How to enable WinRM?

Introduction

On this page we will describe the steps to follow to enable WinRM with the domain controller Group Policy for WMI monitoring.

Step by Step

Step 1: Create a Group Policy object

Fist of all, you need to create a Group Policy object for your domain.

1. From the start menu, open Control Panel.
2. Select **Administrative Tools**.
3. Select **Group Policy Management**.
4. From the menu tree, click **Domains > [your domain's name]**.
5. Right-click and select **Create a GPO in this domain, and Link it here**.
6. Input **Enable WinRM**.
7. Click **OK**.

Step 2: Enable WinRM services

Secondly, it is necessary to enable WinRm services to allow remote management of the server through WinRM. You must edit the Group Policy you just created.

1. Right-click on the new **Enable WinRM Group Policy Object and select Edit**.

2. From the menu tree, click **Computer Configuration > Policies > Administrative Templates: Policy definitions > Windows Components > Windows Remote Management (WinRM) > WinRM Service**.

3. Right-click on **Allow remote server management through WinRM** and click **Edit**.

4. Select **Enabled** to allow remote server management through WinRM.

5. Enter an asterisk (*) into each field.

6. Click **OK**.

Step 3: Enable the service that goes the policy

1. From the Group Policy Management Editor window, click **Preferences > Control Panel Settings > Services**.

2. Right-click on **Services** and select **New > Service**.

3. Select **Automatic** as the startup.

4. Enter WinRM as the service name.

5. Select **Start service** as the service action.

6. All remaining details can stay on the defaults. Click **OK**.

Step 4: Allow for inbound remote administration

You have to allow for inbound remote administration by updating the firewall rules

Step 4.1: Allow inbound remote administration exception

1. Using the Group Policy Management Editor, from the menu tree, click **Computer Configuration > Policies > Administrative Templates: Policy definitions > Network > Network Connections > Windows Firewall > Domain Profile**.

2. Right-click on Windows Firewall: Allow inbound remote administration exception and click **Edit**.

3. Select **Enabled**.

4. Enter the IP address into the field called Allow unsolicited incoming messages from these IP addresses. To allow messages from any IP address, enter an asterisk (*) into each field. You can also restrict unsolicited incoming messages from the Auvik virtual appliance only, by entering the appliances IP address. Otherwise enter a comma-separated list that contains a combination of IP addresses (10.1.100.0), subnet descriptions (10.2.3.0/24), or strings (localsubnet) for the set of devices that will have access for remote administration.

5. Click **OK**.

6. Right-click on **Windows Firewall: Allow ICMP exception** and click **Edit**.

7. Select **Enabled**.

8. Check **Allow inbound echo request**.

9. Click **OK**.

Step 4.2: Allow ICMP exception

1. From the menu tree, click **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound Rules**.

2. Right-click on **Inbound Rules** and click **New Rule**.

3. Select **Predefined**.

4. Select **Windows Remote Management** from the list of services.

5. Click **Next**.

6. Uncheck the **Public** rule. Leave the **Domain**, **Private** rule checked.

7. Click **Next**.

8. Leaving the defaults, click **Finish**.

9. Right-click on the new rule and click **Properties**.

10. Click the **Advanced** tab.

11. Uncheck **Private**.

12. Click **OK**.

13. From the menu tree, click **Computer Configuration > Policies > Windows Settings > Security Settings > Network List Manager Policies**.

14. Right-click **Unidentified Networks** and click **Properties**.

15. Change the location type from Not configured to **Private**.

16. Click **OK**.

17. Close the Local Group Policy Editor window.

Revision #8
Created 26 April 2024 12:58:53 by pgarcia@soffid.com
Updated 30 April 2024 10:26:07 by pgarcia@soffid.com