Configure WMI on Windows Domain Controller for CEM

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Create a new Group Policy Object
WMI: Configure COM security
User Rights Assignment
Firewall Configuration
WMI Namespace Security
Verify
Troubleshoot

Introduction

This document describes the steps to configure Windows Management Instrumentation (WMI) on Windows Domain Controller for Cisco Energywise Management (CEM). WMI is used to remotely access windows machines to gather data and execute commands. Although script is available that performs all the necessary steps at once, if domain controller is being used to apply policies on the domain devices, it is recommended to change settings in the domain policy, as the devices would override the local changes. This document presents the steps to configure group policy on Windows Domain Controller to prepare the domain devices for WMI interrogation.

Note: Although WMI is available in Windows 2000 with SP2, the CEM application does not support Windows 2000. To use WMI, the CEM application requires Microsoft Windows XP Professional SP2 or later.

Prerequisites

Requirements

Cisco recommends that you have access to Windows Domain Controller, Cisco Energywise Management Suite and Remote machines (assets).

Components Used

The information in this document is based on CEMS 5.2 environment in which Active Directory (AD) asset connector is used to pull WMI information from the remote devices.
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

**Configure**

**Create a new Group Policy Object**

The first step is to create a new group policy object. The group policy object can be created on the domain controller under Group Policy Management as shown:

![Group Policy Object](image)

**WMI: Configure COM security**

To execute WMI queries remotely, specific COM permissions are required. Select the Group policy object created in previous step, right click and select **edit** and then browse to this location:

**Group Policy Management Console (GPMC) > Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

Find the screenshots to configure remote access permissions for the Administrators user for the COM permissions for:

**DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax**

**DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)**
Select **Define this policy setting** and click on **Edit Security**. Provide local and remote access permissions to the account you want to use for WMI.
The CEM application requires both the Backup files and directories and Restore files and directories to load the user profile when it tries to invoke a process. It also requires the Force shutdown from a remote shutdown privilege to allow POWER_OFF action to work.
These changes need to be made in the user rights assignment settings within this Group Policy Object. These rights need to be provided to the account used for WMI.

SeRemote Shutdown Privilege - Force shutdown from a remote system

SeBackup Privilege - Back up files and directories

SeRestore Privilege - Restore files and directories

SeNetwork Logon Right - Access this computer from the network

SeSecurity Privilege - Choose Manage auditing and security log

These settings can be configured under this path:

**Group Policy Management Console (GPMC) > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**

![Group Policy Management Console](image)

**User Rights Assignment**

**Firewall Configuration**

To perform WMI calls to a computer, the RPC port (TCP 135) must be accessible externally. This can be done with the use of the Group Policy Management Editor, from the menu tree, navigate to **Computer Configuration > Policies > Administrative Templates: Policy definitions > Network > Network Connections > Windows Firewall**
Select **Domain Profile**, and double-click **Windows Firewall: Allow inbound remote administration exception**. The Windows Firewall: Allow inbound remote administration exception window appears.

Click **Enabled**.

Ensure that you specify the IP address in Allow unsolicited incoming messages from these IP addresses field.

You can enter * to allow messages from any network, or else type a comma-separated list that contains specific IP addresses or Subnets.

---

**WMI Namespace Security**

To enable WMI access to a machine, specific WMI permissions must be enabled for the used account. This configuration can’t be done via Group Policy on Windows Domain Controller, it needs to be done on the remote machines with the WmiSetNsSecurity tool.
Set the WMI security and run the command (replace %account% with the user account you want to set the security for) on Windows command line tool.

```plaintext
WmiSetNsSecurity Root\CIMV2 -r %account%
```

```plaintext
WmiSetNsSecurity Root\CIMV2\power -r %account%
```

```plaintext
WmiSetNsSecurity Root\Default -r %account%
```

```plaintext
WmiSetNsSecurity Root\WMI -r %account%
```

This configuration needs to be pushed to all the remote machines that remain. This step can also be performed when you create a batch script and push it via an admin logon script or a machine startup script under a group policy.

Configure file system permissions.

The CEM application requires full permissions to access the Cisco subfolder inside the Windows folder (e.g. C:\Windows\Cisco) to store and execute scripts. This step needs to be done on remote assets and details of configuration can be found in this article under remote file system permission section.

https://cem-update.cisco.com/download/files/5.0/docs/CEM_Online_Help/aa1808350.html

Configure registry permissions

The CEM application needs access to the device registry to store various data. Refer to section configuring registry permissions in this article.

https://cem-update.cisco.com/download/files/5.0/docs/CEM_Online_Help/aa1808350.html

**Verify**

Use this section in order to confirm that your configuration works properly.

Verify the WMI functioning by running diagnostics on one of the domain devices from the CEMS GUI. A successful configuration should not show any WMI related errors.

**Troubleshoot**

There is currently no specific troubleshooting information available for this configuration.