# Purpose

This document describes how to configure the WinRM configuration wizard in Nagios XI.

# Setup

In order to monitor a Windows machine with the WinRM wizard, the target machine will need to be configured to utilize the WinRM protocol. The process is defined below.

## Initialization

- 1. Open PowerShell running as the local computer Administrator account.
- 2. Run the following command to initialize WinRM:

winrm quickconfig

3. When the tool displays Make these changes [y/n]?, type y.

## **Enabling Basic HTTP**

1. Run the following commands in PowerShell:

```
winrm set winrm/config/service/auth '@{Basic="true"}'` ''
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

# **Enabling Basic HTTPS**

**Note:** WinRM HTTPS requires a valid SSL certificate, and you will need to generate one if you do not already have one.

## **Generating a Self-Signed Certificate**

1. Run the following command in PowerShell:

```
New-SelfSignedCertificate -DnsName "[SERVER_HOSTNAME] -CertStoreLocation
Cert:\LocalMachine\My
```

2. Copy the thumbprint that is generated and continue to the **Create WinRM HTTPS Listener** section

## Adding an Existing Certificate With Microsoft Management Console

- 1. Search for and Run mmc.exe
- 2. In the top left, click File -> Add/Remove Snap-in

#### www.nagios.com



- 3. Select Certificates from the list of available snap-ins, and click Add
- 4. Select Computer account and click Next
- 5. Click Finish, then Ok
- Navigate to Console Root -> Certificates (Local Computer) and ensure your certificate is in both:
  - a. Personal -> Certificates
  - b. Trusted Root Certification Authorities -> Certificates

**Note:** If you do not see the certificate in the **Trusted Root Certification Authorities** and **Personal** folders, it must manually be installed.

- 7. Navigate to Console Root -> Certificates (Local Computer) -> Personal -> Certificates and double click the certificate you wish to use
- 8. Click Details
- 9. Scroll to the bottom, copy the **Thumbprint**, and continue to the **Create WinRM HTTPS Listener** section

## **Create WinRM HTTPS Listener**

1. Create a HTTPS listener with the server's host name and the certificates thumbprint using the following command in PowerShell:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
'@{Hostname="[SERVER_HOSTNAME]";
CertificateThumbprint="[CERTIFICATE_THUMBPRINT]"}'
```

## Users

**Note:** User accounts using WinRM must be part of either the local administration or a local group with WinRM execute permissions.

To create a new local user account run the following commands in PowerShell:

- 1. \$Password = Read-Host -AsSecureString
  - a. This will prompt you for a password and store it in the \$Password variable as a secure string
- 2. New-LocalUser -Name '[username]' -Password \$Password -FullName '[user full name]' -Description '[user descrip-tion]'

To create a new local group with WinRM execute permissions do the following:

1. Create a new local group with the following command in PowerShell:

www.nagios.com



New-LocalGroup -Name '[local group name]'

2. Open the WinRM SDDL permissions configuration by running the following in PowerShell:

winrm configSDDL default

- 3. Add the newly created local group:
- Click Add
- Type the name of the local group and click **Ok**
- Select the local group
- Check Allow next to the Execute(Invoke) option
- Click Apply then Ok

# Wizard Usage

1. Navigate to Configure > Configuration Wizards > Windows WinRM

Windows WinRM Configuration Wizard		Step 1	•
Windows Server Information			
* Address ()			
Enter IP Address/Hostname			
• Username ()			
Enter Username			<b></b> ►
* Password ()			
Enter Password	0		
Enable HTTPS ()			
Next >			

www.nagios.com



# How To Configure the WinRM Wizard in Nagios XI

2. In the first step of the **WinRM** wizard, enter the IP address, username, and password for the windows machine you intend on monitoring. Here you are also given the option to use either HTTP or HTTPS to communicate with the target machine. (The default is HTTP)

**Note**: If any of the Windows details/credentials are invalid, the wizard will prevent you from moving to the next step.

- 3. In the second step of the WinRM wizard, configure the services you wish to monitor:
  - a. Memory Usage The memory usage of the target machine.
  - b. CPU Usage The CPU usage of the target machine.
  - c. Disk Usage The disk space usage of the specified disk.
  - d. Windows Services The current state of the specified Windows service(s).
  - e. **Windows Processes** The memory usage, CPU usage, or total count of the specified Windows process(es).
- 4. The remaining steps contain the usual monitoring configuration options each wizard provides.

# More Information:

Using Configuration Wizards

# **Finishing Up**

This completes the documentation on how to configure the WinRM configuration wizard in Nagios XI. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum

Visit Nagios Knowledge Base

Visit Nagios Library

www.nagios.com



Page 4 of 4