

# Final Project

Tanner Klock, Adam Sabatini

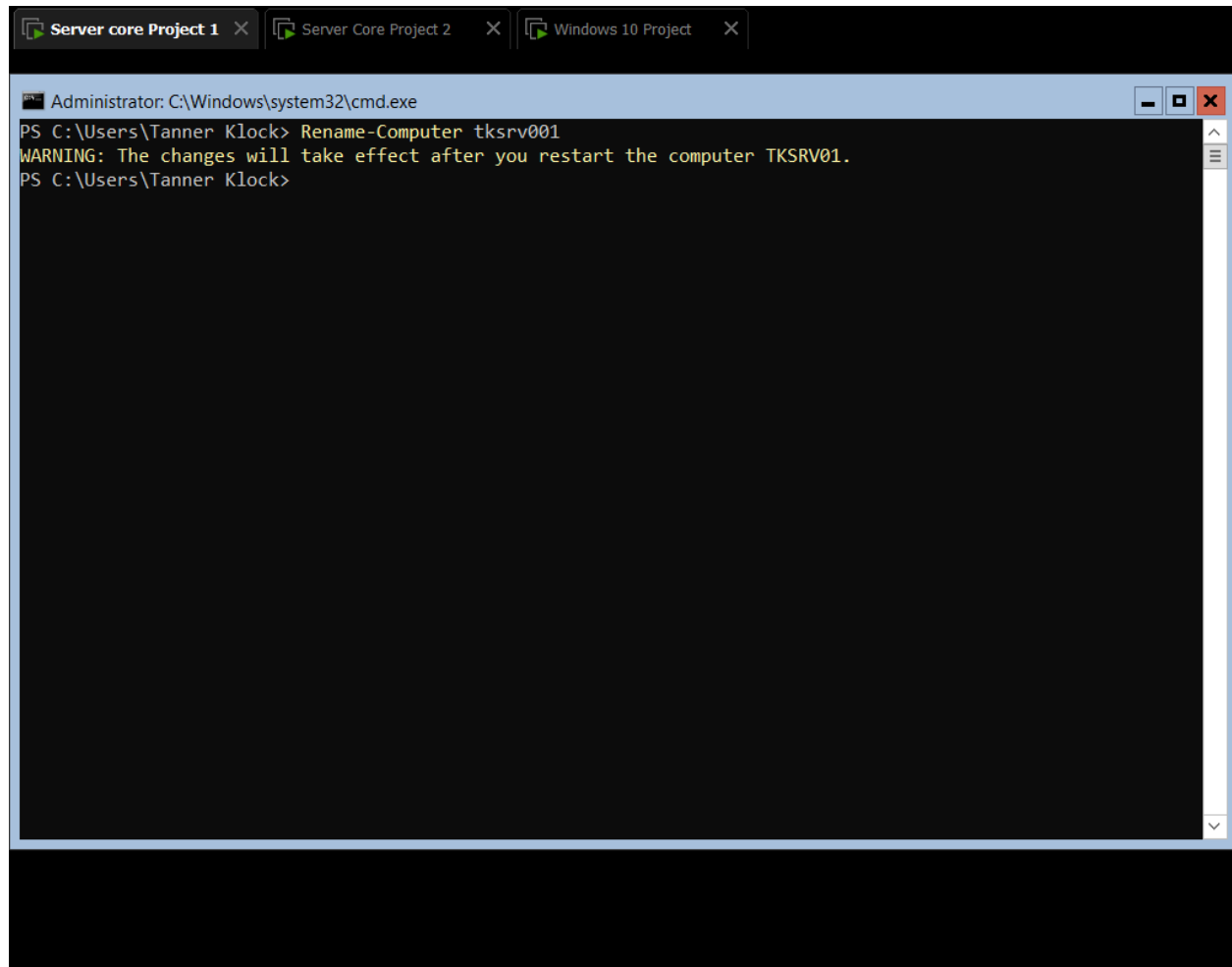
100923929, 100945612

COSC 2101

December 2<sup>nd</sup>, 2024

## PART 1:

Setting Static IP on DC server:



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window has three tabs at the top: "Server core Project 1", "Server Core Project 2", and "Windows 10 Project". The command prompt shows the following text:

```
PS C:\Users\Tanner Klock> Rename-Computer tksrv001
WARNING: The changes will take effect after you restart the computer TKSRV01.
PS C:\Users\Tanner Klock>
```

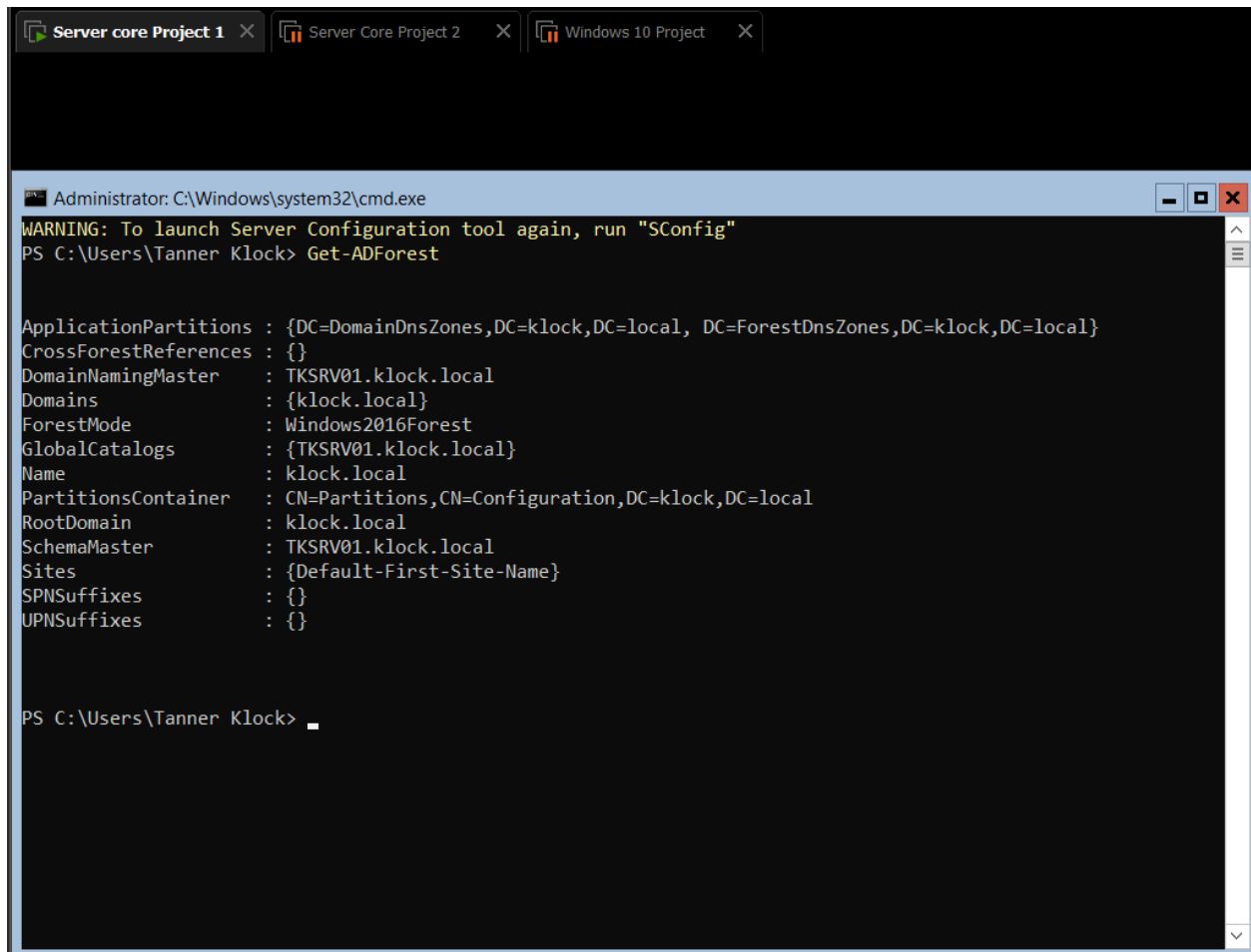
```
Server core Project 1 X Server Core Project 2 X Windows 10 Project X
Administrator: C:\Windows\system32\cmd.exe
PrefixLength      : 8
PrefixOrigin      : WellKnown
SuffixOrigin      : WellKnown
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

PS C:\Users\Tanner Klock> New-NetIPAddress -IPAddress 192.168.188.100 -PrefixLength 24 -InterfaceIndex 4

IPAddress      : 192.168.188.100
InterfaceIndex : 4
InterfaceAlias  : Ethernet0
AddressFamily   : IPv4
Type           : Unicast
PrefixLength    : 24
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState    : Tentative
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : ActiveStore

IPAddress      : 192.168.188.100
InterfaceIndex : 4
```

## Setting up server as Domain Controller:

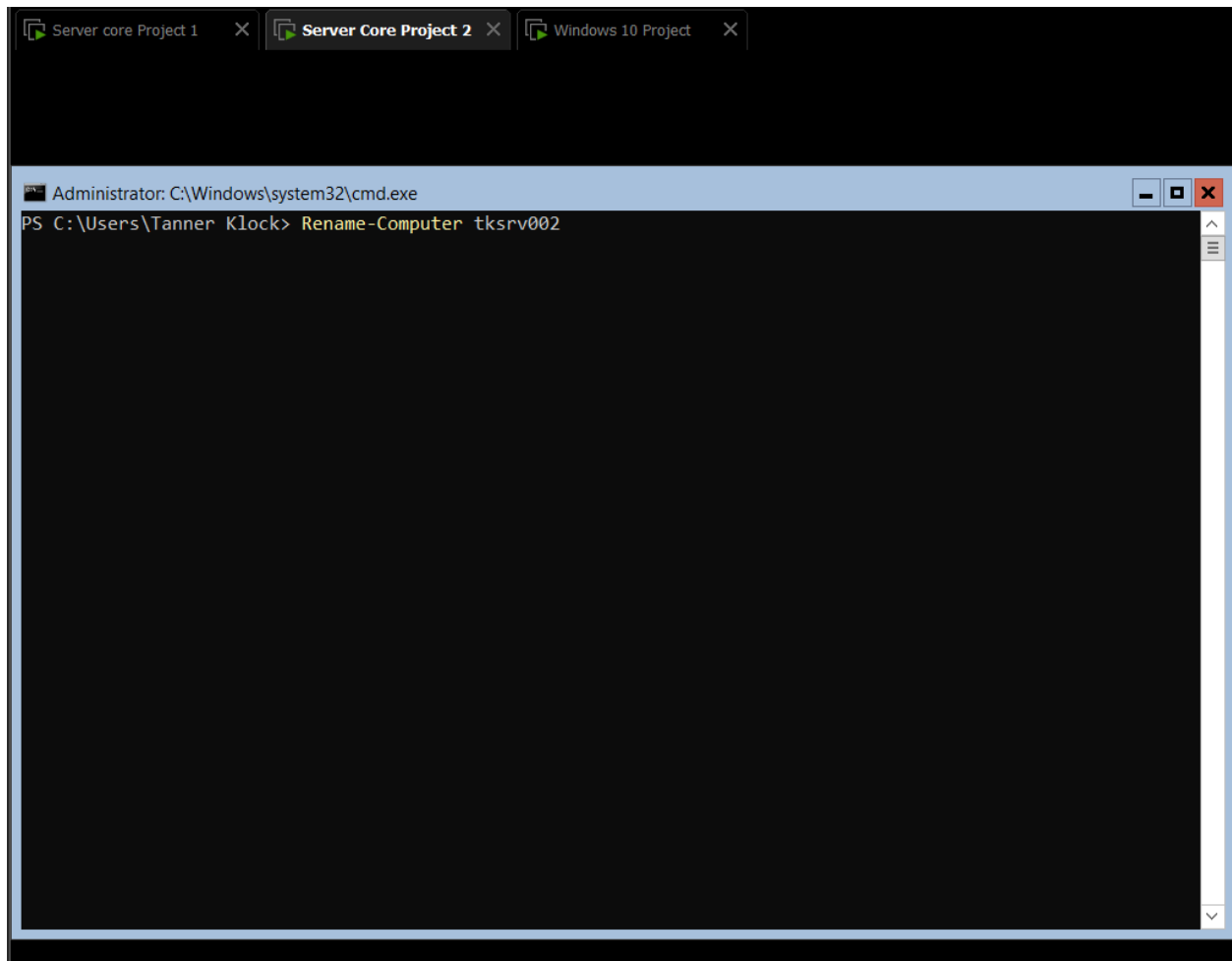


The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window has three tabs at the top: "Server core Project 1", "Server Core Project 2", and "Windows 10 Project". The command prompt displays a warning message: "WARNING: To launch Server Configuration tool again, run 'SConfig'". Below this, the user enters the command "PS C:\Users\Tanner Klock> Get-ADForest". The output of the command is displayed as follows:

```
ApplicationPartitions : {DC=DomainDnsZones,DC=klock,DC=local, DC=ForestDnsZones,DC=klock,DC=local}
CrossForestReferences : {}
DomainNamingMaster    : TKSRV01.klock.local
Domains               : {klock.local}
ForestMode             : Windows2016Forest
GlobalCatalogs        : {TKSRV01.klock.local}
Name                  : klock.local
PartitionsContainer    : CN=Partitions,CN=Configuration,DC=klock,DC=local
RootDomain             : klock.local
SchemaMaster           : TKSRV01.klock.local
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

The command prompt then shows the user's next prompt: "PS C:\Users\Tanner Klock> \_".

Setting Static IP on member server:



```
Server core Project 1 X Server Core Project 2 X Windows 10 Project X

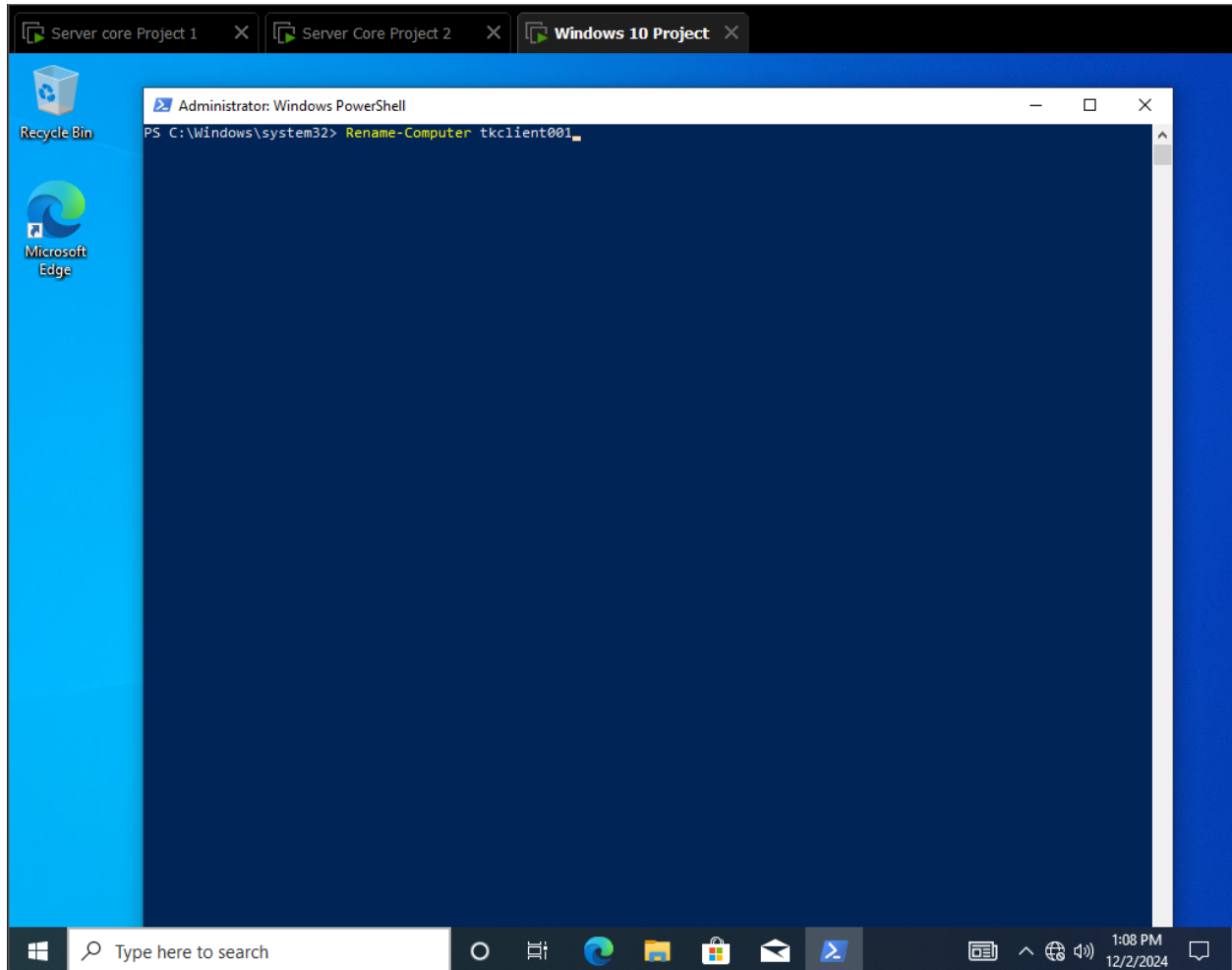
Administrator: C:\Windows\system32\cmd.exe
InterfaceAlias : Loopback Pseudo-Interface 1
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 8
PrefixOrigin   : WellKnown
SuffixOrigin   : WellKnown
AddressState   : Preferred
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore

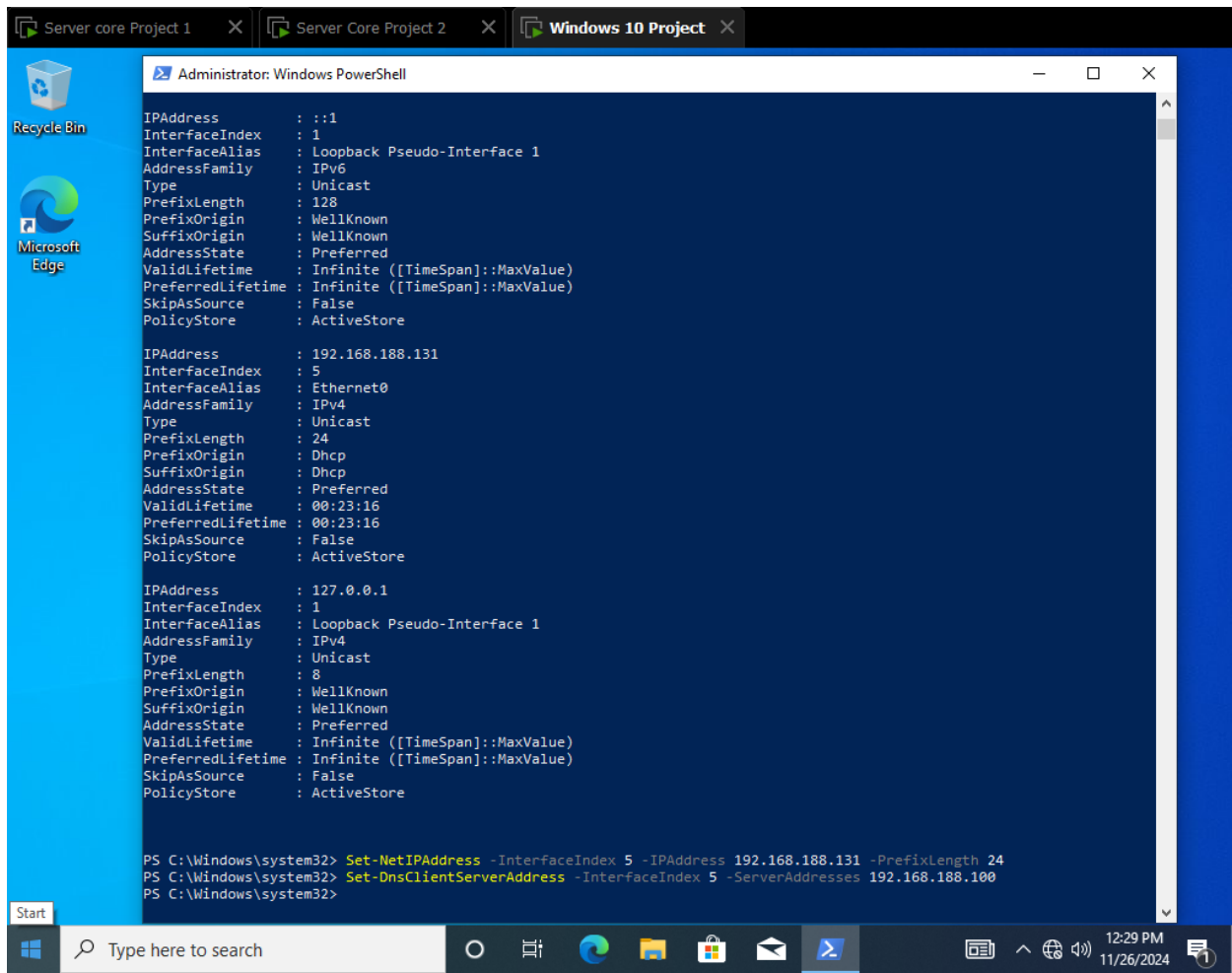
PS C:\Users\Tanner Klock> New-NetIPAddress -InterfaceIndex 6 -IPAddress 192.168.188.129 -PrefixLength 24
New-NetIPAddress : Instance MSFT_NetIPAddress already exists
At line:1 char:1
+ New-NetIPAddress -InterfaceIndex 6 -IPAddress 192.168.188.129 -Prefix ...
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (MSFT_NetIPAddress:ROOT/StandardCimv2/MSFT_NetIPAddress) [New-NetIPAddress], CimException
+ FullyQualifiedErrorId : Windows System Error 87,New-NetIPAddress

PS C:\Users\Tanner Klock> Set-NetIPAddress -InterfaceIndex 6 -IPAddress 192.168.188.129 -PrefixLength 24
PS C:\Users\Tanner Klock> Set-DnsClientServerAddress -InterfaceIndex 6 -ServerAddresses 192.168.188.100
PS C:\Users\Tanner Klock>
```

Since there was already an ip address assigned to this server the Set-NetIPAddress cmdlet needed to be used rather than New-NetIPAddress.

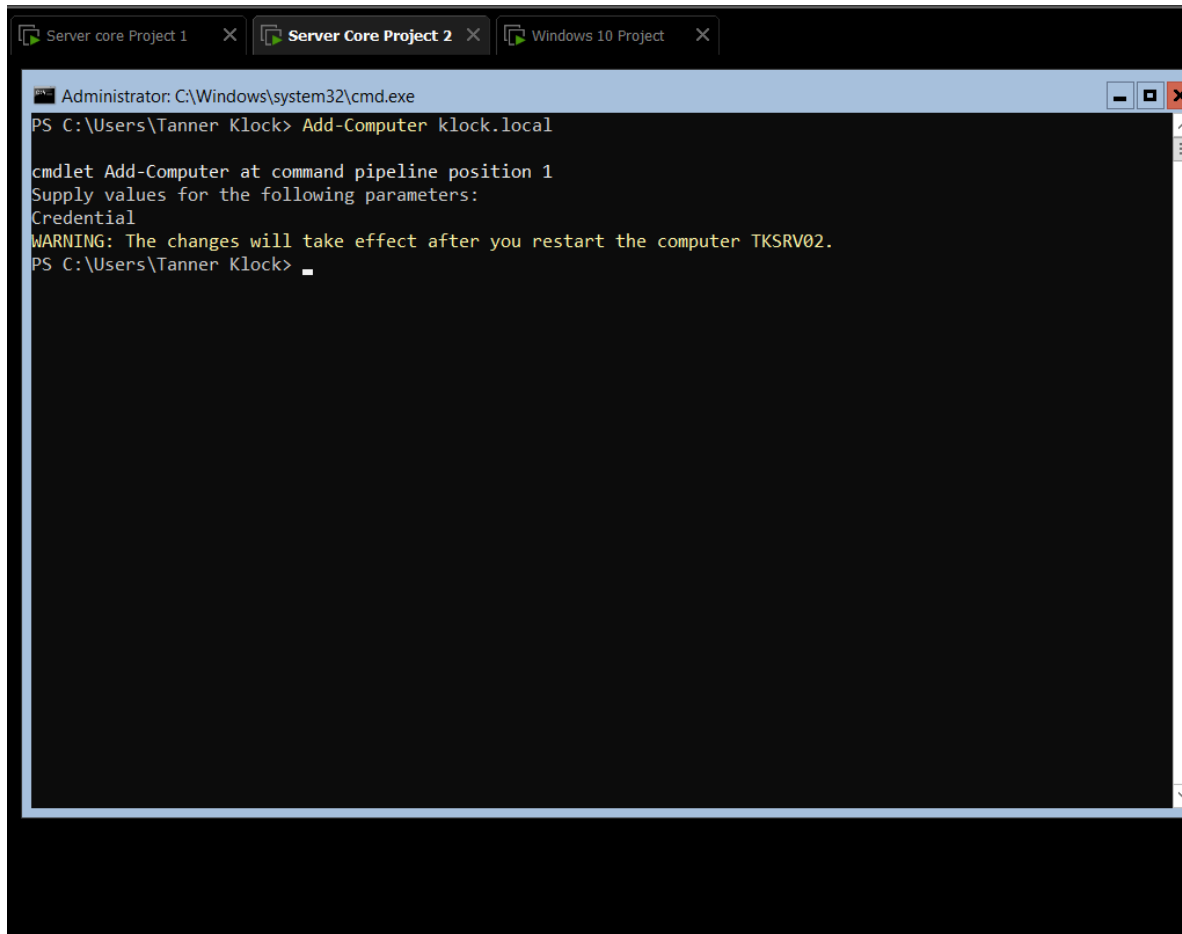
Setting Static IP on client:







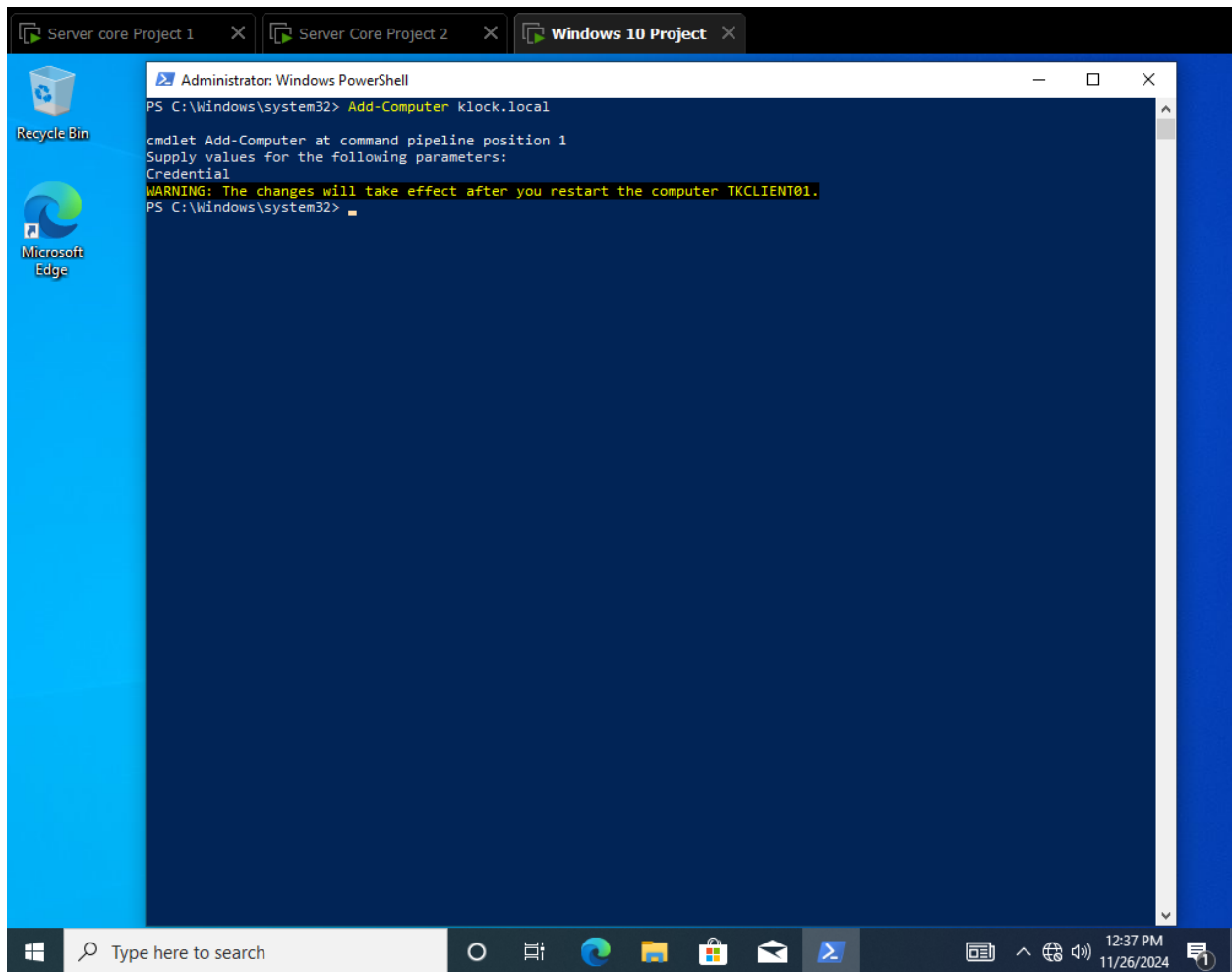
Joining member server and client:



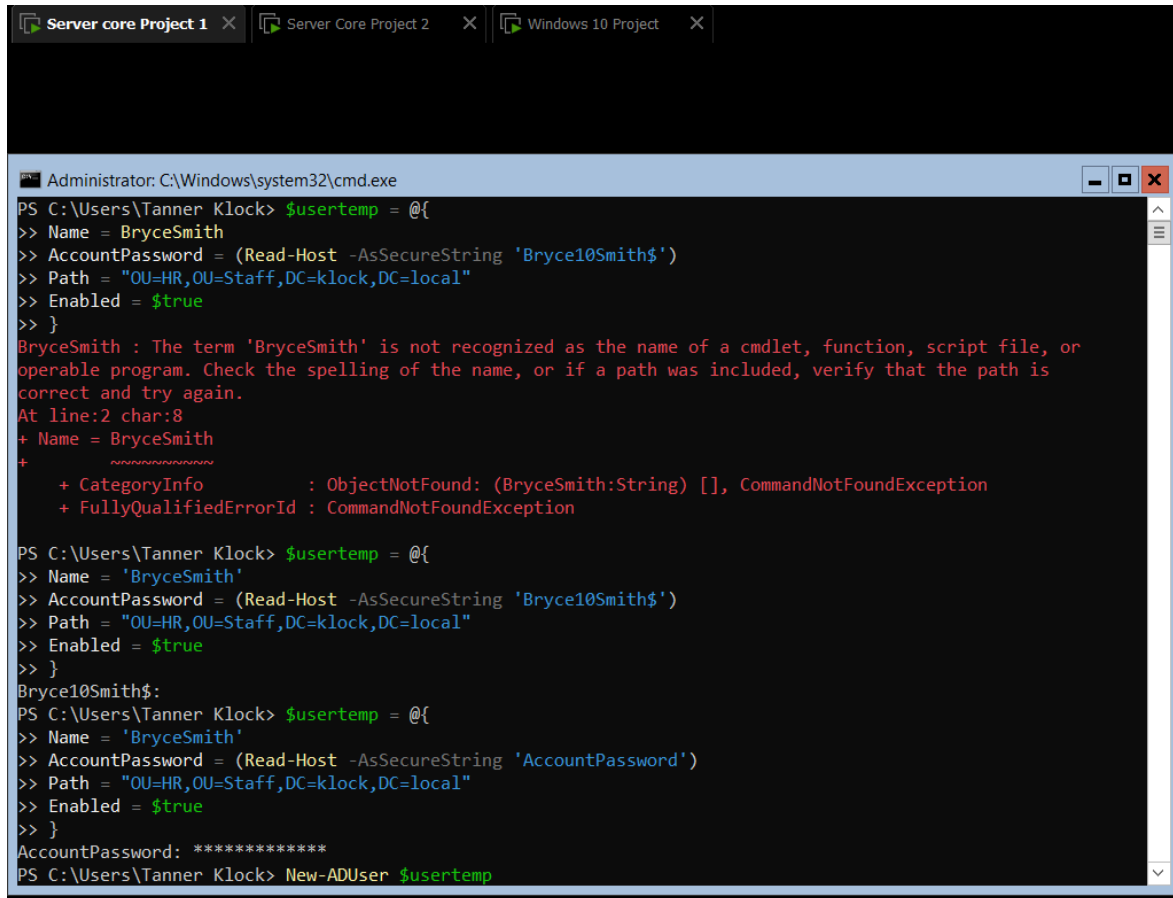
The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window has three tabs at the top: "Server core Project 1", "Server Core Project 2", and "Windows 10 Project". The command prompt shows the following text:

```
PS C:\Users\Tanner Klock> Add-Computer klock.local

cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Credential
WARNING: The changes will take effect after you restart the computer TKSRV02.
PS C:\Users\Tanner Klock> _
```



## Creating Users and OUS:



```
Server core Project 1 | Server Core Project 2 | Windows 10 Project |
Administrator: C:\Windows\system32\cmd.exe
PS C:\Users\Tanner Klock> $usertemp = @{
>> Name = BryceSmith
>> AccountPassword = (Read-Host -AsSecureString 'Bryce10Smith$')
>> Path = "OU=HR,OU=Staff,DC=klock,DC=local"
>> Enabled = $true
>> }
BryceSmith : The term 'BryceSmith' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
At line:2 char:8
+ Name = BryceSmith
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (BryceSmith:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tanner Klock> $usertemp = @{
>> Name = 'BryceSmith'
>> AccountPassword = (Read-Host -AsSecureString 'Bryce10Smith$')
>> Path = "OU=HR,OU=Staff,DC=klock,DC=local"
>> Enabled = $true
>> }
Bryce10Smith$:
PS C:\Users\Tanner Klock> $usertemp = @{
>> Name = 'BryceSmith'
>> AccountPassword = (Read-Host -AsSecureString 'AccountPassword')
>> Path = "OU=HR,OU=Staff,DC=klock,DC=local"
>> Enabled = $true
>> }
AccountPassword: *****
PS C:\Users\Tanner Klock> New-ADUser $usertemp
```

This error occurred due to Powershell interpreting the name field BryceSmith as a cmdlet rather than a string. This was fixed by placing the name within quotation marks.

```
Server core Project 1 X Server Core Project 2 X Windows 10 Project X

Administrator: C:\Windows\system32\cmd.exe

>> Enabled = $true
>> }
AccountPassword: *****
PS C:\Users\Tanner Klock> New-AdUser @usertemp
PS C:\Users\Tanner Klock> $usertemp = @{
>> Name = 'WendyDavid'
>> AccountPassword = (Read-Host -AsSecureString 'AccountPassword')
>> Path = "OU=IT,OU=Staff,DC=klock,DC=local"
>> Enabled = $true
>> }
AccountPassword: *****
PS C:\Users\Tanner Klock> New-AdUser @usertemp
PS C:\Users\Tanner Klock> $usertemp = @{
>> Name = 'DellRio'
>> AccountPassword = (Read-Host -AsSecureString 'AccountPassword')
>> Path = "OU=Admin,OU=Staff,DC=klock,DC=local"
>> Enabled = $true
>> }
AccountPassword: *****
PS C:\Users\Tanner Klock> New-AdUser @usertemp
PS C:\Users\Tanner Klock> $usertemp = @{
>> Name = 'MikeyMcfly'
>> AccountPassword = (Read-Host -AsSecureString 'AccountPassword')
>> Path = "OU=Admin,OU=Staff,DC=klock,DC=local"
>> Enabled = $true
>> }
AccountPassword: *****
PS C:\Users\Tanner Klock> New-AdUser @usertemp
PS C:\Users\Tanner Klock>
```

```
Server core Project 1 X Server Core Project 2 X Windows 10 Project X

Administrator: C:\Windows\system32\cmd.exe
PS C:\Users\Tanner Klock> New-ADOrganizationalUnit -Name "Staff" -Path "DC=klock,DC=local"
PS C:\Users\Tanner Klock> New-ADOrganizationalUnit -Name "HR" -Path "OU=Staff,DC=klock,DC=local"
PS C:\Users\Tanner Klock> New-ADOrganizationalUnit -Name "Admin" -Path "OU=Staff,DC=klock,DC=local"
PS C:\Users\Tanner Klock> New-ADOrganizationalUnit -Name "IT" -Path "OU=Staff,DC=klock,DC=local"
PS C:\Users\Tanner Klock> Get-ADOrganizationalUnit

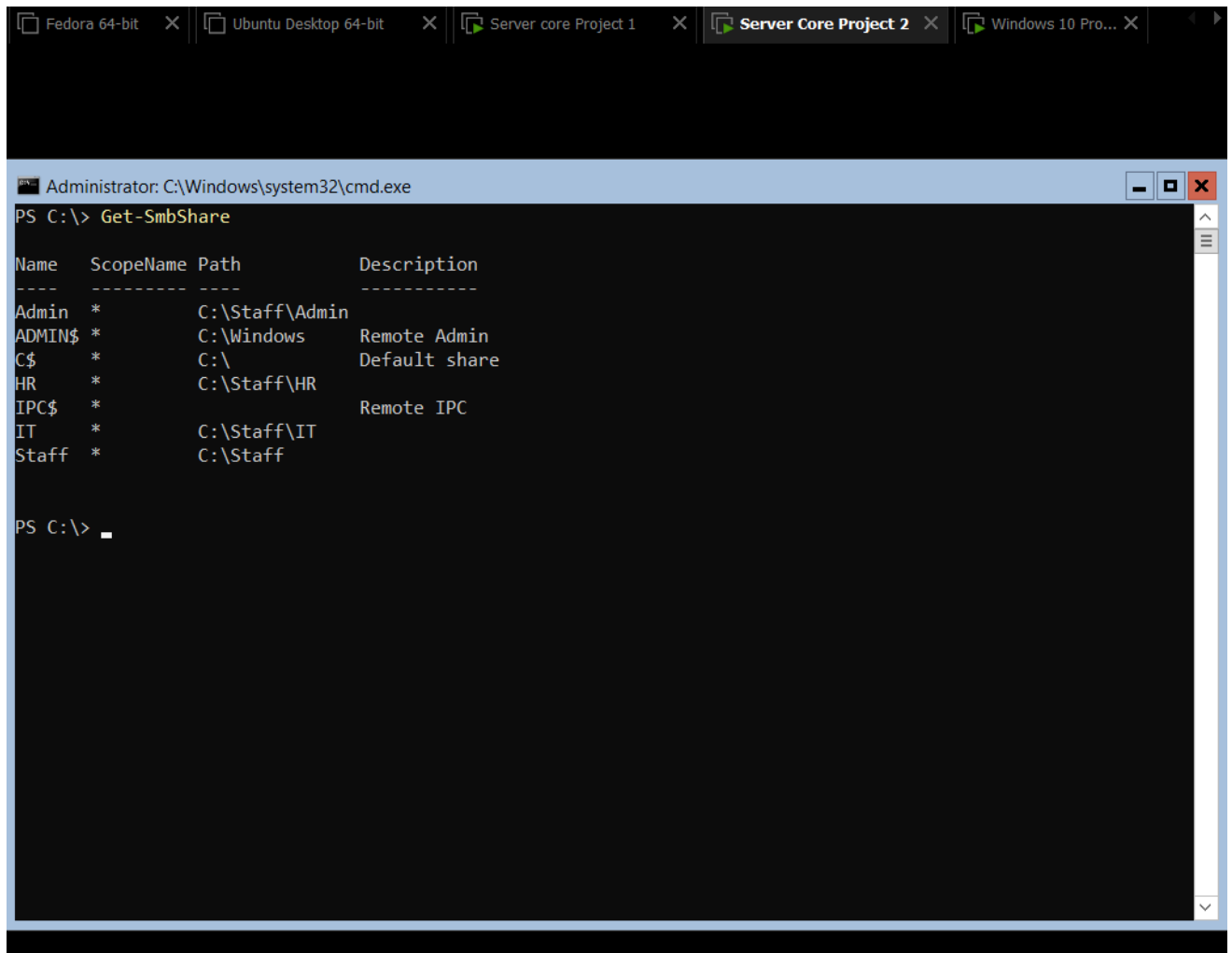
cmdlet Get-ADOrganizationalUnit at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Filter: *

City :
Country :
DistinguishedName : OU=Domain Controllers,DC=klock,DC=local
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=klock,DC=local}
ManagedBy :
Name : Domain Controllers
ObjectClass : organizationalUnit
ObjectGUID : a2a11e7f-933f-47c5-875b-8ddeb406b25d
PostalCode :
State :
StreetAddress :

City :
Country :
DistinguishedName : OU=Staff,DC=klock,DC=local
LinkedGroupPolicyObjects : {}
ManagedBy :
```

## PART 2:

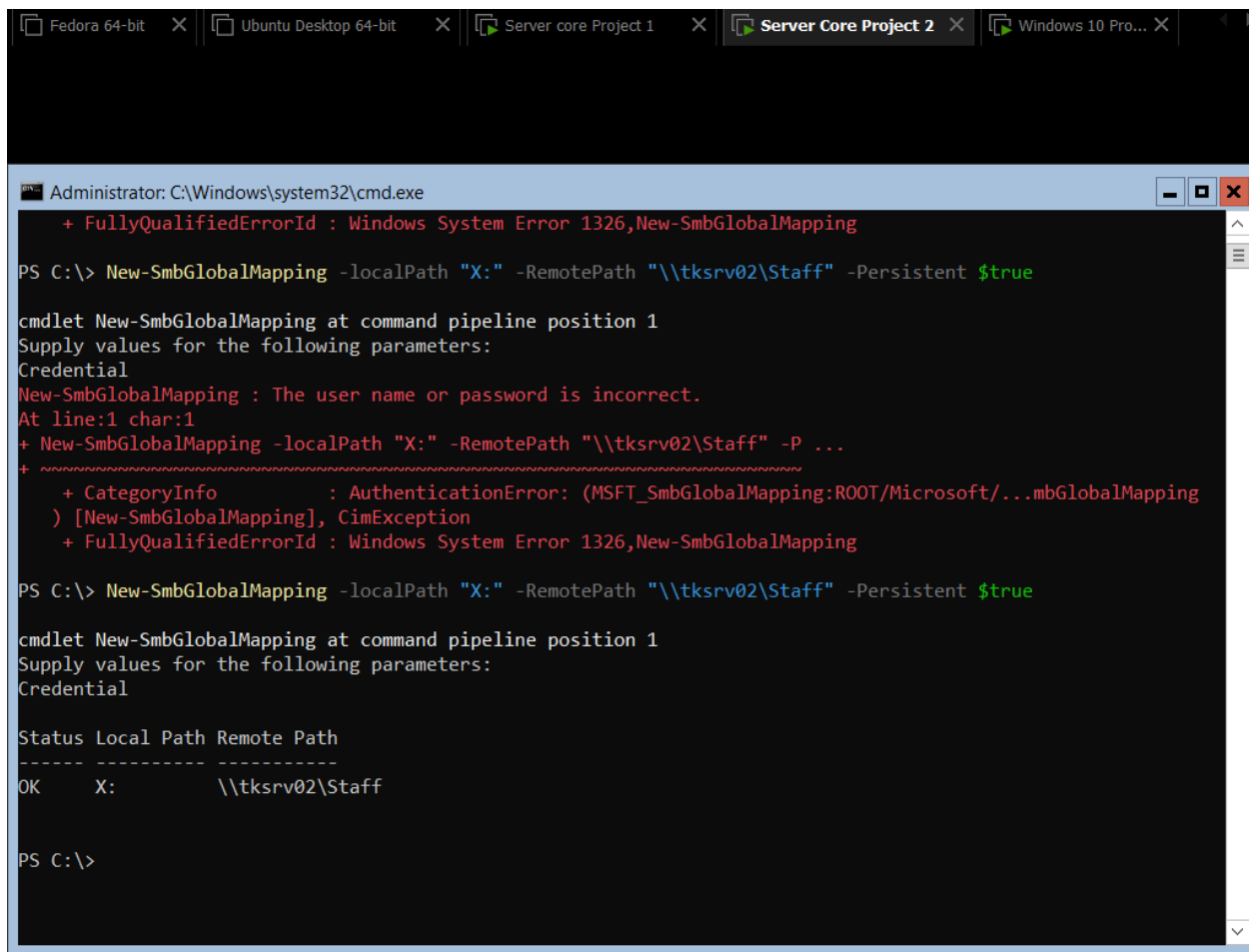
Folder share system that mirrors OUS:



The screenshot shows a Windows taskbar at the top with several open applications: Fedora 64-bit, Ubuntu Desktop 64-bit, Server core Project 1, Server Core Project 2, and Windows 10 Pro... Below the taskbar is a command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The prompt shows the command "Get-SmbShare" has been executed, resulting in a table of SMB shares.

Name	ScopeName	Path	Description
Admin	*	C:\Staff\Admin	
ADMIN\$	*	C:\Windows	Remote Admin
C\$	*	C:\	Default share
HR	*	C:\Staff\HR	
IPC\$	*		Remote IPC
IT	*	C:\Staff\IT	
Staff	*	C:\Staff	

The command prompt shows the prompt "PS C:\>" followed by the command "Get-SmbShare" and the output table. The prompt is currently at "PS C:\>".



```
Administrator: C:\Windows\system32\cmd.exe
+ FullyQualifiedErrorId : Windows System Error 1326,New-SmbGlobalMapping

PS C:\> New-SmbGlobalMapping -localPath "X:" -RemotePath "\\tksrv02\Staff" -Persistent $true

cmdlet New-SmbGlobalMapping at command pipeline position 1
Supply values for the following parameters:
Credential
New-SmbGlobalMapping : The user name or password is incorrect.
At line:1 char:1
+ New-SmbGlobalMapping -localPath "X:" -RemotePath "\\tksrv02\Staff" -P ...
+ ~~~~~
+ CategoryInfo          : AuthenticationError: (MSFT_SmbGlobalMapping:ROOT/Microsoft/...mbGlobalMapping
) [New-SmbGlobalMapping], CimException
+ FullyQualifiedErrorId : Windows System Error 1326,New-SmbGlobalMapping

PS C:\> New-SmbGlobalMapping -localPath "X:" -RemotePath "\\tksrv02\Staff" -Persistent $true

cmdlet New-SmbGlobalMapping at command pipeline position 1
Supply values for the following parameters:
Credential

Status Local Path Remote Path
-----
OK      X:          \\tksrv02\Staff

PS C:\>
```

The error above occurred because we tried to use the local administrator's login information rather than the Active Directory administrator's login information. Once we tried to login using the right credentials, we were able to make the share.

Fedora 64-bit X Ubuntu Desktop 64-bit X Server core Project 1 X Server Core Project 2 X Windows 10 Pro... X

Administrator: C:\Windows\system32\cmd.exe

```
PS C:\Staff> cd X:
PS X:\> ls

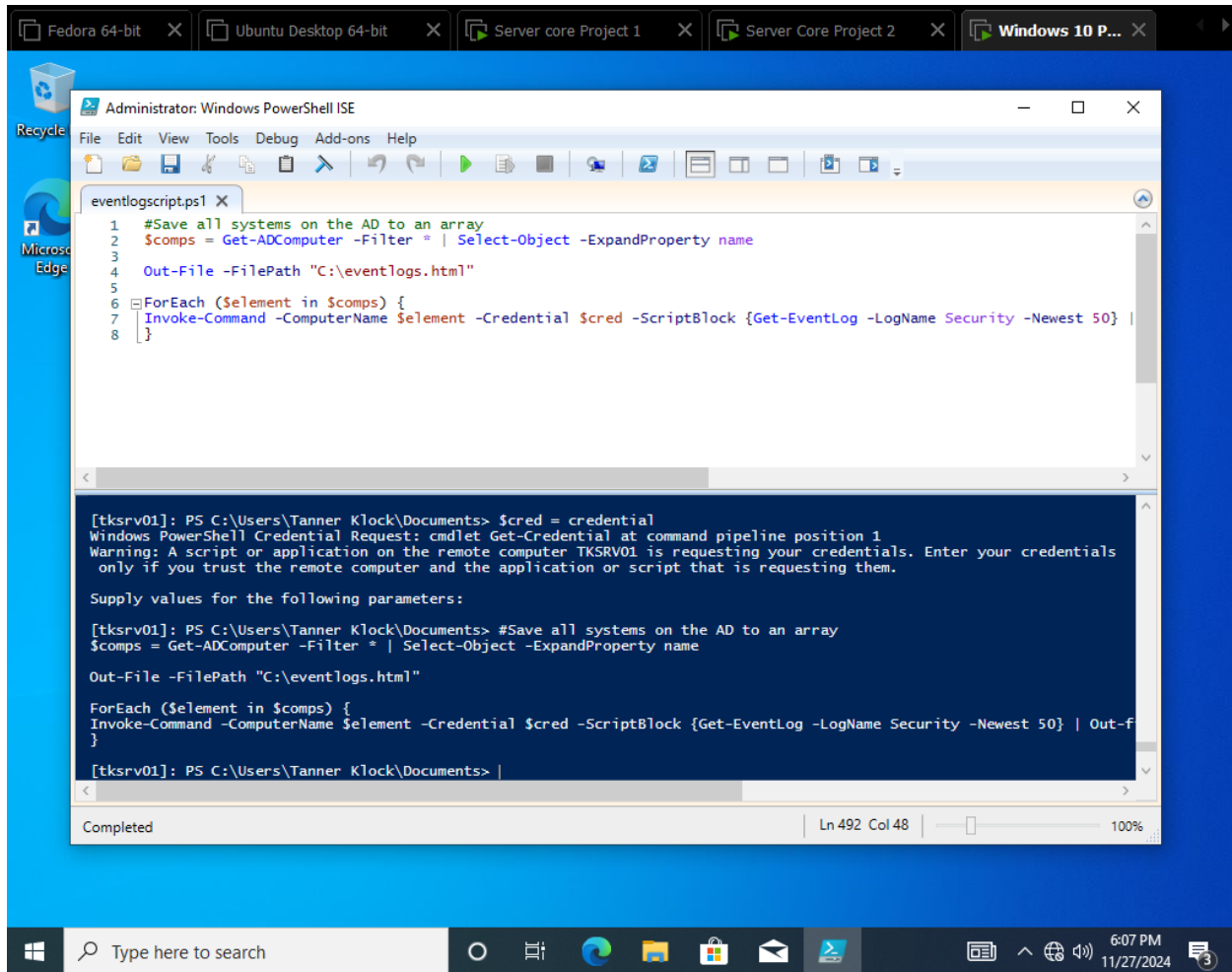
Directory: X:\

Mode                LastWriteTime         Length Name
----                -
d-----         11/27/2024   5:03 PM             Admin
d-----         11/27/2024   5:03 PM             HR
d-----         11/27/2024   5:03 PM             IT

PS X:\>
```



Script to get the 50 latest system and security events:



The screenshot shows a Windows PowerShell ISE window titled "Administrator: Windows PowerShell ISE". The script file is named "eventlogscript.ps1". The script contains the following commands:

```
1 #Save all systems on the AD to an array
2 $comps = Get-ADComputer -Filter * | Select-Object -ExpandProperty name
3
4 Out-File -FilePath "C:\eventlogs.html"
5
6 ForEach ($element in $comps) {
7     Invoke-Command -ComputerName $element -Credential $cred -ScriptBlock {Get-EventLog -LogName Security -Newest 50} |
8 }
```

The console output shows the execution of the script. It starts with a credential request for "cmdlet Get-Credential at command pipeline position 1". A warning message states: "Warning: A script or application on the remote computer TKSRV01 is requesting your credentials. Enter your credentials only if you trust the remote computer and the application or script that is requesting them." The user is prompted to supply values for the following parameters:

```
[tksrv01]: PS C:\Users\Tanner Klock\Documents> #Save all systems on the AD to an array
$comps = Get-ADComputer -Filter * | Select-Object -ExpandProperty name

Out-File -FilePath "C:\eventlogs.html"

ForEach ($element in $comps) {
    Invoke-Command -ComputerName $element -Credential $cred -ScriptBlock {Get-EventLog -LogName Security -Newest 50} | Out-f
}
```

The console output ends with the prompt: [tksrv01]: PS C:\Users\Tanner Klock\Documents> |

The status bar at the bottom of the PowerShell ISE window indicates "Completed" and "Ln 492 Col 48".

```
Fedora 64-bit X Ubuntu Desktop 64-bit X Server core Project 1 X Server Core Project 2 X Windows 10 Pro... X
Administrator: C:\Windows\system32\cmd.exe
GroupCategory : Security
GroupScope : Global
Name : DnsUpdateProxy
ObjectClass : group
ObjectGUID : 5b5628bd-d25a-4d8d-8433-4ad3a6ac0701
SamAccountName : DnsUpdateProxy
SID : S-1-5-21-3603142376-4199937490-3948543780-1103

PS C:\Users\Tanner Klock>
PS C:\Users\Tanner Klock> Add-ADGroupMember -Identity Administrators -Members "Tanner Klock"
PS C:\Users\Tanner Klock> cd C:\
PS C:\> ls

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          5/8/2021   4:15 AM                PerfLogs
d-r-----       11/26/2024  10:54 AM                Program Files
d-----          5/8/2021   5:34 AM                Program Files (x86)
d-r-----       11/26/2024  11:06 AM                Users
d-----       11/27/2024   4:27 PM                Windows
-a-----       11/27/2024   6:06 PM          37166 eventlogs.html

PS C:\>
```

```
Administrator: C:\Windows\system32\cmd.exe
PS C:\> cat eventlogs.html

Index Time          EntryType Source                InstanceID Message                                PSComputerName
-----
4183 Nov 27 18:06 SuccessA... Microsoft-Windows... 4634 An account was logged... TKSRV01
4182 Nov 27 18:06 SuccessA... Microsoft-Windows... 4624 An account was succes... TKSRV01
4181 Nov 27 18:06 SuccessA... Microsoft-Windows... 4672 Special privileges as... TKSRV01
4180 Nov 27 18:06 SuccessA... Microsoft-Windows... 4634 An account was logged... TKSRV01
4179 Nov 27 18:06 SuccessA... Microsoft-Windows... 4624 An account was succes... TKSRV01
4178 Nov 27 18:06 SuccessA... Microsoft-Windows... 4672 Special privileges as... TKSRV01
4177 Nov 27 18:06 SuccessA... Microsoft-Windows... 4634 An account was logged... TKSRV01
4176 Nov 27 18:06 SuccessA... Microsoft-Windows... 4624 An account was succes... TKSRV01
4175 Nov 27 18:06 SuccessA... Microsoft-Windows... 4672 Special privileges as... TKSRV01
4174 Nov 27 18:05 SuccessA... Microsoft-Windows... 4648 A logon was attempted... TKSRV01
4173 Nov 27 18:05 SuccessA... Microsoft-Windows... 4648 A logon was attempted... TKSRV01
4172 Nov 27 18:05 SuccessA... Microsoft-Windows... 4648 A logon was attempted... TKSRV01
```

Script:

```
$comps = Get-ADComputer -Filter * | Select-Object -ExpandProperty name
```

```
Out-File -FilePath "C:\eventlogs.html"
```

```
ForEach ($element in $comps) {
```

```
Invoke-Command -ComputerName $element -Credential $cred -ScriptBlock {Get-EventLog -LogName
Security -Newest 50} | Out-file -Append -FilePath "C:\eventlogs.html"
```

```
}
```

Schedule script to run once a day:

