL=128

192.168.36.128 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 1ms, 平均 = 0ms

```
C:\Users\XuWanpeng>ping a.xuwp05191643.com
```

正在 Ping a.xuwp05191643.com [192.168.36.129] 具有 32 字节的数据:
来自 192.168.36.129 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.129 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.129 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.129 的回复: 字节=32 时间<1ms TTL=128

192.168.36.129 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```
C:\Users\XuWanpeng>ping xuwp05191643.org
```

正在 Ping xuwp05191643.org [192.168.36.130] 具有 32 字节的数据:
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.36.130 的回复: 字节=32 时间<1ms TTL=128

192.168.36.130 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

Client-No1 ping Server-No1、Server-No2 和 Server-No3



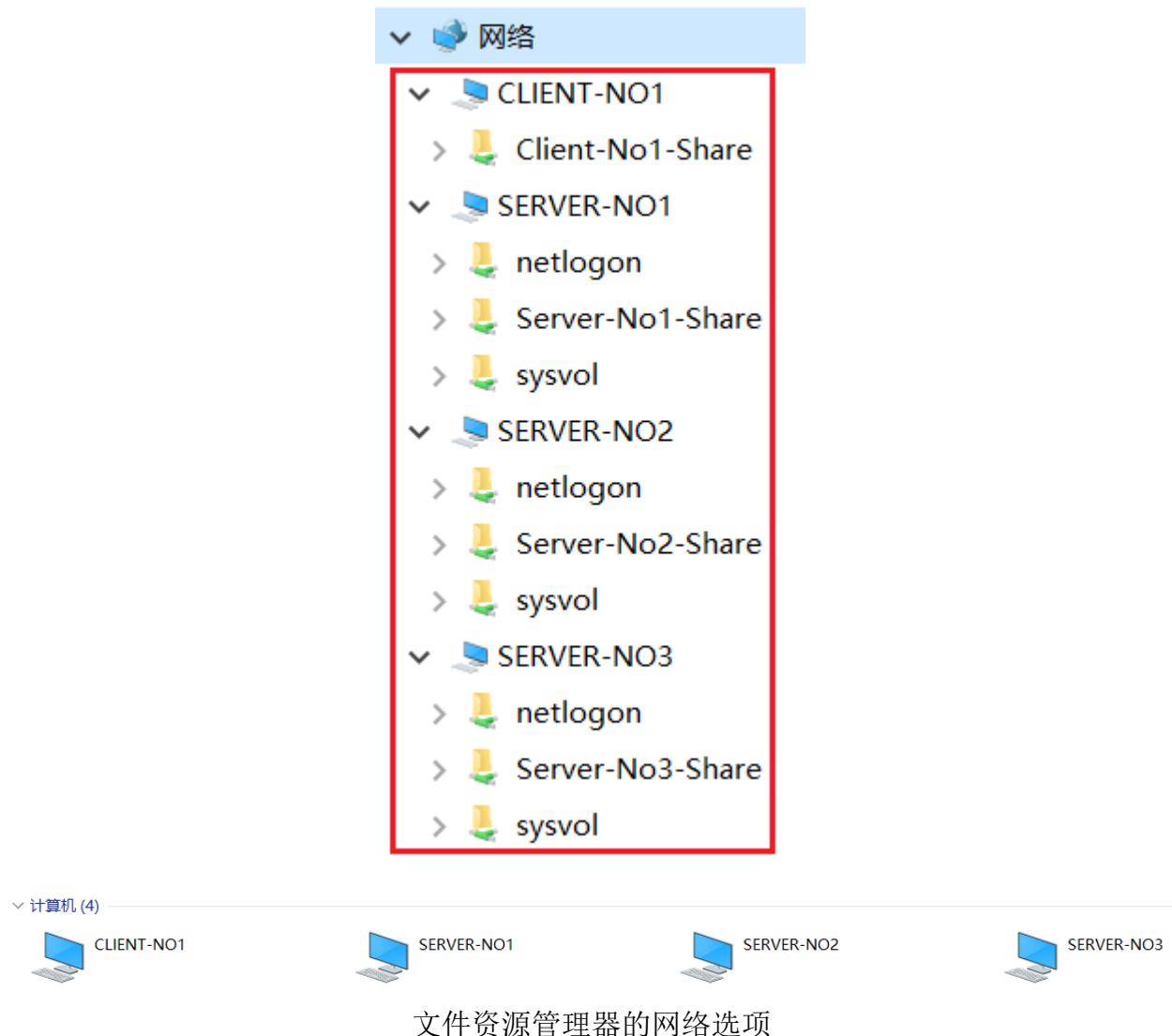
6.3 林中不同域计算机用户登录客户机的截图



点击开始菜单可以看到的已登录用户



6.4 可查询共享资源截图





查找 共享文件夹

文件(F) 编辑(E) 查看(V)

查找(D): 共享文件夹 范围(N): 整个目录 浏览(B)...

共享文件夹 高级

名称(A):
关键字(K):

开始查找(I) 停止(P) 全部清除(C)

搜索结果(S):

名称	共享名	关键字
Server-No3-ADShare	\SERVER-NO3\Server-No3-ADShare	adshare
Server-No2-ADShare	\SERVER-NO2\Server-No2-ADShare	adshare
Server-No1-ADShare	\SERVER-NO1\Server-No1-ADShare	adshare

找到了 3 个项目

在 AD 上查询共享文件夹