Microsoft Exchange Server Scan User Privileges and Configurations

December 10, 2019

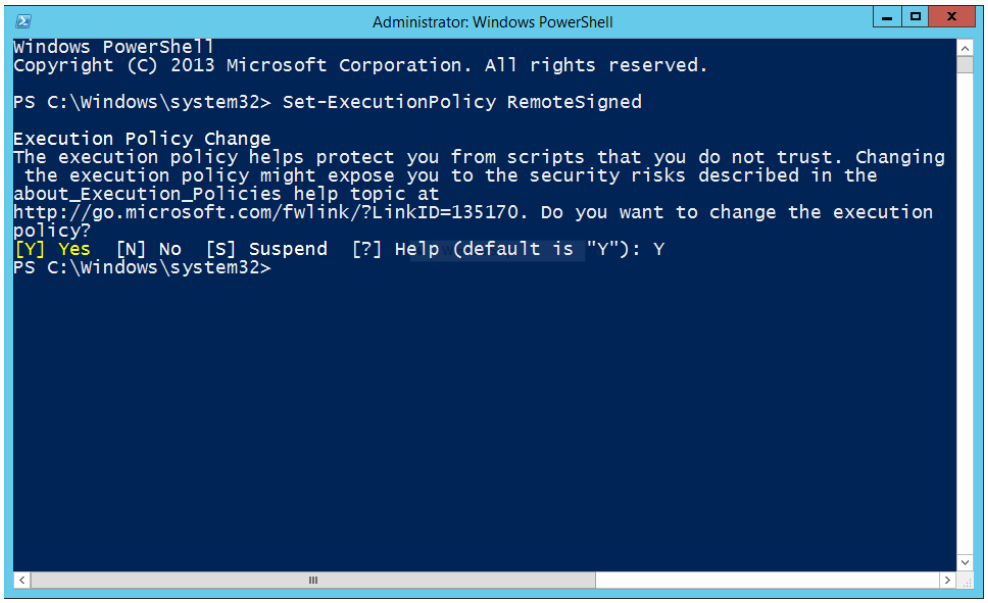
Contents

System Configuration Requirements

- Set PowerShell Execution Policies
- Verify WinRM IIS Extensions
- Enable Windows Authentication for PowerShell Virtual Directory
- Verify SSL setting for PowerShell Virtual Directory
- Verify the application pool for PowerShell Virtual Directory
- Verify the Security in for PowerShell Virtual Directory

1. Open a Windows PowerShell window you open by selecting Run as administrator and run the command as shown:

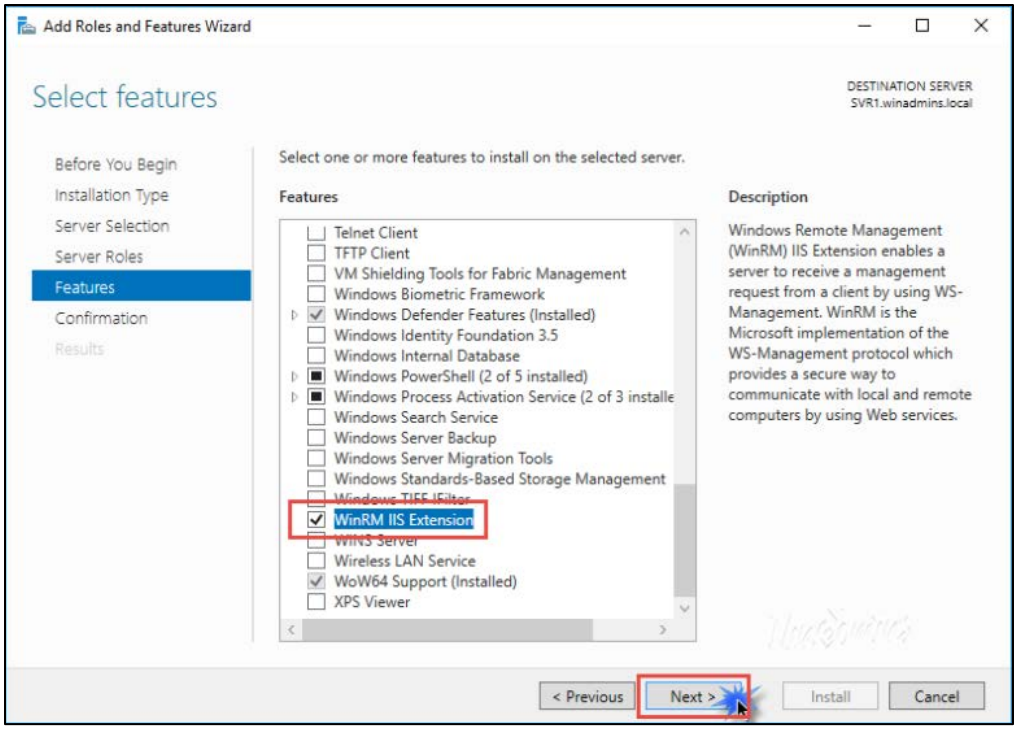
Set-ExecutionPolicy RemoteSigned

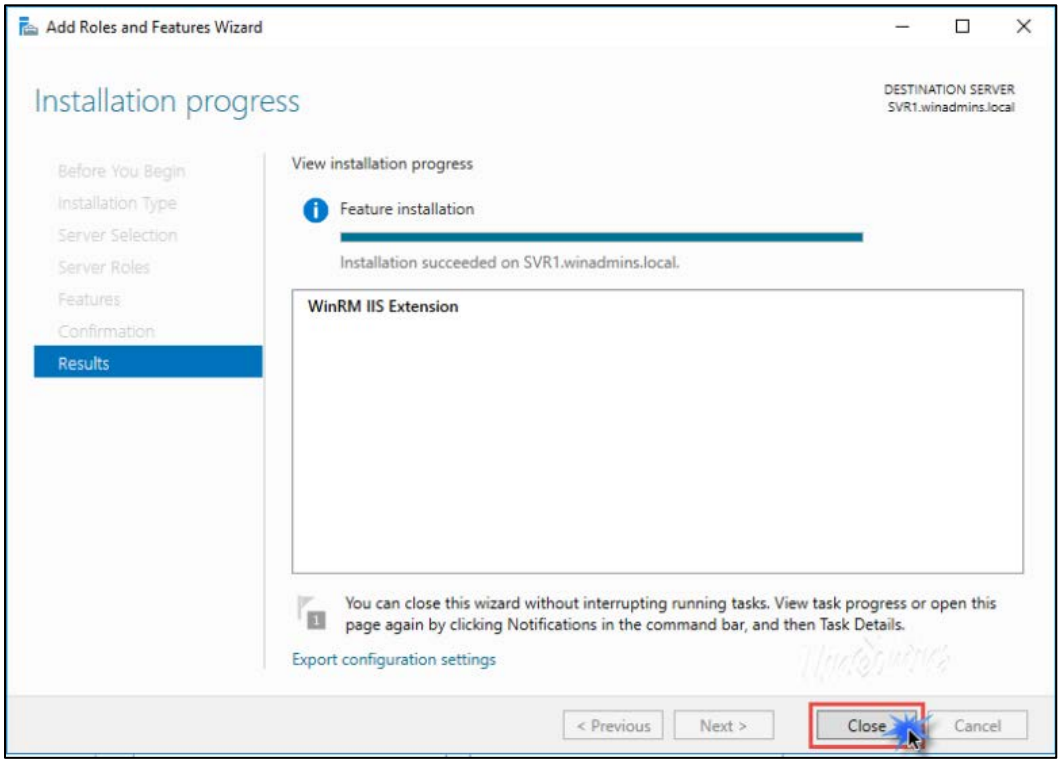


2. Enable the WinRM IIS Extensions under Add Roles and Features in Server Manager:

   Windows Remote Management (WinRM) IIS Extension enables a server to receive a management request from a client computer by using the WS-Management protocol. WinRM is the Microsoft implementation of the WS-Management protocol. This helps secure communication between local and remote computers by using Web-based services.

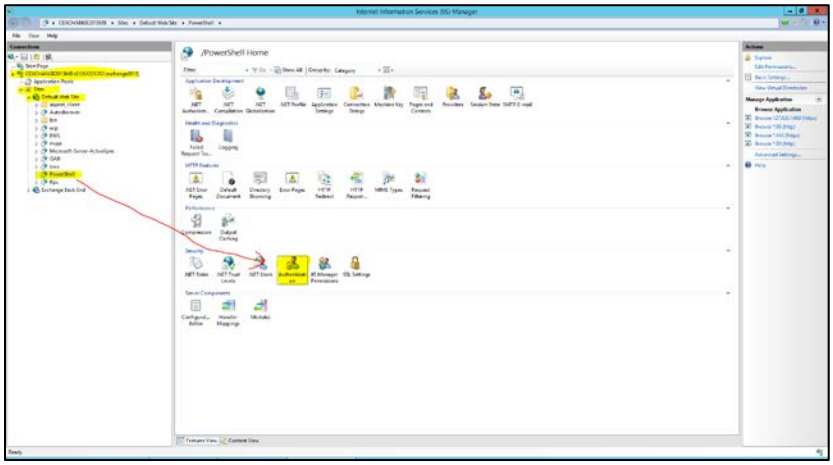
   Steps are shown below:



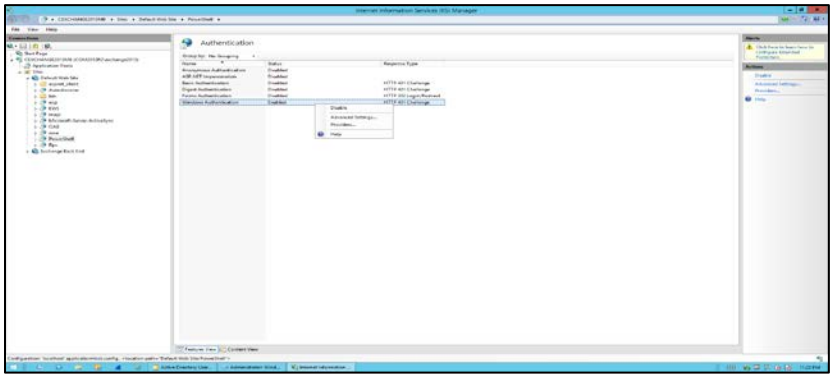


3. Log in to your Exchange 2010+ server and enable the Windows Authentication on the PowerShell site:
   Open “Internet Information Services (IIS) Manager” console.

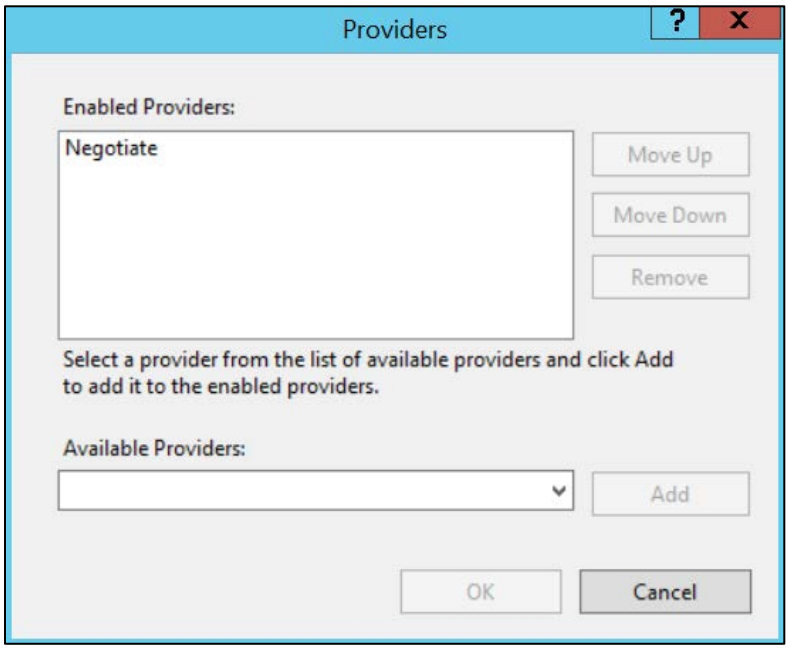
Connect to the Exchange Server.
Open: Sites -> “Name of your Exchange Site” -> PowerShell and Open Authentication as shown:



Enable Windows Authentication. Right click the same and Select Providers as ’ Negotiate as shown:

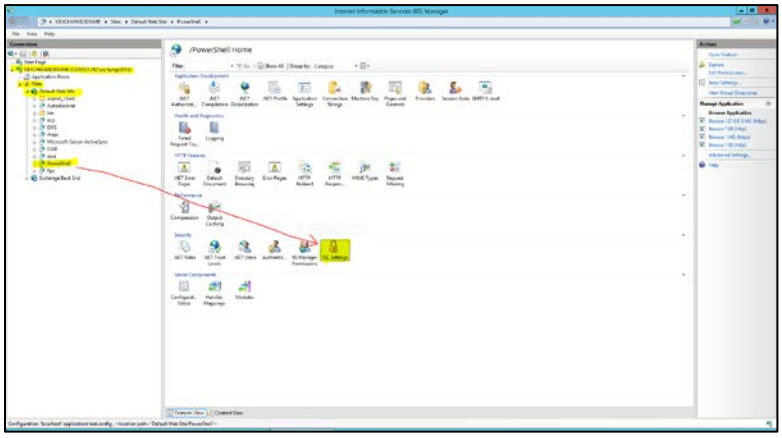


Providers:

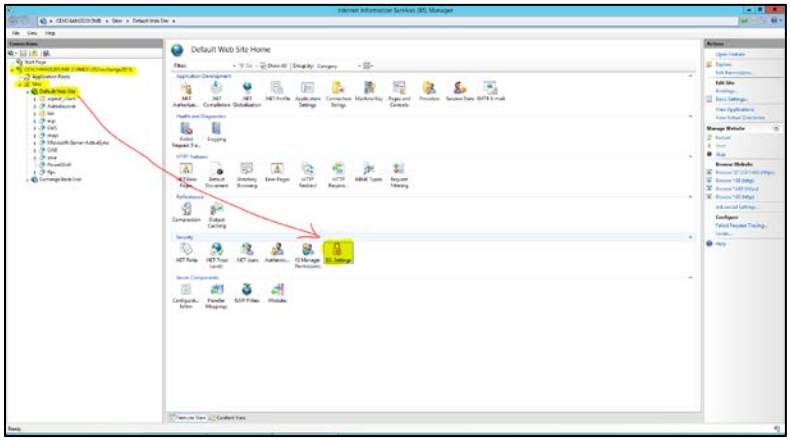


4. For using http URI to access PowerShell Virtual Directory, Disable the SSL checking (with ignore) for the PowerShell Virtual Directory as well as Default IIS site as shown:

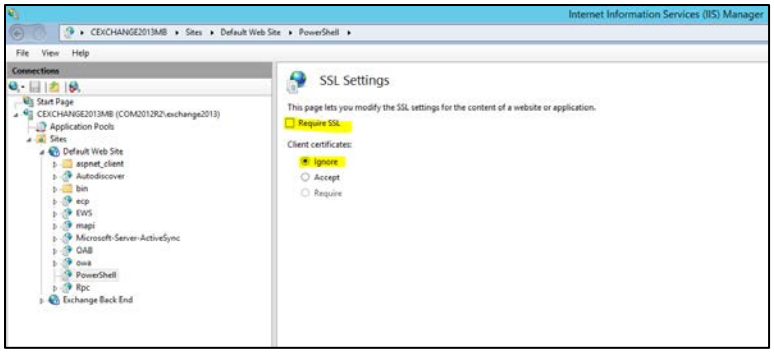
   PowerShell Virtual Directory:



Default Web Site:

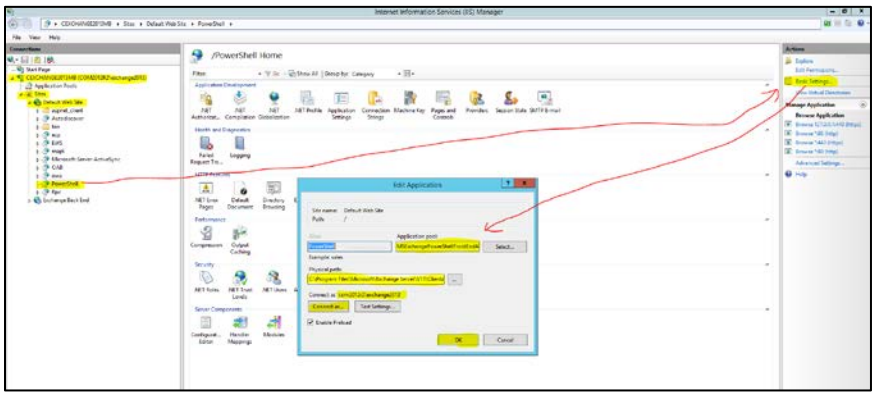


Disable “Require SSL”:

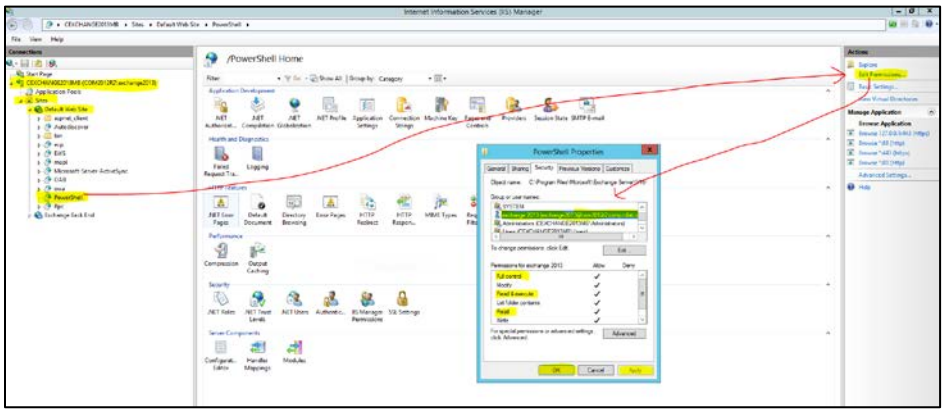


P.S.: Remember to Click on Apply to save the changes.

5. Also under Powershell Virtual Directory ’ Basic Settings ’ Make sure you have the Correct application pool (MSExchangePowerShellAppPool or MSExchangePowerShellFrontEndAppPool) and Physical path (C:\Program Files\Microsoft\Exchange Server\V<Exchange Version>\ClientAccess\PowerShell) selected to access the PowerShell virtual directory on the host under IIS root as shown:



6. Also make sure the Exchange user has read permissions on the Physical path specified. To do this go to PowerShell Virtual Directory ’ Edit Permissions ’ Security tab ’ Assign read permissions to user performing the scan as shown:

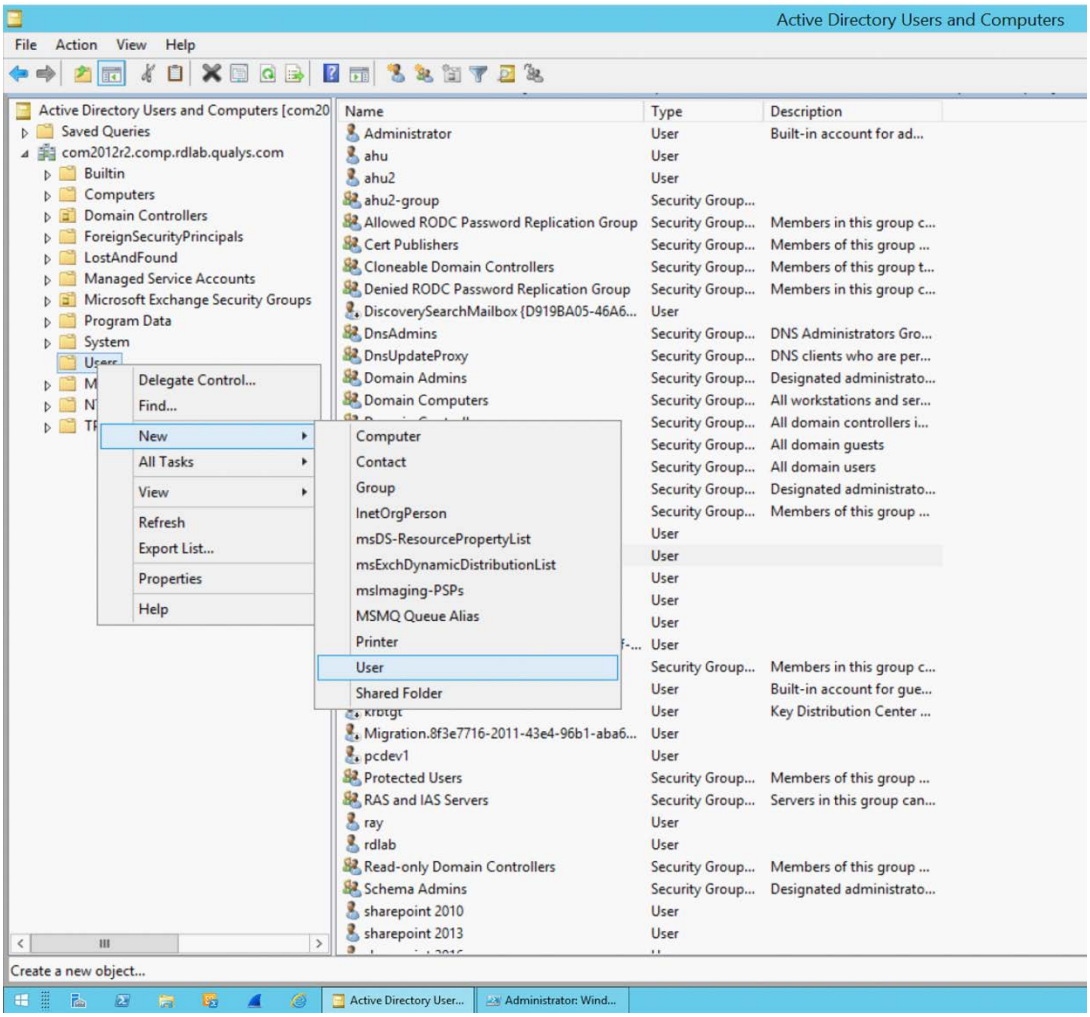


Scan User Privilege

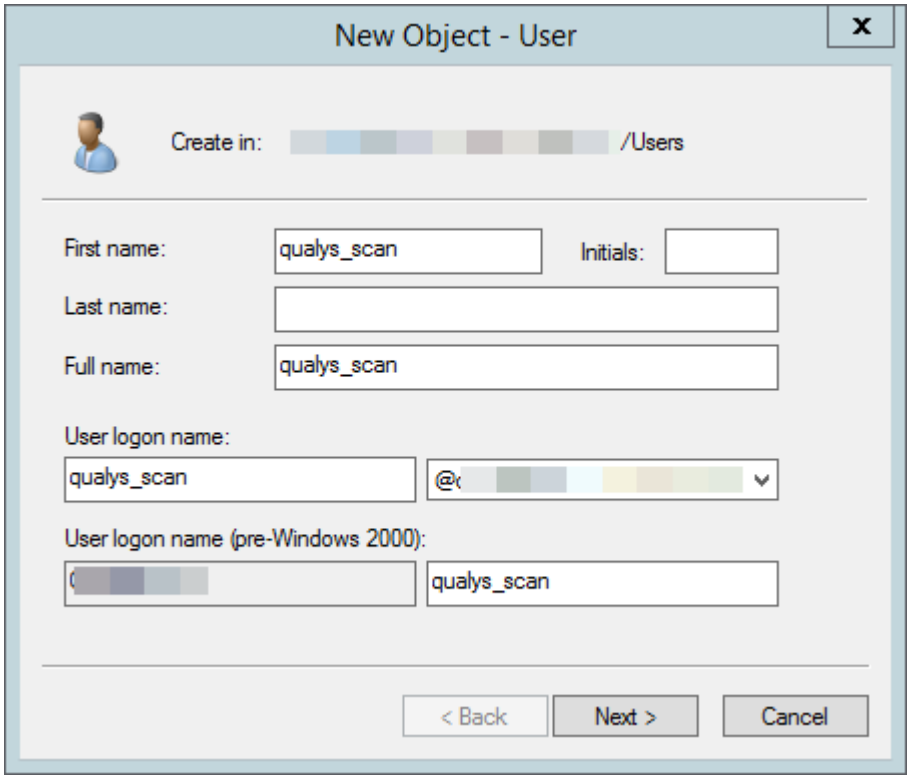
- Add new user account in Active Directory
- Add Roles/Group membership for new created user account
- Enable Remote PowerShell for new created user account

Creating a new user account as a MS Exchange scan user in Active Directory

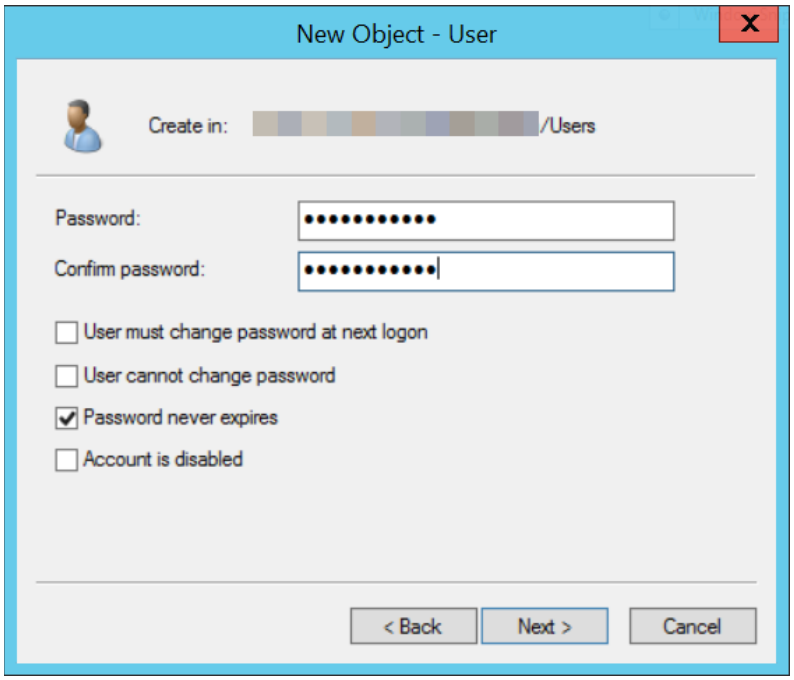
1. Open Server Manager and select Active Directory Users and Computers from the Tools menu.
2. In the left pane of ADUC, expand your domain and click the Users container.
3. In the right pane, right click some empty space and select New > User from the menu as shown:



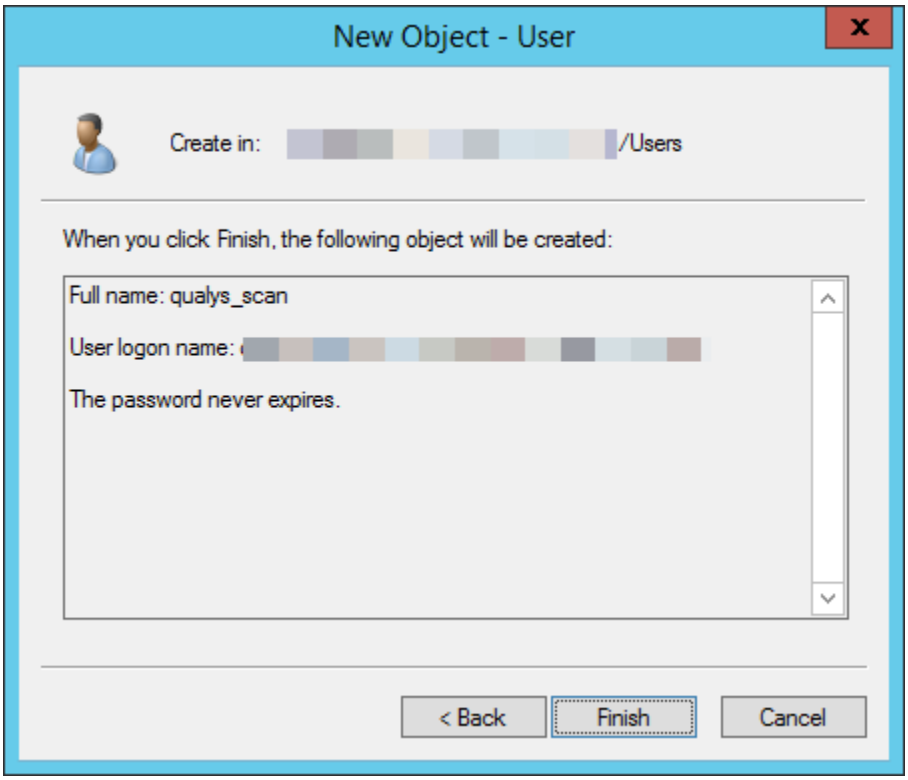
4. In the New Object – User dialog, enter a First name, Last name, User logon name and then click Next as shown:



5. Type and confirm a Password, then click Next.



6. Check the information for the new user on the confirmation screen and click Finish :



Add Roles/Group membership for new created user account

The user performing the scan should be an Exchange AD user with following Roles/Group membership configurations to run specific Exchange PowerShell Cmdlets

Ensure the user is a part of Exchange Management Role Groups to run specific set of Exchange PowerShell cmdlets as mentioned below:

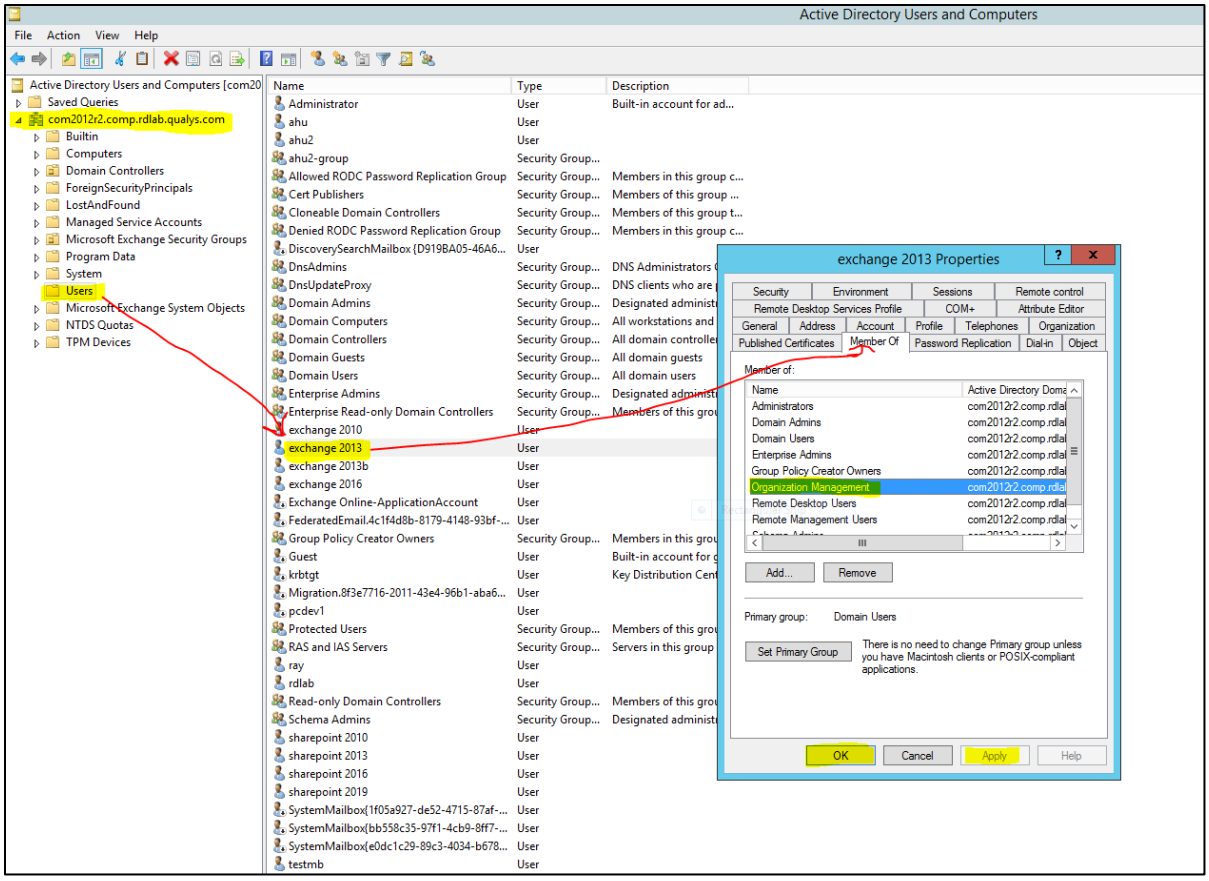
Procedure (Perform using Domain Administrator user) as shown:

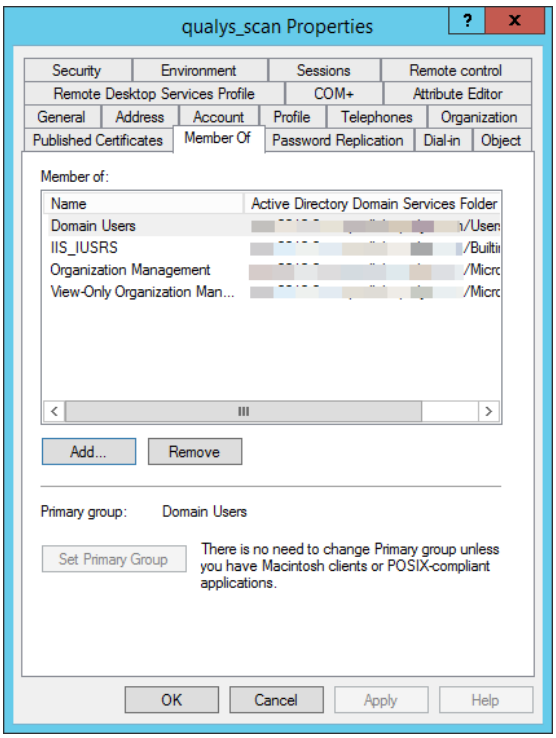
To assign a specific role to the user Navigate to:
Active Directory Users and Computers (dsa.msc) ’ Under "Microsoft Exchange Security Groups" ’ Right click the required group and add the "Exchange user" to Exchange Role Group as per requirement listed below:

- IIS_IUSRS
- Organization Management
- Domain Users
- View-Only Audit Logs management

Feature/Exchange Cmdlets Category	Exchange Role/Security Group membership required
Administrator audit logging	Organization Management Records Management

Feature/Exchange Cmdlets Category	Exchange Role/Security Group membership required
Exchange admin center configuration settings	View-Only Organization Management
Exchange admin center connectivity	Organization Management Server Management
Exchange server configuration settings	Organization Management Server Management
Exchange Help settings	Organization Management
Message categories	Organization Management Hygiene Management Recipient Management Help Desk
Product key	Organization Management
Test system health	Organization Management Server Management
View-only administrator audit logging	Organization Management Records Management Note: You can also manually assign the View-Only Audit Logs management role to a management role group. For more information, see View-Only Audit Logs.
Write to audit log	Users that are members of any role group or assigned any management role can write to the administrator audit log.
Active Directory Domain Services server settings	Organization Management Server Management Recipient Management UM Management
Cmdlet extension agents	Organization Management
PowerShell virtual directories	Organization Management Server Management
PowerShell and WinRM installation	Local Server Administrator
Remote PowerShell	Organization Management

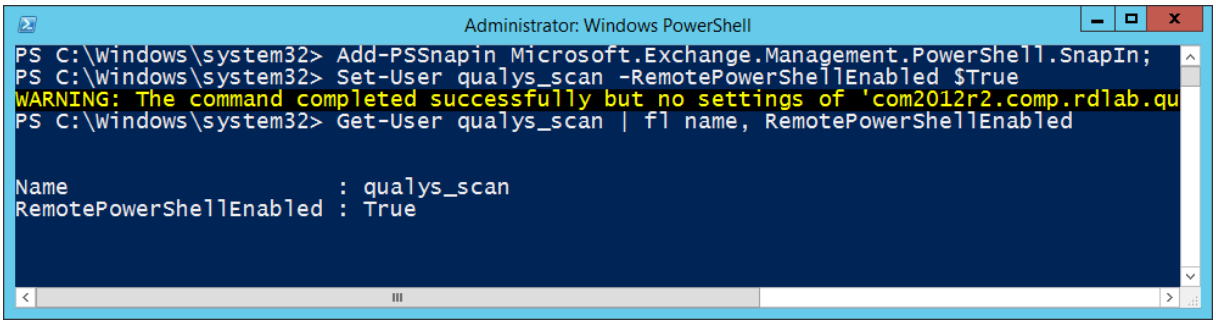

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [com20
Saved Queries
com2012r2.comp.rdlab.qualys.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Managed Service Accounts
Microsoft Exchange Security Groups
Program Data
System
Users
Microsoft Exchange System Objects
NTDS Quotas
TPM Devices
Name Type Description
Administrator User Built-in account for ad...
ahu User
ahu2 User
ahu2-group Security Group...
Allowed RODC Password Replication Group Security Group... Members in this group c...
Cert Publishers Security Group... Members of this group ...
Cloneable Domain Controllers Security Group... Members of this group t...
Denied RODC Password Replication Group Security Group... Members in this group c...
DiscoverySearchMailbox {D919BA05-46A6... User
DnsAdmins Security Group... DNS Administrators
DnsUpdateProxy Security Group... DNS clients who are
Domain Admins Security Group... Designated administ
Domain Computers Security Group... All workstations and
Domain Controllers Security Group... All domain controlle
Domain Guests Security Group... All domain guests
Domain Users Security Group... All domain users
Enterprise Admins Security Group... Designated administ
Enterprise Read-only Domain Controllers Security Group... Members of this grou
exchange 2010 User
exchange 2013 User
exchange 2013b User
exchange 2016 User
Exchange Online-ApplicationAccount User
FederatedEmail.4c1f4d8b-8179-4148-93bf-... User
Group Policy Creator Owners Security Group... Members in this grou
Guest User Built-in account for g
krbtgt User Key Distribution Cent
Migration.8f3e7716-2011-43e4-96b1-aba6... User
pcdev1 User
Protected Users Security Group... Members of this grou
RAS and IAS Servers Security Group... Servers in this group
ray User
rdlab User
Read-only Domain Controllers Security Group... Members of this grou
Schema Admins Security Group... Designated administ
sharepoint 2010 User
sharepoint 2013 User
sharepoint 2016 User
sharepoint 2019 User
SystemMailbox{1f05a927-de52-4715-87af-... User
SystemMailbox{bb558c35-97f1-4cb9-8ff7-... User
SystemMailbox{e0dc1c29-89c3-4034-b678... User
testmb User
exchange 2013 Properties
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization
Published Certificates Member Of Password Replication Dial-in Object
Member of:
Name Active Directory Doma
Administrators com2012r2.comp.rdla
Domain Admins com2012r2.comp.rdla
Domain Users com2012r2.comp.rdla
Enterprise Admins com2012r2.comp.rdla
Group Policy Creator Owners com2012r2.comp.rdla
Organization Management com2012r2.comp.rdla
Remote Desktop Users com2012r2.comp.rdla
Remote Management Users com2012r2.comp.rdla
Add... Remove
Primary group: Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK Cancel Apply Help


qualys_scan Properties
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization
Published Certificates Member Of Password Replication Dial-in Object
Member of:
Name Active Directory Domain Services Folder
Domain Users
IIS_IUSRS
Organization Management
View-Only Organization Man...
Add... Remove
Primary group: Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK Cancel Apply Help

Enable Remote PowerShell for new created user account

(Open a Windows PowerShell window you open by selecting Run as administrator) and run the command as shown:

```
Set-User ”qualys_scan” -RemotePowerShellEnabled $True
```



Verify scan user membership and test connection by PowerShell script

- Verify the membership of groups assigned to users
- Test connect to MS Exchange Server via Remote PowerShell

Verify the membership of groups assigned to users

Using below PowerShell commands we can also verify the above membership of groups assigned to users in AD:
Note: Firstly, your user must be assigned the Role Management management role to run the ***Get-ManagementRoleAssignment*** *cmdlet.*

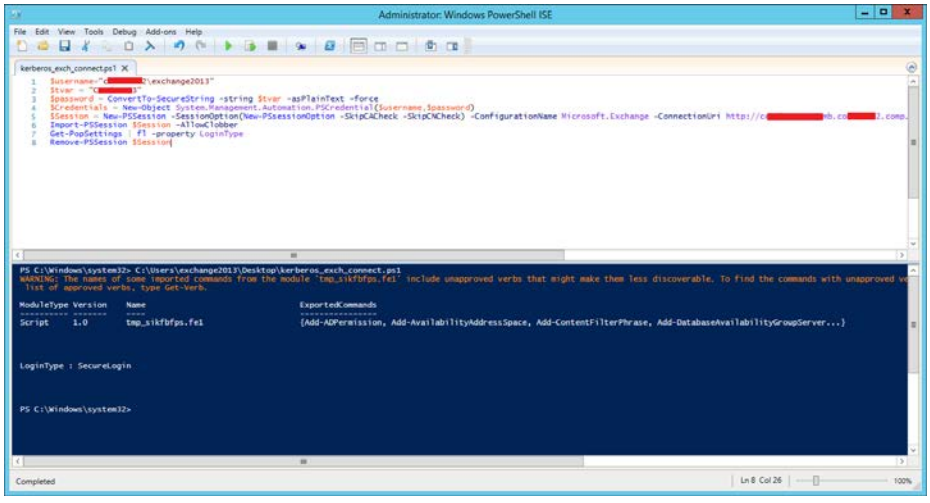
Below is the PowerShell Command:
`Get-ManagementRoleAssignment -RoleAssignee <Scan User Name>`

Test connect to MS Exchange Server via Remote PowerShell
Steps required to connect to PowerShell Virtual Directory using PS Script :
Open PowerShell or PowerShell ISE with "Run as Administrator" and insert below code as shown:

```
$username="<DomainName>\<ScanUserName>"
      $tvar = "<Password_Of_Scan_User>"
      $password = ConvertTo-SecureString -string $tvar -asPlainText –force
      $Credentials = New-Object
      System.Management.Automation.PSCredential($username,$password)
      $Session = New-PSSession -SessionOption(New-PSsessionOption -SkipCACheck
      -SkipCNCheck) -ConfigurationName Microsoft.Exchange -ConnectionUri
      http://<FQDN_of_Exchange_Server_Host>:80/powershell -authentication
      Kerberos -Credential $Credentials
      Import-PSSession $Session –AllowClobber
      #You Can test any Exchange PowerShell Command as shown in below line:
      Get-PopSettings | fl -property LoginType
      Remove-PSSession $Session
```

Run the above code with correct input details as per your host setup and you should be able to see the connection result as follows (Following is an example scenario):

This ensures you are able to connect the PowerShell Virtual Directory using Remote PowerShell with the Scan User specified.



Manage Authentication Records

Create an MS Exchange Server record in order to authenticate to a Microsoft Exchange Server running on a Windows host, and scan it for compliance. Windows authentication is required so you'll also need a Windows record for the host running the web server.

Supported versions

We support Microsoft Exchange Server 2010, 2013, and 2016.

Create one or more Windows Records

- Go to Scans > Authentication.

- Check that you have a Windows record already defined for the host running the web server.

- Create an MS Exchange Server record for the same host. Go to New > Application Records > MS Exchange Server.

Which users have permission to create records?

Managers can add authentication records. Unit Managers must be granted these permissions:
- Manage PC module
- Create/edit authentication records/vaults

How does it work?

We'll authenticate to each target host using the credentials provided in the Windows record. If the host is running an MS Exchange Server then we'll check to see if an MS Exchange Server record exists. If yes, we'll use credentials from the Windows record to authenticate to the Windows system, access the web server configuration, and scan it for compliance.