

How can we help?

 Search

Auvik Support (/hc/en-us) > Setting up and troubleshooting Auvik (/hc/en-us/categories/201136656-Setting-up-and-troubleshooting-Auvik)

> Device setup and configuration (/hc/en-us/sections/200786200-Device-setup-and-configuration)

How to enable WinRM with domain controller Group Policy for WMI monitoring



Krista Foisy

July 21, 2017 21:21

FOLLOW (/HC/EN-US/ARTICLES/204424994-HOW-TO-ENABLE-WINRM-WITH-DOMAIN-CONTROLLER-GROUP-POLICY-FOR-WMI-MONITORING/SUBSCRIPTION)

If you can't connect to a domain controller but would still like to monitor your Windows devices, you'll need to enable WMI device by device. Please see [How to enable WMI monitoring on a single Windows device \(/hc/en-us/articles/204610500\)](#) for complete instructions.

[REQUEST FREE TRIAL](#)

Auvik uses the Windows Remote Management (WinRM) protocol to access Windows Management Instrumentation (WMI) data. This article walks you through how to enable and configure WinRM using Group Policy so you can use Auvik to remotely manage all Windows devices on your network.

Keep in mind there's a delay between completing the set-up steps and the change propagating to all computers in your network.

Note: These instructions are written for Windows Server 2012 R2. If you're using an older version of Windows Server, your steps and the labels you see may vary.

First, we 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**.

Next, edit the new Group Policy object you just created. When you're done, there will be three WinRM service settings enabled:

Allow remote server management through WinRM

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**.

Now that Windows Remote Management has been enabled on the Group Policy, you need to enable the service that goes with it.

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**.

Now you must allow for inbound remote administration by updating the firewall rules. When you're done, there will be two rules enabled:

Windows Firewall: 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**.

Almost done! The final steps is to create a new inbound firewall rule and update the network list manager for unidentified networks.

1. From the menu tree, click **Computer Configuration > 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 > 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.

All the Windows machines on your network are now WMI-enabled and can be monitored and managed through Auvik.

Was this article helpful?



2 out of 2 found this helpful



Have more questions? [Submit a request \(/hc/en-us/requests/new\)](/hc/en-us/requests/new)

Comments



Brandon Fox

December 05, 2016 21:48

Please note that in different versions of Windows the first step looks for: "Allow remote server management through WinRM" but sometimes it is called: "Allow automatic configuration of listeners."



Krista Foisy

December 05, 2016 22:13

Thanks Brandon! :)



AUVIK SYSTEM STATUS

● Check system status (<http://auvik.statuspage.io/>)

● Check system status (<http://auvik.statuspage.io/>)

Submit your question or comment and we'll be in touch.

Submit your question or comment and we'll be in touch.

SEND A MESSAGE ([HTTP://SUPPORT.AUVIK.COM/HC/EN-US/REQUESTS/NEW](http://support.auvik.com/hc/en-us/requests/new))



RELATED ARTICLES

[How to enable WMI monitoring on a single Windows device \(/hc/en-us/related/click?\)](#)

data=BAH7CjobZGVzDGluYXRpb25fYXJ0aWNsZV9pZGkExBsyDDoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkElkc vDDoLbG9jYWxlSSIKZW4tdXMGOgZFVDoldXJsSSJlZ2hjL2VuLXVzL2FydGljbGV
-3b038c319a3145fbc446b6d2f2a89b367b3b4832)

[How to install the Auvik collector using the Windows service \(/hc/en-us/related/click?\)](#)

data=BAh7CjobZGVZdGluYXRpb25fYXJ0aWNSZV9pZGkEB55pDDoYcmVmZXJyZXJfYXJ0aWNSZV9pZGkElkcvDDoLbG9jYWxlSSIKZW4tdXMGOgZFVDoIdXJsSjEl2hjL2VuLXVzL2FydGJlbGV
-41a4644f559ec7890ff6e745ef10f7a536a86e64)

[How are my credentials used? \(/hc/en-us/related/click?\)](#)

data=BAh7CjobZGVZdGluYXRpb25fYXJ0aWNsZV9pZGkEzt4YDDoYcmVmZXJfYXJ0aWNsZV9pZGkElkcVDDoLbG9jYWxlSSIKZW4tdXMGOgZFVDdoIdXsSSI%2BL2hjL2VuLXVzL2FydGJlbi01da10952ccaab599ebff72324619b0b319eaa6b)

[How to enable SNMP on a VMware ESXi hypervisor \(/hc/en-us/related/click?\)](#)

data=BAH7CjobZGVZdGluYXRpb25fYXJ0aWNSZV9pZGkEZhBMDDoYcmVmZXJyZXJfYXJ0aWNSZV9pZGkElkcvDDoLbG9jYXWxSSIKZW4tdXMGOgZFVDoldXsSSjQL2hjL2VuLXVzL2FydGljbG
-883063eb3b9d78e8bc3e292dea10874a2440aa6d)

[Integrating Auvik with ConnectWise Manage \(/hc/en-us/related/click?\)](#)

data=BAH7CjobZGVZdGluYXRpb25fYXJ0aWNsZV9pZGkE4MU4DDoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkElkcvDDoLbG9jYWxlSSJlKZW4tdXMGOGZFVDoIdXsSSjLL2hjL2VuLXVzL2FydGljbG'
-59a08f1a5c4fa5bb4da900ab744c57fb37e94125)



Auvik is the most efficient & profitable way to manage network infrastructure

Follow on Facebook (<http://www.facebook.com/AuvikNetworksInc>) Follow on Twitter (http://twitter.com/intent/follow?source=followbutton&variant=1.0&screen_name=auviknetworks) Follow on Google+ (<https://plus.google.com/u/0/+Auvik/posts>) Follow on LinkedIn (<http://www.linkedin.com/company/auvik-networks-inc->) Follow on RSS (<http://www.auvik.com/feed/rss/>)

Privacy Policy (<https://www.auvik.com/privacy-policy>) | Terms of Service (<https://www.auvik.com/terms/>).

© Copyright 2013-2017 Auvik Networks. All rights reserved.

