```
PS C:\Users\Administrator> winrm set winrm/config/service/auth '@{Basic="true"}'
Auth
    Basic = true
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed
```

```
                          cbthardeningLevel = Relaxed

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> Test-WSMan -ComputerName localhost -Credential (Get-Credential "forest\ravi")
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
```
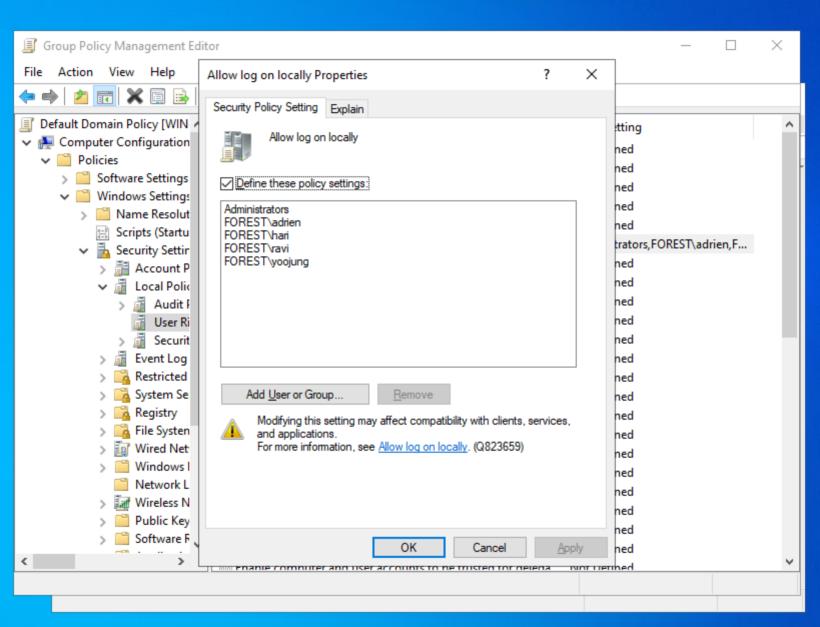
```
PS C:\Users\Administrator> winrm set winrm/config/service/auth '@{Kerberos="true";Negotiate="true"}'
Auth
    Basic = true
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed

PS C:\Users\Administrator> Test-WSMan -ComputerName localhost -Credential (Get-Credential "forest\ravi")
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> _
```

```
Administrator: Windows PowerShell                                    —  □  ✕

PS C:\Users\Administrator> New-ADGroup -Name "Workstation_Users" -GroupScope Global -Path "OU=GROUPS, DC=forest, DC=loca
l" -Description "Users allowed to log on to workstations"
PS C:\Users\Administrator> Add-ADGroupMember -Identity "Workstation_Users" -Members " adrien", "ravi", "hari", "yoojung"

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on ⌐6/⌐20/⌐2025 at 8:50:42 PM


RSOP data for FOREST\Administrator on WIN-IA4DIC092BB : Logging Mode
----------------------------------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
-----------------
    CN=WIN-IA4DIC092BB,OU=Domain Controllers,DC=forest,DC=local
    Last time Group Policy was applied: 6/20/2025 at 8:50:11 PM
    Group Policy was applied from:      WIN-IA4DIC092BB.forest.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        FOREST
```

```
Site Name:                       Default-First-Site-Name
Roaming Profile:                 N/A
Local Profile:                   C:\Users\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
-----------------
    CN=WIN-IA4DIC092BB,OU=Domain Controllers,DC=forest,DC=local
    Last time Group Policy was applied: 6/20/2025 at 8:50:11 PM
    Group Policy was applied from:      WIN-IA4DIC092BB.forest.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        FOREST
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        Default Domain Controllers Policy
        Default Domain Policy
        Enforce_Strong_Passwords
        Local Group Policy

    The computer is a part of the following security groups
    -------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Pre-Windows 2000 Compatible Access
        BUILTIN\Users
        Windows Authorization Access Group
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        This Organization
        WIN-IA4DIC092BB$
        Domain Controllers
        NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
        Authentication authority asserted identity
        Denied RODC Password Replication Group
        System Mandatory Level


USER SETTINGS
-------------
    CN=Administrator,CN=Users,DC=forest,DC=local
```

```
        Denied RODC Password Replication Group
        System Mandatory Level


USER SETTINGS
-------------
    CN=Administrator,CN=Users,DC=forest,DC=local
    Last time Group Policy was applied: 6/20/2025 at 8:50:12 PM
    Group Policy was applied from:      WIN-IA4DIC092BB.forest.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        FOREST
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ---------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    ------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        BUILTIN\Pre-Windows 2000 Compatible Access
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Domain Admins
        Group Policy Creator Owners
        Schema Admins
        Enterprise Admins
        Authentication authority asserted identity
        Denied RODC Password Replication Group
        High Mandatory Level

PS C:\Users\Administrator> Add-ADGriupMember -Identity "Remote Management Users" -Members " adrien", "ravi", "hari", "yoojun
```

```
PS C:\Users\Administrator> Get-ADGroupMember -Identity "Workstation_Users" | Select-Object Name, SamAccountName

Name           SamAccountName
----           --------------
Ravi           ravi
Hari           hari
Adrien         adrien
Kim Yoo Jung   yoojung
```

```
PS C:\Users\Administrator> Get-GPRegistryValue -Name "Default Domain Policy" -Key "HKLM\SOFTWARE\Microsoft\Windows\CureentVe
rsion\Policies\System" -ValueName "SeInteractiveLogonRight"
Get-GPRegistryValue : The following Group Policy registry setting was not found:
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CureentVersion\Policies\System SeInteractiveLogonRight".
Parameter name: keyPath
At line:1 char:1
+ Get-GPRegistryValue -Name "Default Domain Policy" -Key "HKLM\SOFTWARE ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (Microsoft.Group...tryValueCommand:GetGPRegistryValueCommand) [Get-GPRegist
   ryValue], ArgumentException
    + FullyQualifiedErrorId : UnableToRetrievePolicyRegistryItem,Microsoft.GroupPolicy.Commands.GetGPRegistryValueCommand


PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> Get-ADUser -Identity ravi -Properties PasswordExpired, LockedOut, Enabled


DistinguishedName : CN=Ravi,OU=MARKETING,OU=PUNE,OU=INDIA,DC=forest,DC=local
Enabled           : True
GivenName         : Ravi
LockedOut         : False
Name              : Ravi
ObjectClass       : user
ObjectGUID        : 8542a2a6-db96-4bdc-8e0b-6851f505a27f
PasswordExpired   : False
SamAccountName    : ravi
SID               : S-1-5-21-1955954324-206265833-1145328094-1103
Surname           : Sharma
UserPrincipalName :



PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Administrator: Windows PowerShell

```
Windows Event Collector service was configured successfully.
PS C:\Users\Administrator> winrm quickconfig
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Users\Administrato
PS C:\Users\Administrato
Windows Event Collector
PS C:\Users\Administrato
Subscription Id: MyForwa
SubscriptionType: Source
Description: Critical ev
Enabled: true
Uri: http://schemas.micr
ConfigurationMode: Norma
DeliveryMode: Push
DeliveryMaxLatencyTime:
HeartbeatInterval: 90000
Query: <QueryList><Query
up">*</Select><Select Pa
b Services">*</Select><S
t-AppV-Client/Admin">*</
lient/Virtual Applicatio
crosoft-System-Diagnosti
on-Agent Driver/Operatio
Select><Select Path="Mic
perience Virtualization-
Select Path="Microsoft-W
al">*</Select><Select Pa
">*</Select><Select Path
pplication Server-Applic
```

Event Viewer

File   Action   Vie

Event Viewer (L
> Custom View
> Windows Lo
> Applications
Subscription

Subscription Properties - MyForwardedEvents

Subscription name: MyForwardedEvents

Description: Critical events collection

Destination log: Forwarded Events

Subscription type and source computers

○ Collector initiated   [Select Computers...]

This computer contacts the selected source computers and provides the subscription.

● Source computer initiated   [Select Computer Groups...]

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect: [Select Events... ▼]

Configure advanced settings: [Advanced...]

[OK]   [Cancel]

```
Administrator: Windows PowerShell                                    —    □    ✕

Windows Event Collector service was configured successfully.
PS C:\Users\Administrator> winrm quickconfig
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Users\Administrator> Enable-PSRemoting -Force
PS C:\Users\Administrator> wecutil  qc /quiet
Windows Event Collector service was configured successfully.
PS C:\Users\Administrator> wecutil get-subscription "MyForwardedEvents"
Subscription Id: MyForwardedEvents
SubscriptionType: SourceInitiated
Description: Critical events collection
Enabled: true
Uri: http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog
ConfigurationMode: Normal
DeliveryMode: Push
DeliveryMaxLatencyTime: 900000
HeartbeatInterval: 900000
Query: <QueryList><Query Id="0"><Select Path="Application">*</Select><Select Path="Security">*</Select><Select Path="Set
up">*</Select><Select Path="System">*</Select><Select Path="ForwardedEvents">*</Select><Select Path="Active Directory We
b Services">*</Select><Select Path="DNS Server">*</Select><Select Path="HardwareEvents">*</Select><Select Path="Microsof
t-AppV-Client/Admin">*</Select><Select Path="Microsoft-AppV-Client/Operational">*</Select><Select Path="Microsoft-AppV-C
lient/Virtual Applications">*</Select><Select Path="Microsoft-ServerCore-ShellLauncher/Admin">*</Select><Select Path="Mi
crosoft-System-Diagnostics-DiagnosticInvoker/Operational">*</Select><Select Path="Microsoft-User Experience Virtualizati
on-Agent Driver/Operational">*</Select><Select Path="Microsoft-User Experience Virtualization-App Agent/Operational">*</
Select><Select Path="Microsoft-User Experience Virtualization-IPC/Operational">*</Select><Select Path="Microsoft-User Ex
perience Virtualization-SQM Uploader/Operational">*</Select><Select Path="Microsoft-Windows-AAD/Operational">*</Select><
Select Path="Microsoft-Windows-All-User-Install-Agent/Admin">*</Select><Select Path="Microsoft-Windows-AllJoyn/Operation
al">*</Select><Select Path="Microsoft-Windows-AppHost/Admin">*</Select><Select Path="Microsoft-Windows-AppID/Operational
">*</Select><Select Path="Microsoft-Windows-ApplicabilityEngine/Operational">*</Select><Select Path="Microsoft-Windows-A
pplication Server-Applications/Admin">*</Select><Select Path="Microsoft-Windows-Application Server-Applications/Operatio
```

```
="Microsoft-Windows-TaskScheduler/Maintenance">*</Select><Select Path="Microsoft-Windows-TaskScheduler/Operational">*</S
elect><Select Path="Microsoft-Windows-TCPIP/Operational">*</Select><Select Path="Microsoft-Windows-TerminalServices-RDPC
lient/Operational">*</Select><Select Path="Microsoft-Windows-TerminalServices-ClientUSBDevices/Admin">*</Select><Select
Path="Microsoft-Windows-TerminalServices-ClientUSBDevices/Operational">*</Select><Select Path="Microsoft-Windows-Termina
lServices-LocalSessionManager/Admin">*</Select><Select Path="Microsoft-Windows-TerminalServices-LocalSessionManager/Oper
ational">*</Select><Select Path="Microsoft-Windows-TerminalServices-PnPDevices/Admin">*</Select><Select Path="Microsoft-
Windows-TerminalServices-PnPDevices/Operational">*</Select><Select Path="Microsoft-Windows-TerminalServices-Printers/Adm
in">*</Select><Select Path="Microsoft-Windows-TerminalServices-Printers/Operational">*</Select><Select Path="Microsoft-W
indows-TerminalServices-RemoteConnectionManager/Admin">*</Select><Select Path="Microsoft-Windows-TerminalServices-Remote
ConnectionManager/Operational">*</Select><Select Path="Microsoft-Windows-TerminalServices-ServerUSBDevices/Admin">*</Sel
ect><Select Path="Microsoft-Windows-TerminalServices-ServerUSBDevices/Operational">*</Select><Select Path="Microsoft-Win
dows-TerminalServices-SessionBroker-Client/Admin">*</Select><Select Path="Microsoft-Windows-TerminalServices-SessionBrok
er-Client/Operational">*</Select><Select Path="Microsoft-Windows-Time-Service/Operational">*</Select><Select Path="Micro
soft-Windows-Time-Service-PTP-Provider/PTP-Operational">*</Select><Select Path="Microsoft-Windows-TZSync/Operational">*<
/Select><Select Path="Microsoft-Windows-TZUtil/Operational">*</Select><Select Path="Microsoft-Windows-UAC/Operational">*
</Select><Select Path="Microsoft-Windows-UAC-FileVirtualization/Operational">*</Select><Select Path="Microsoft-Windows-S
earchUI/Operational">*</Select><Select Path="Microsoft-Windows-UniversalTelemetryClient/Operational">*</Select><Select P
ath="Microsoft-Windows-User Control Panel/Operational">*</Select><Select Path="Microsoft-Windows-User Device Registratio
n/Admin">*</Select><Select Path="Microsoft-Windows-User Profile Service/Operational">*</Select><Select Path="Microsoft-W
indows-User-Loader/Operational">*</Select><Select Path="Microsoft-Windows-UserPnp/ActionCenter">*</Select><Select Path="
Microsoft-Windows-UserPnp/DeviceInstall">*</Select><Select Path="Microsoft-Windows-VDRVROOT/Operational">*</Select><Sele
ct Path="Microsoft-Windows-VerifyHardwareSecurity/Admin">*</Select><Select Path="Microsoft-Windows-VerifyHardwareSecurit
y/Operational">*</Select><Select Path="Microsoft-Windows-VHDMP-Operational">*</Select><Select Path="Microsoft-Windows-Vo
lumeSnapshot-Driver/Operational">*</Select><Select Path="Windows Networking Vpn Plugin Platform/Operational">*</Select><
Select Path="Windows Networking Vpn Plugin Platform/OperationalVerbose">*</Select><Select Path="Microsoft-Windows-VPN-Cl
ient/Operational">*</Select><Select Path="Microsoft-Windows-Wcmsvc/Operational">*</Select><Select Path="Microsoft-Window
s-WebAuth/Operational">*</Select><Select Path="Microsoft-Windows-WebAuthN/Operational">*</Select><Select Path="Microsoft
-Windows-WebIO-NDF/Diagnostic">*</Select><Select Path="Microsoft-Windows-WEPHOSTSVC/Operational">*</Select><Select Path=
"Microsoft-Windows-WER-PayloadHealth/Operational">*</Select><Select Path="Microsoft-Windows-IKE/Operational">*</Select><
Select Path="Microsoft-Windows-VPN/Operational">*</Select><Select Path="Microsoft-Windows-WFP/Operational">*</Select><Se
lect Path="Microsoft-Windows-Win32k/Operational">*</Select><Select Path="Microsoft-Windows-Windows Defender/Operational"
>*</Select><Select Path="Microsoft-Windows-Windows Defender/WHC">*</Select><Select Path="Microsoft-Windows-Windows Firew
all With Advanced Security/ConnectionSecurity">*</Select><Select Path="Microsoft-Windows-Windows Firewall With Advanced
Security/ConnectionSecurityVerbose">*</Select><Select Path="Microsoft-Windows-Windows Firewall With Advanced Security/Fi
rewall">*</Select><Select Path="Microsoft-Windows-Windows Firewall With Advanced Security/FirewallDiagnostics">*</Select
><Select Path="Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose">*</Select><Select Path="Networ
k Isolation Operational">*</Select><Select Path="Microsoft-Windows-WinRM/Operational">*</Select><Select Path="Microsoft-
Windows-WindowsColorSystem/Operational">*</Select><Select Path="Microsoft-Windows-WindowsSystemAssessmentTool/Operationa
l">*</Select><Select Path="Microsoft-Windows-WindowsUIImmersive/Operational">*</Select><Select Path="Microsoft-Windows-W
indowsUpdateClient/Operational">*</Select><Select Path="Microsoft-Windows-WinINet-Config/ProxyConfigChanged">*</Select><
Select Path="Microsoft-Windows-WinHTTP-NDF/Diagnostic">*</Select><Select Path="Microsoft-Windows-WinHttp/Operational">*<
/Select><Select Path="Microsoft-Windows-WinINet-Capture/Analytic">*</Select><Select Path="Microsoft-Windows-WinINet/Oper
ational">*</Select><Select Path="Microsoft-Windows-Winlogon/Operational">*</Select><Select Path="Microsoft-Windows-WinNa
```

n/Admin">*</Select><Select Path="Microsoft-Windows-User Profile Service/Operational">*</Select><Select Path="Microsoft-W
indows-User-Loader/Operational">*</Select><Select Path="Microsoft-Windows-UserPnp/ActionCenter">*</Select><Select Path="
Microsoft-Windows-UserPnp/DeviceInstall">*</Select><Select Path="Microsoft-Windows-VDRVROOT/Operational">*</Select><Sele
ct Path="Microsoft-Windows-VerifyHardwareSecurity/Admin">*</Select><Select Path="Microsoft-Windows-VerifyHardwareSecurit
y/Operational">*</Select><Select Path="Microsoft-Windows-VHDMP-Operational">*</Select><Select Path="Microsoft-Windows-Vo
lumeSnapshot-Driver/Operational">*</Select><Select Path="Windows Networking Vpn Plugin Platform/Operational">*</Select><
Select Path="Windows Networking Vpn Plugin Platform/OperationalVerbose">*</Select><Select Path="Microsoft-Windows-VPN-Cl
ient/Operational">*</Select><Select Path="Microsoft-Windows-Wcmsvc/Operational">*</Select><Select Path="Microsoft-Window
s-WebAuth/Operational">*</Select><Select Path="Microsoft-Windows-WebAuthN/Operational">*</Select><Select Path="Microsoft
-Windows-WebIO-NDF/Diagnostic">*</Select><Select Path="Microsoft-Windows-WEPHOSTSVC/Operational">*</Select><Select Path=
"Microsoft-Windows-WER-PayloadHealth/Operational">*</Select><Select Path="Microsoft-Windows-IKE/Operational">*</Select><
Select Path="Microsoft-Windows-VPN/Operational">*</Select><Select Path="Microsoft-Windows-WFP/Operational">*</Select><Se
lect Path="Microsoft-Windows-Win32k/Operational">*</Select><Select Path="Microsoft-Windows-Windows Defender/Operational"
>*</Select><Select Path="Microsoft-Windows-Windows Defender/WHC">*</Select><Select Path="Microsoft-Windows-Windows Firew
all With Advanced Security/ConnectionSecurity">*</Select><Select Path="Microsoft-Windows-Windows Firewall With Advanced
Security/ConnectionSecurityVerbose">*</Select><Select Path="Microsoft-Windows-Windows Firewall With Advanced Security/Fi
rewall">*</Select><Select Path="Microsoft-Windows-Windows Firewall With Advanced Security/FirewallDiagnostics">*</Select
><Select Path="Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose">*</Select><Select Path="Networ
k Isolation Operational">*</Select><Select Path="Microsoft-Windows-WinRM/Operational">*</Select><Select Path="Microsoft-
Windows-WindowsColorSystem/Operational">*</Select><Select Path="Microsoft-Windows-WindowsSystemAssessmentTool/Operationa
l">*</Select><Select Path="Microsoft-Windows-WindowsUIImmersive/Operational">*</Select><Select Path="Microsoft-Windows-W
indowsUpdateClient/Operational">*</Select><Select Path="Microsoft-Windows-WinINet-Config/ProxyConfigChanged">*</Select><
Select Path="Microsoft-Windows-WinHTTP-NDF/Diagnostic">*</Select><Select Path="Microsoft-Windows-WinHttp/Operational">*<
/Select><Select Path="Microsoft-Windows-WinINet-Capture/Analytic">*</Select><Select Path="Microsoft-Windows-WinINet/Oper
ational">*</Select><Select Path="Microsoft-Windows-Winlogon/Operational">*</Select><Select Path="Microsoft-Windows-WinNa
t/Oper">*</Select><Select Path="Microsoft-Windows-Winsock-WS2HELP/Operational">*</Select><Select Path="Microsoft-Windows
-Winsock-NameResolution/Operational">*</Select><Select Path="Microsoft-Windows-Winsock-AFD/Operational">*</Select><Selec
t Path="Microsoft-Windows-Wired-AutoConfig/Operational">*</Select><Select Path="Microsoft-Windows-WMI-Activity/Operation
al">*</Select><Select Path="Microsoft-Windows-WMPNSS-Service/Operational">*</Select><Select Path="Microsoft-Windows-Word
pad/Admin">*</Select><Select Path="Microsoft-Windows-Workplace Join/Admin">*</Select><Select Path="Microsoft-Windows-WPD
-ClassInstaller/Operational">*</Select><Select Path="Microsoft-Windows-WPD-CompositeClassDriver/Operational">*</Select><
Select Path="Microsoft-Windows-WPD-MTPClassDriver/Operational">*</Select><Select Path="Windows PowerShell">*</Select></Q
uery></QueryList>
ReadExistingEvents: false
TransportName: HTTP
ContentFormat: RenderedText
Locale: en-US
LogFile: ForwardedEvents
PublisherName: Microsoft-Windows-EventCollector
AllowedIssuerCAList:
AllowedSubjectList:
DeniedSubjectList:
AllowedSourceDomainComputers: O:NSG:BAD:P(A;;GA;;;S-1-5-21-1955954324-206265833-1145328094-1109)(A;;GA;;;S-1-5-21-195595

```
PS C:\Users\Administrator> Get-WinEvent -LogName ForwardedEvents -MaxEvents 10 | Format-Table -AutoSize
Get-WinEvent : No events were found that match the specified selection criteria.
At line:1 char:1
+ Get-WinEvent -LogName ForwardedEvents -MaxEvents 10 | Format-Table -A ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:) [Get-WinEvent], Exception
    + FullyQualifiedErrorId : NoMatchingEventsFound,Microsoft.PowerShell.Commands.GetWinEventCommand
```

```
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-ADDomain).DNSRoot
forest.local
PS C:\Users\Administrator>
```

```
Select 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-ADDomain).NetBIOSName
FOREST
PS C:\Users\Administrator> set-adaccountpassword -identity adrien -reset -newpassword (convertto-securestring "Test@1234
" -asplaintext -force)
PS C:\Users\Administrator> Enable-ADAccount adrien
PS C:\Users\Administrator> Get-ADUser adrien -Properties Enabled, PasswordLastSet


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
PasswordLastSet   : 6/20/2025 9:53:48 PM
SamAccountName    : adrien
SID               : S-1-5-21-1955954324-206265833-1145328094-1105
Surname           : Agreste
UserPrincipalName :
```

```
ObjectGUID             : 660bfeb8-b8df-4246-93c3-6c994b20b321
SamAccountName         : adrien
SID                    : S-1-5-21-1955954324-206265833-1145328094-1105
Surname                : Agreste
UserPrincipalName      :


PS C:\Users\Administrator> secedit /export /cfg C:\secpolicy.txt

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
PS C:\Users\Administrator> notepad C:\secpolicy.txt
PS C:\Users\Administrator> Get-ADUser ravi -Properties Enabled, AccountExpirationDate


AccountExpirationDate :
DistinguishedName      : CN=Ravi,OU=MARKETING,OU=PUNE,OU=INDIA,DC=forest,DC=local
Enabled                : True
GivenName              : Ravi
Name                   : Ravi
ObjectClass            : user
ObjectGUID             : 8542a2a6-db96-4bdc-8e0b-6851f505a27f
SamAccountName         : ravi
SID                    : S-1-5-21-1955954324-206265833-1145328094-1103
Surname                : Sharma
UserPrincipalName      :
```

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> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                      State
========================================= ================================================================ ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                               Disabled
SeMachineAccountPrivilege                 Add workstations to domain                                       Disabled
SeSecurityPrivilege                       Manage auditing and security log                                 Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                         Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                   Disabled
SeSystemProfilePrivilege                  Profile system performance                                       Disabled
SeSystemtimePrivilege                     Change the system time                                           Disabled
SeProfileSingleProcessPrivilege           Profile single process                                           Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                     Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                Disabled
SeBackupPrivilege                         Back up files and directories                                    Disabled
SeRestorePrivilege                        Restore files and directories                                    Disabled
SeShutdownPrivilege                       Shut down the system                                             Disabled
SeDebugPrivilege                          Debug programs                                                   Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                               Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                         Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                              Disabled
SeUndockPrivilege                         Remove computer from docking station                             Disabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation   Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                 Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                        Enabled
SeCreateGlobalPrivilege                   Create global objects                                            Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                   Disabled
SeTimeZonePrivilege                       Change the time zone                                             Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                            Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
PS C:\Users\Administrator>
```

Type here to search

10:12 PM
6/20/2025