Microsoft Exchange Server Scan User Privileges and Configurations

March 23, 2022

Contents

System Configuration Requirements ................................................................. 2
Scan User Privilege .......................................................................................... 8
  Creating a new user account as a MS Exchange scan user in Active Directory ... 8
  Add Roles/Group membership for new created user account ......................... 10
  Enable Remote PowerShell for new created user account .............................. 13
Verify scan user membership and test connection by PowerShell script .......... 14
Manage Authentication Records ..................................................................... 15
  Supported versions ....................................................................................... 15
  Create one or more Windows Records ......................................................... 15
  Which users have permission to create records? ........................................... 15
  How does it work? ....................................................................................... 16
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:
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:
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:

![New Object - User dialog](image1)

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

![New Object - User dialog](image2)
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

<table>
<thead>
<tr>
<th>Feature/Exchange Cmdlets Category</th>
<th>Exchange Role/Security Group membership required</th>
</tr>
</thead>
</table>
| Administrator audit logging     | [Organization Management]
<p>|                                  | [Records Management] |</p>
<table>
<thead>
<tr>
<th>Feature/Exchange Cmdlets Category</th>
<th>Exchange Role/Security Group membership required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange admin center configuration settings</td>
<td><strong>View-Only Organization Management</strong></td>
</tr>
<tr>
<td>Exchange admin center connectivity</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td>Exchange server configuration settings</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td>Exchange Help settings</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td>Message categories</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Hygiene Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Recipient Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Help Desk</strong></td>
</tr>
<tr>
<td>Product key</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td>Test system health</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server Management</strong></td>
</tr>
<tr>
<td>View-only administrator audit logging</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Records Management</strong></td>
</tr>
<tr>
<td></td>
<td>Note: You can also manually assign the View-Only Audit Logs management role to a management role group. For more information, see <a href="#">View-Only Audit Logs</a>.</td>
</tr>
<tr>
<td>Write to audit log</td>
<td>Users that are members of any role group or assigned any management role can write to the administrator audit log.</td>
</tr>
<tr>
<td>Active Directory Domain Services server settings</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Recipient Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>UM Management</strong></td>
</tr>
<tr>
<td>Cmdlet extension agents</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td>PowerShell virtual directories</td>
<td><strong>Organization Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server Management</strong></td>
</tr>
<tr>
<td>PowerShell and WinRM installation</td>
<td><strong>Local Server Administrator</strong></td>
</tr>
<tr>
<td>Remote PowerShell</td>
<td><strong>Organization Management</strong></td>
</tr>
</tbody>
</table>
Microsoft Exchange Server Scan User Privileges and Configurations
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)
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


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 > Applications > MS Exchange Server.

![Image of Windows record creation]

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.