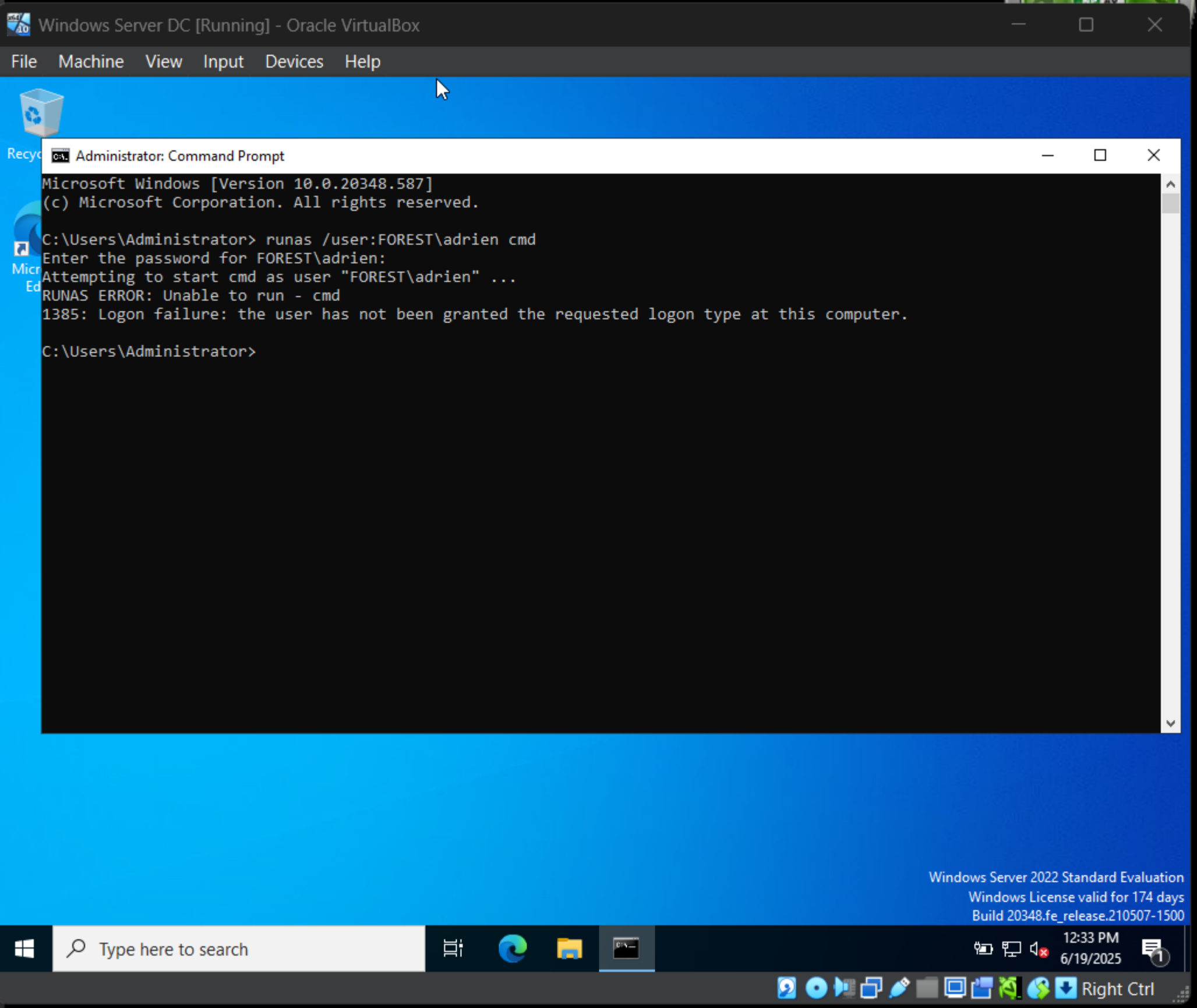
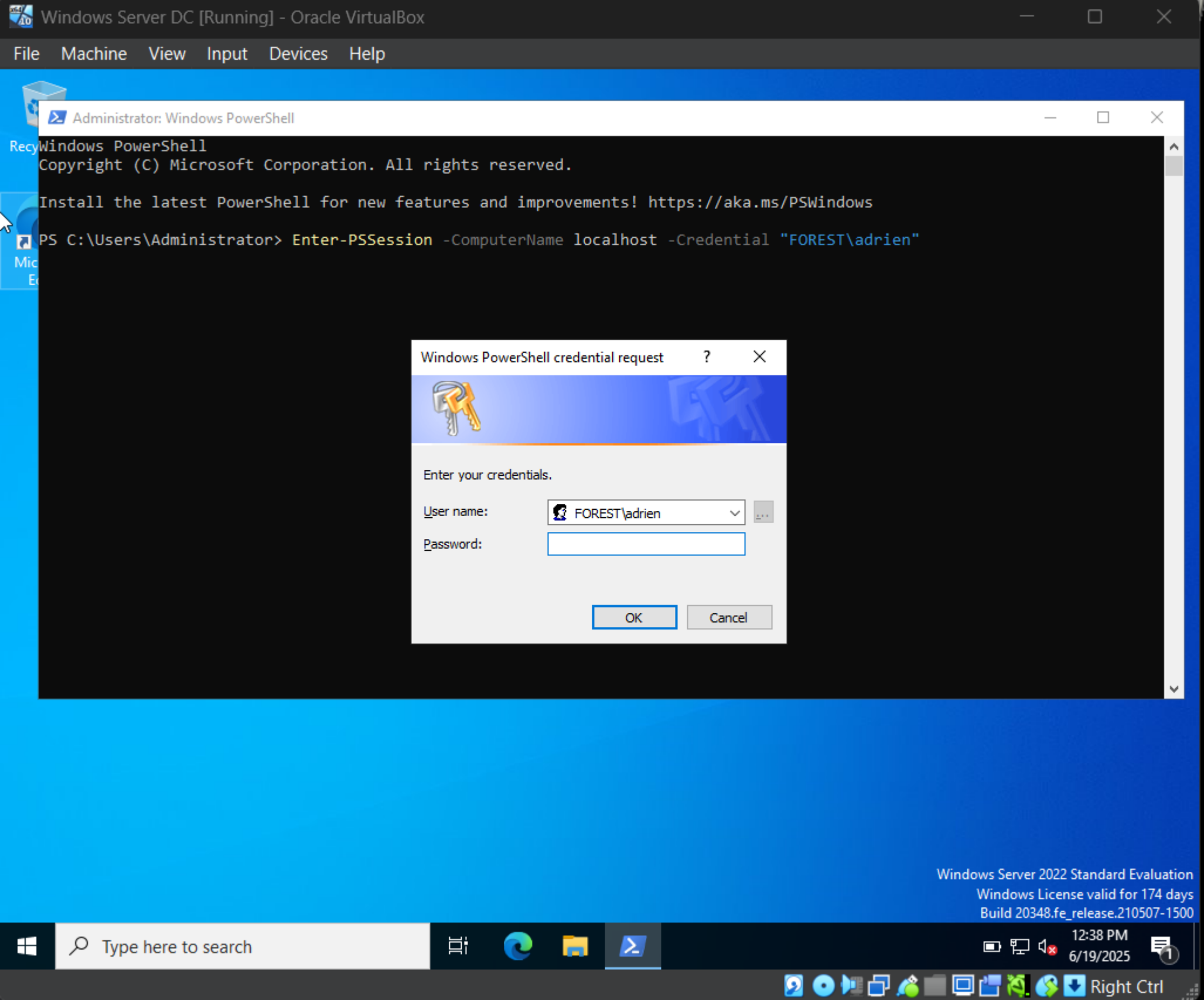
Administrator: Windows PowerShell

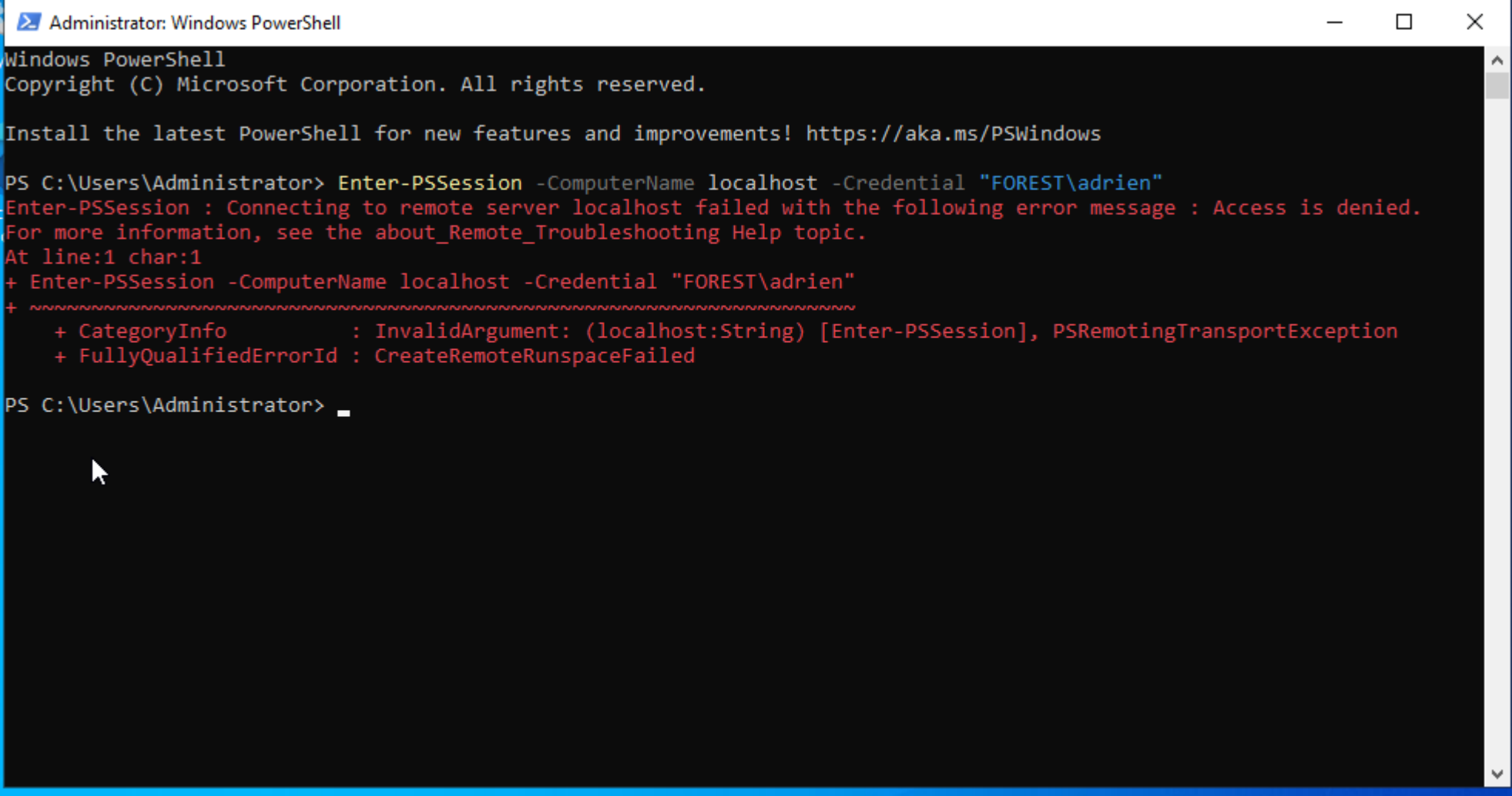
```
PS C:\Users\Administrator>  Get-ADOrganizationalUnit -Filter * | ForEach-Object { (Get-Acl "AD:\$($_.DistinguishedName)"
).Access | Where-Object { $_.IdentityReference -like "*DOMAIN*" } | Select-Object @{n='OU';e={$_.DistinguishedName}}, Id
entityReference, ActiveDirectoryRights
>> }
>>

OU IdentityReference                                                                               ActiveDirectoryRights
-- -----------------                                                                               ---------------------
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
   FOREST\Domain Admins                          ...Self, WriteProperty, ExtendedRight, GenericRead, WriteDacl, WriteOwner
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
   FOREST\Domain Admins                                                                                       GenericAll
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
   FOREST\Domain Admins                                                                                       GenericAll
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
   FOREST\Domain Admins                                                                                       GenericAll
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
   FOREST\Domain Admins                                                                                       GenericAll
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
   FOREST\Domain Admins                                                                                       GenericAll
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                               ReadProperty
   NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                                                                GenericRead
```

Administrator: Windows PowerShell

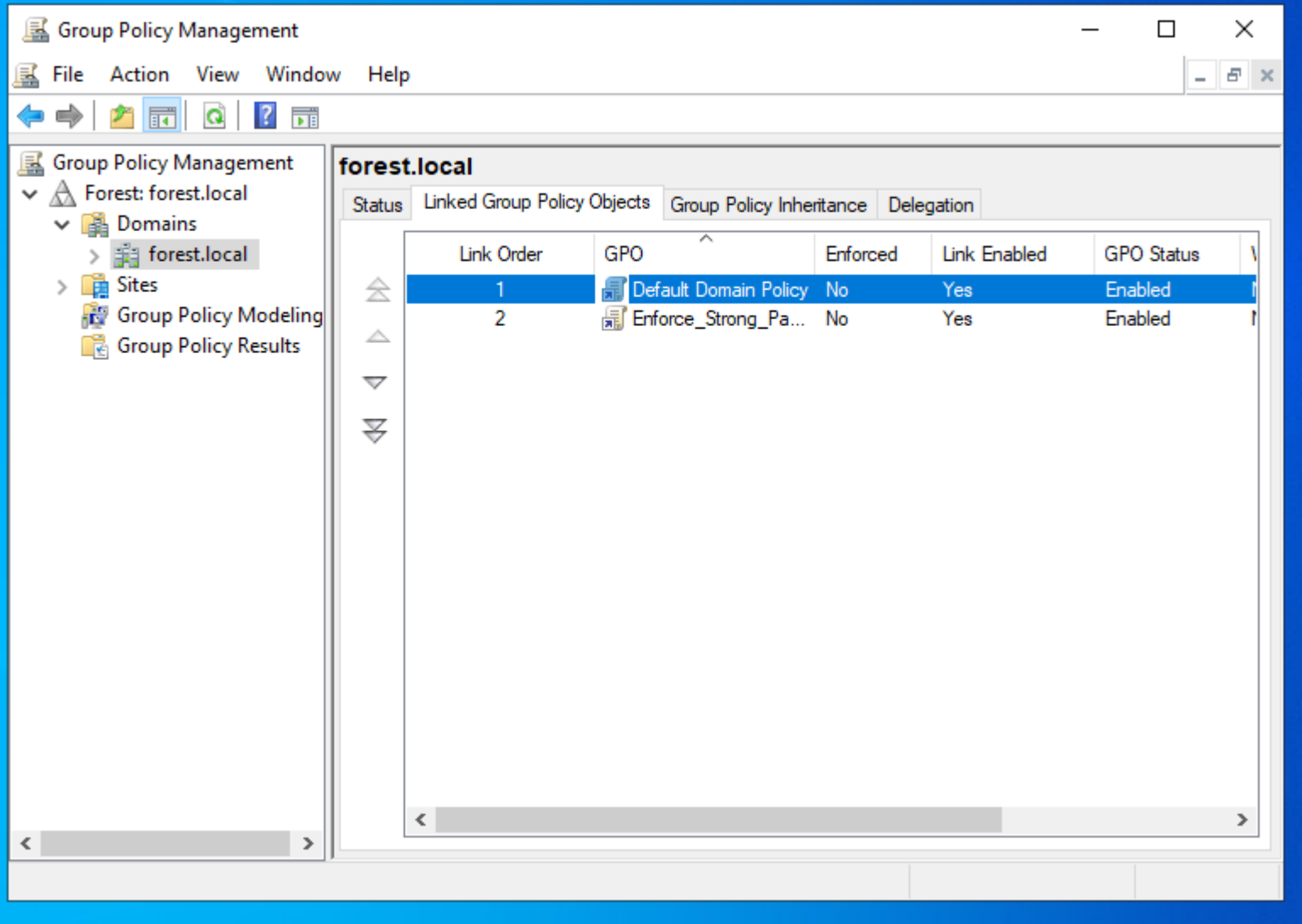
```
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                       GenericRead
FOREST\Domain Admins                                              GenericAll
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS                      ReadProperty
```

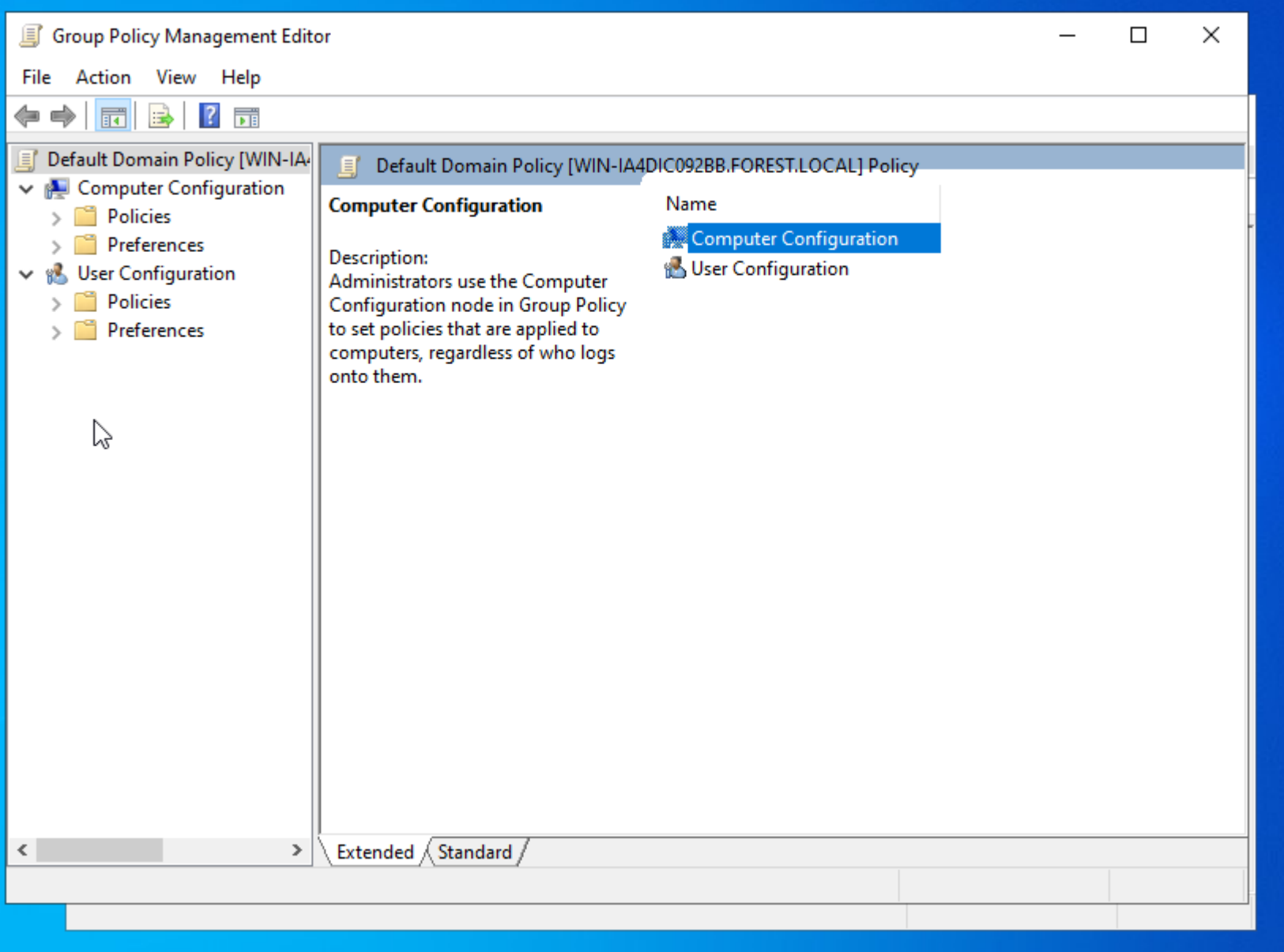

Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator> runas /user:FOREST\adrien cmd
Enter the password for FOREST\adrien:
Attempting to start cmd as user "FOREST\adrien" ...
RUNAS ERROR: Unable to run - cmd
1385: Logon failure: the user has not been granted the requested logon type at this computer.
C:\Users\Administrator>
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Type here to search
12:33 PM
6/19/2025
Right Ctrl

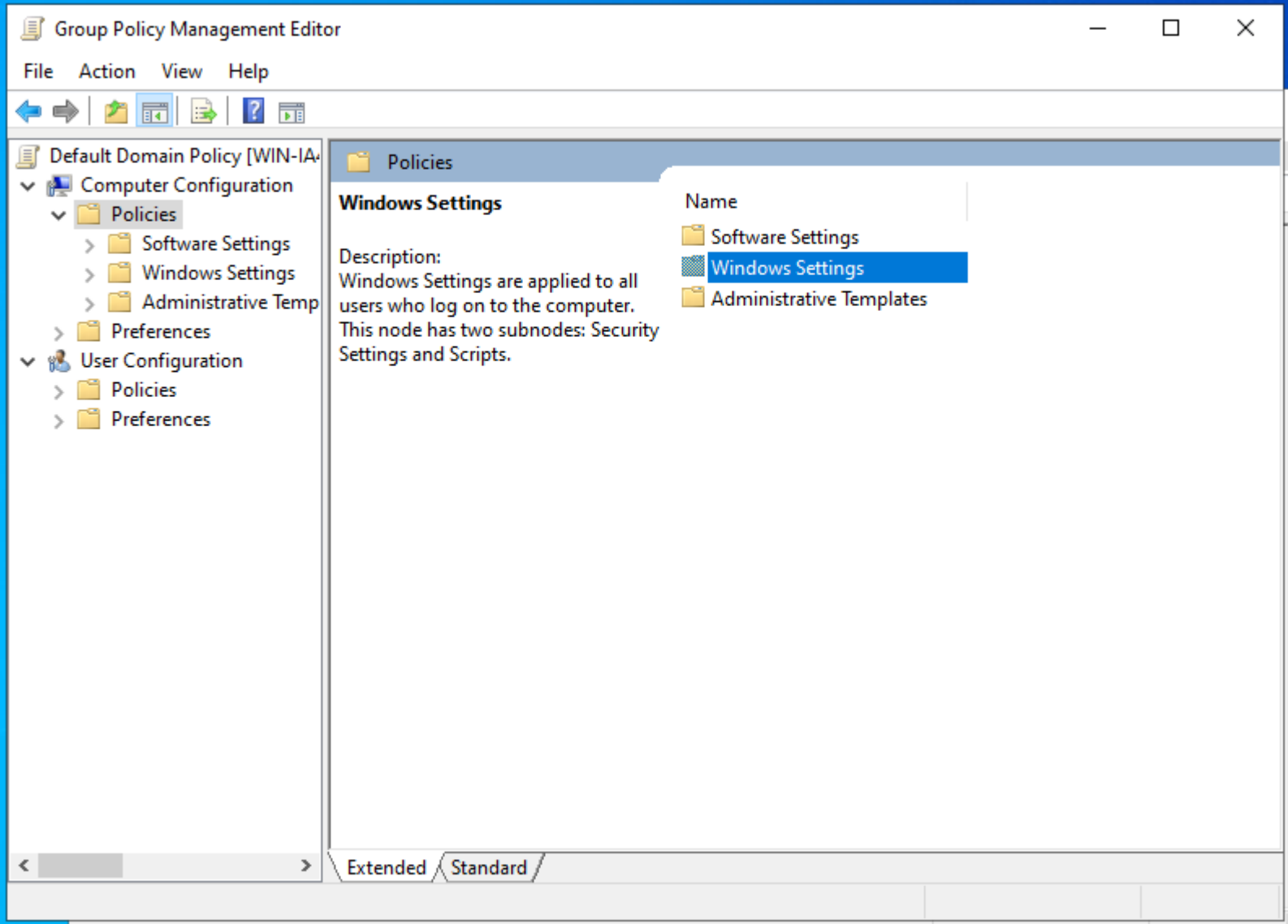

Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> Enter-PSSession -ComputerName localhost -Credential "FOREST\adrien"
Windows PowerShell credential request
Enter your credentials.
User name:
FOREST\adrien
Password:
OK
Cancel
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Type here to search
12:38 PM
6/19/2025
Right Ctrl

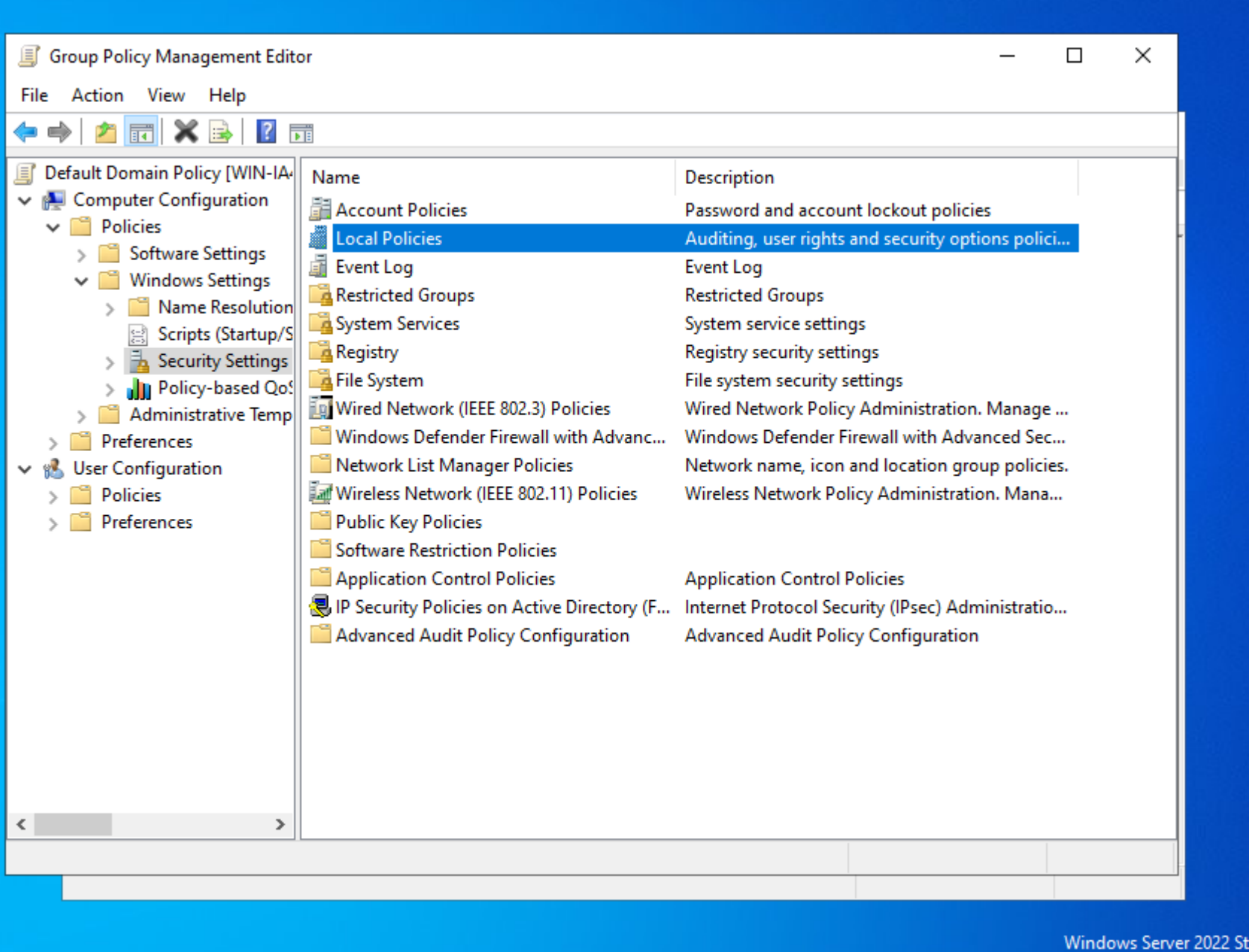

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> Enter-PSSession -ComputerName localhost -Credential "FOREST\adrien"
Enter-PSSession : Connecting to remote server localhost failed with the following error message : Access is denied.
For more information, see the about_Remote_Troubleshooting Help topic.
At line:1 char:1
+ Enter-PSSession -ComputerName localhost -Credential "FOREST\adrien"
+ ~~~~~~
+ CategoryInfo : InvalidArgument: (localhost:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
PS C:\Users\Administrator>

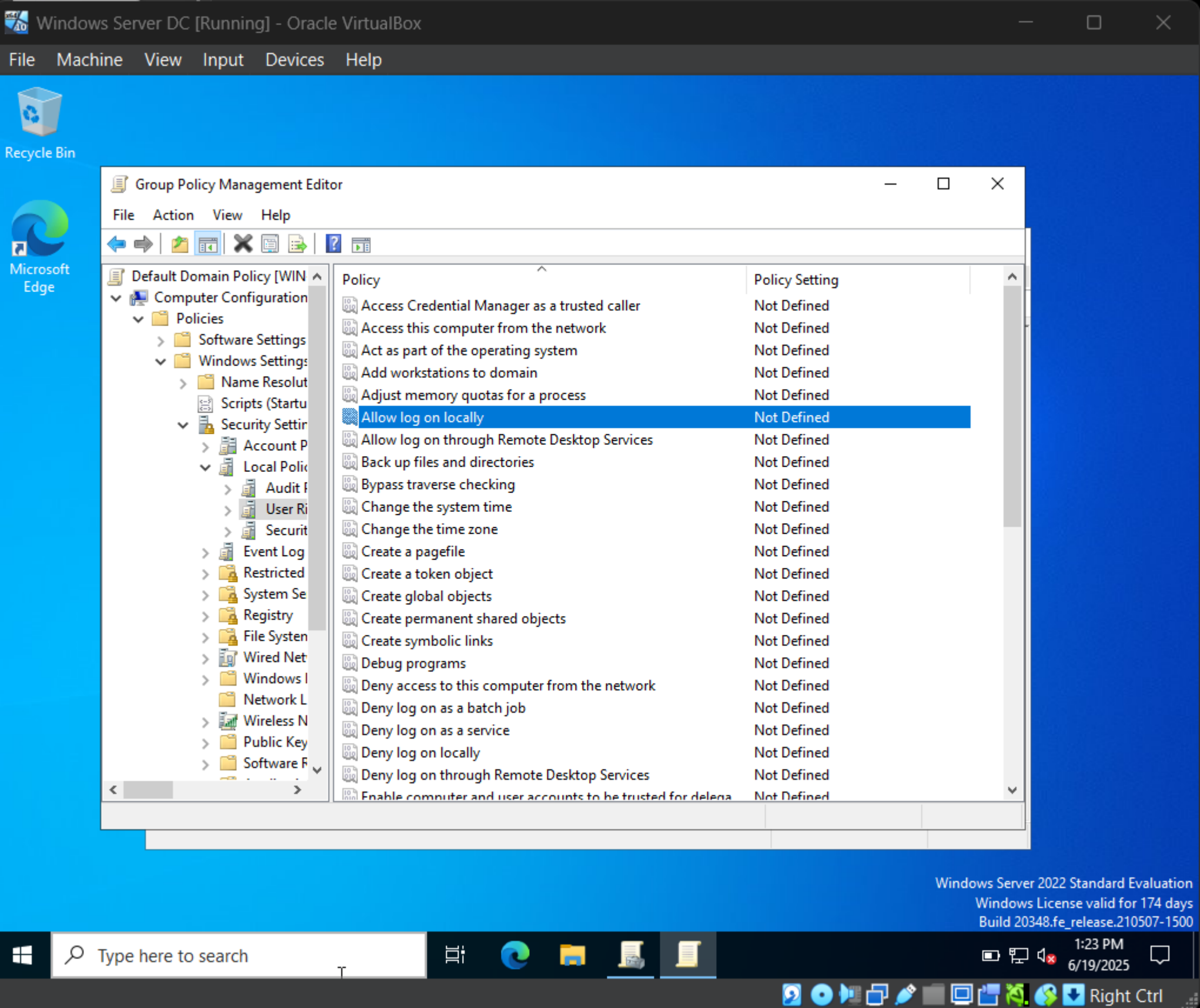
```
PS C:\Users\Administrator> $cred = Get-Credential "FOREST\adrien"
PS C:\Users\Administrator> Start-Process "cmd.exe" -Credential $cred -NoNewWindow -ArgumentList "/c whoami > C:\temp\adr
ien_test.txt"
Start-Process : This command cannot be run due to the error: Logon failure: the user has not been granted the
requested logon type at this computer.
At line:1 char:1
+ Start-Process "cmd.exe" -Credential $cred -NoNewWindow -ArgumentList  ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Start-Process], InvalidOperationException
    + FullyQualifiedErrorId : InvalidOperationException,Microsoft.PowerShell.Commands.StartProcessCommand

PS C:\Users\Administrator> Test-AdfsAuthentication -Server localhost -Credential $cred
Test-AdfsAuthentication : The term 'Test-AdfsAuthentication' 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:1 char:1
+ Test-AdfsAuthentication -Server localhost -Credential $cred
+ ~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Test-AdfsAuthentication:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Administrator>
```

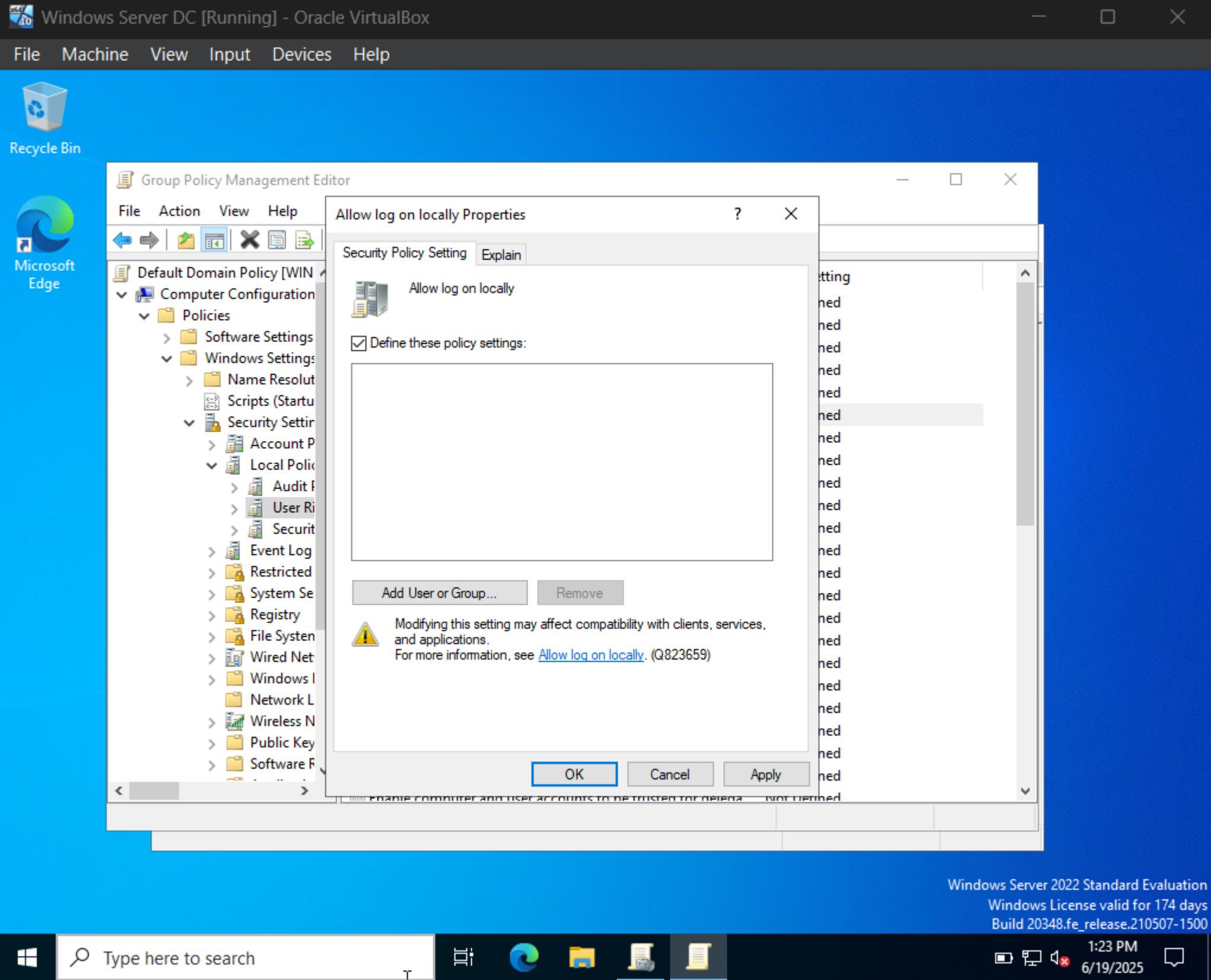

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: forest.local
Domains
forest.local
Sites
Group Policy Modeling
Group Policy Results
forest.local
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1
Default Domain Policy
No
Yes
Enabled
2
Enforce_Strong_Pa...
No
Yes
Enabled

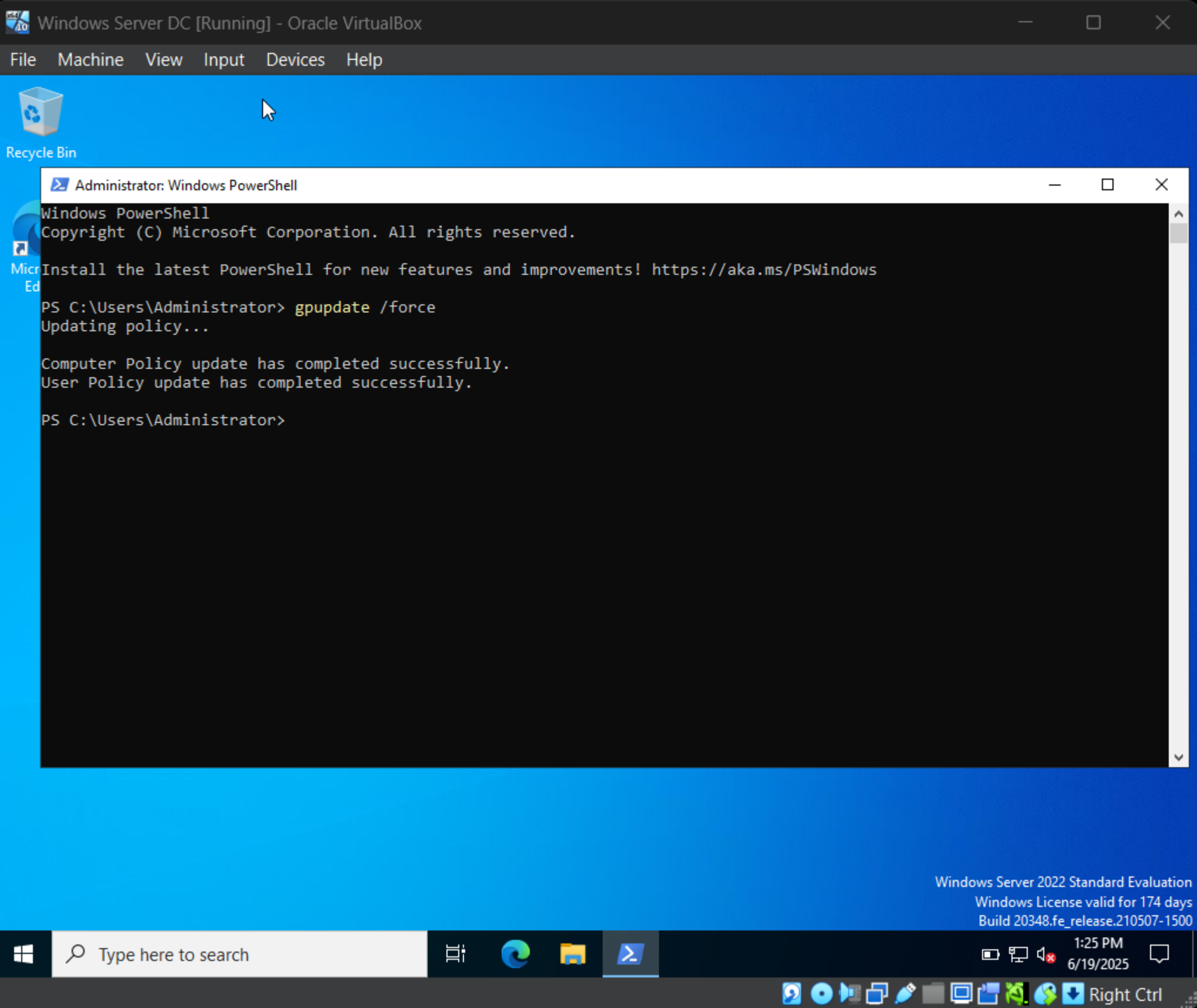

Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [WIN-IA
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [WIN-IA4DIC092BB.FOREST.LOCAL] Policy
Computer Configuration
Description:
Administrators use the Computer Configuration node in Group Policy to set policies that are applied to computers, regardless of who logs onto them.
Name
Computer Configuration
User Configuration
Extended
Standard

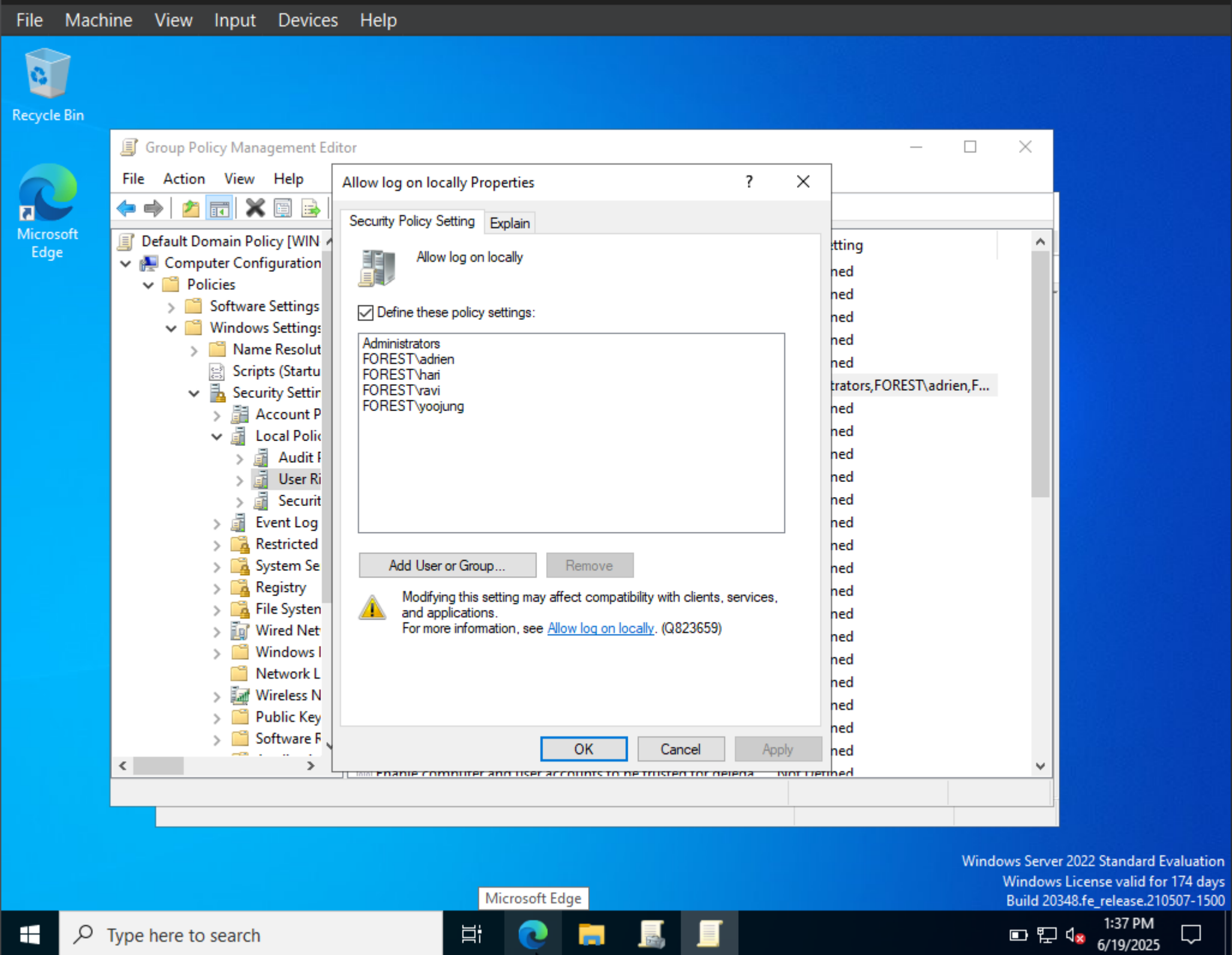

Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [WIN-IA
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Preferences
User Configuration
Policies
Preferences
Policies
Windows Settings
Description:
Windows Settings are applied to all users who log on to the computer. This node has two subnodes: Security Settings and Scripts.
Name
Software Settings
Windows Settings
Administrative Templates
Extended
Standard

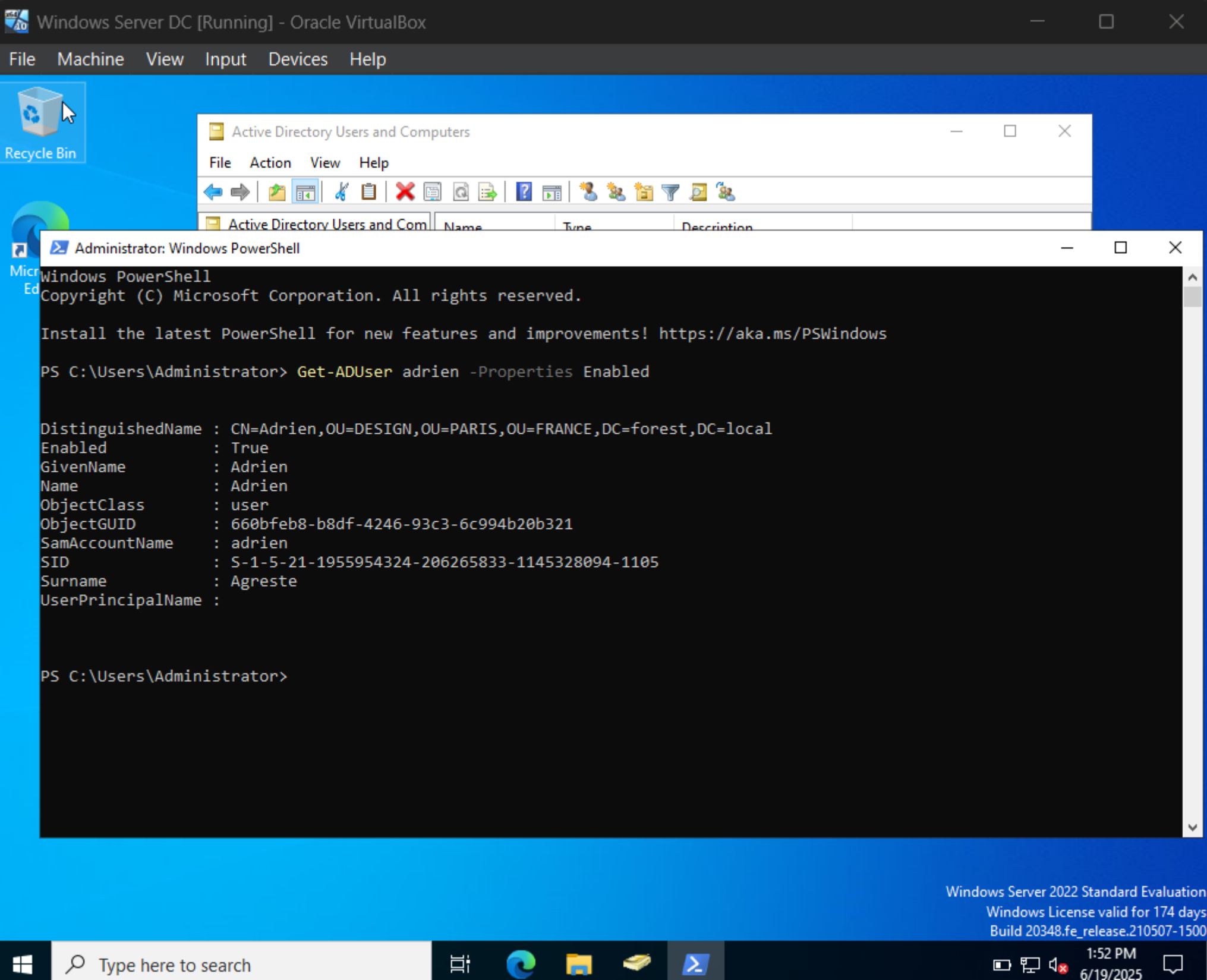

Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN-IA
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution
Scripts (Startup/S
Security Settings
Policy-based QoS
Administrative Temp
Preferences
User Configuration
Policies
Preferences
Name
Description
Account Policies
Password and account lockout policies
Local Policies
Auditing, user rights and security options polici...
Event Log
Event Log
Restricted Groups
Restricted Groups
System Services
System service settings
Registry
Registry security settings
File System
File system security settings
Wired Network (IEEE 802.3) Policies
Wired Network Policy Administration. Manage ...
Windows Defender Firewall with Advanc...
Windows Defender Firewall with Advanced Sec...
Network List Manager Policies
Network name, icon and location group policies.
Wireless Network (IEEE 802.11) Policies
Wireless Network Policy Administration. Mana...
Public Key Policies
Software Restriction Policies
Application Control Policies
Application Control Policies
IP Security Policies on Active Directory (F...
Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration
Advanced Audit Policy Configuration
Windows Server 2022 St

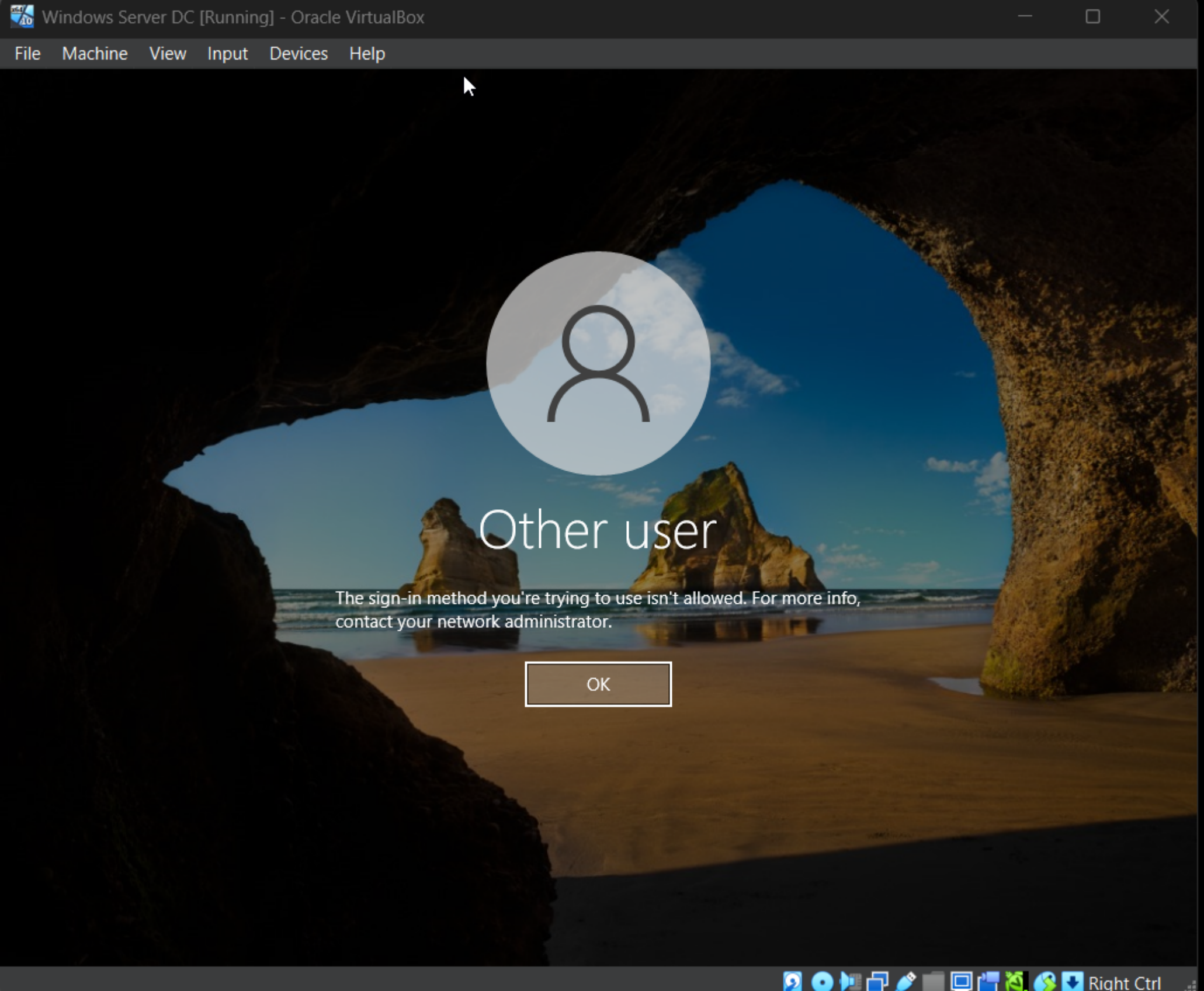

Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Local Polic
Audit P
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software R
Policy
Policy Setting
Access Credential Manager as a trusted caller Not Defined
Access this computer from the network Not Defined
Act as part of the operating system Not Defined
Add workstations to domain Not Defined
Adjust memory quotas for a process Not Defined
Allow log on locally Not Defined
Allow log on through Remote Desktop Services Not Defined
Back up files and directories Not Defined
Bypass traverse checking Not Defined
Change the system time Not Defined
Change the time zone Not Defined
Create a pagefile Not Defined
Create a token object Not Defined
Create global objects Not Defined
Create permanent shared objects Not Defined
Create symbolic links Not Defined
Debug programs Not Defined
Deny access to this computer from the network Not Defined
Deny log on as a batch job Not Defined
Deny log on as a service Not Defined
Deny log on locally Not Defined
Deny log on through Remote Desktop Services Not Defined
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Type here to search
1:23 PM
6/19/2025
Right Ctrl


Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Local Polic
Audit P
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software R
Allow log on locally Properties
Security Policy Setting
Explain
Allow log on locally
Define these policy settings:
Add User or Group...
Remove
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)
OK
Cancel
Apply
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Type here to search
1:23 PM
6/19/2025


Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\Users\Administrator>
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Type here to search
1:25 PM
6/19/2025
Right Ctrl


File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Local Polic
Audit F
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Allow log on locally Properties
Security Policy Setting
Explain
Allow log on locally
Define these policy settings:
Administrators
FOREST\adrien
FOREST\hari
FOREST\ravi
FOREST\yoojung
Add User or Group...
Remove
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)
OK
Cancel
Apply
trators,FOREST\adrien,F...
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Microsoft Edge
Type here to search
1:37 PM
6/19/2025


Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Name
Type
Description
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Administrator> Get-ADUser adrien -Properties Enabled
DistinguishedName : CN=Adrien,OU=DESIGN,OU=PARIS,OU=FRANCE,DC=forest,DC=local
Enabled : True
GivenName : Adrien
Name : Adrien
ObjectClass : user
ObjectGUID : 660bfeb8-b8df-4246-93c3-6c994b20b321
SamAccountName : adrien
SID : S-1-5-21-1955954324-206265833-1145328094-1105
Surname : Agreste
UserPrincipalName :
PS C:\Users\Administrator>
Windows Server 2022 Standard Evaluation
Windows License valid for 174 days
Build 20348.fe_release.210507-1500
Type here to search
1:52 PM
6/19/2025


Windows Server DC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Other user
The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.
OK
Right Ctrl

> 🔐 Built entirely using PowerShell and hands-on configuration inside a virtual environment.

OU Structure to be implemented :

forest.local ├── OU=INDIA │ ├── OU=PUNE │ │ └── OU=MARKETING (User: Ravi) │ └── OU=CHENNAI │ └── OU=HR (User: Hari) ├── OU=FRANCE │ └── OU=PARIS │ └── OU=DESIGN (User: Adrien) └── OU=SOUTH_KOREA └── OU=SEOUL └── OU=MARKETING (User: Kim Yoo Jung)

```
PS C:\Users\Administrator> Get-WinEvent -LogName Security -MaxEvents 20 | Where-Object { $_.Id -in (4624,4625,4724,4769)
 } | Format-table TimeCreated,Id,Message -AutoSize

TimeCreated              Id Message
-----------              -- -------
6/20/2025 4:55:31 PM 4624 An account was successfully logged on....
6/20/2025 4:54:31 PM 4624 An account was successfully logged on....
6/20/2025 4:53:31 PM 4624 An account was successfully logged on....
6/20/2025 4:53:31 PM 4624 An account was successfully logged on....
6/20/2025 4:53:31 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:58 PM 4624 An account was successfully logged on....
6/20/2025 4:52:57 PM 4624 An account was successfully logged on....
```

```
PS C:\Users\Administrator> Add-ADGroupMember -Identity "Remote Management Users" -Members " adrien", "ravi", "hari", "yo
ojung"
PS C:\Users\Administrator> Enable-PSRemoting
PS C:\Users\Administrator> Enable-PSRemoting -Force
PS C:\Users\Administrator> Test-WSMan -ComputerName localhost -Credential (Get-Credential "forest\adrien")
Test-WSMan : The WinRM client could not process the request because credentials were specified along with the 'no
authentication' flag.   No user name, password or client certificate should be specified with the 'no authentication'
option.
At line:1 char:1
+ Test-WSMan -ComputerName localhost -Credential (Get-Credential "fores ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Test-WSMan], InvalidOperationException
    + FullyQualifiedErrorId : WsManError,Microsoft.WSMan.Management.TestWSManCommand

PS C:\Users\Administrator> _
```

```
PS C:\Users\Administrator> winrm get winrm/config/service
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
        Basic = false
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true
```