Grant Minimum Permission to an Active Directory User Account Used by the Sourcefire User Agent

Document ID: 118637

Contributed by Nazmul Rajib and Douglas Loss, Cisco TAC Engineers.
Jun 05, 2015

Contents

Introduction

This document describes how to provide an Active Directory (AD) user with the minimal permissions needed to query the AD domain controller. The Sourcefire User Agent uses an AD user in order to query the AD domain controller. In order to perform a query, an AD user does not require any additional permissions.

Prerequisites

Requirements

Cisco requires that you install the Sourcefire User Agent on a Microsoft Windows system and provide access to the AD domain controller.

Components Used

This document is not restricted to specific software and hardware versions.

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

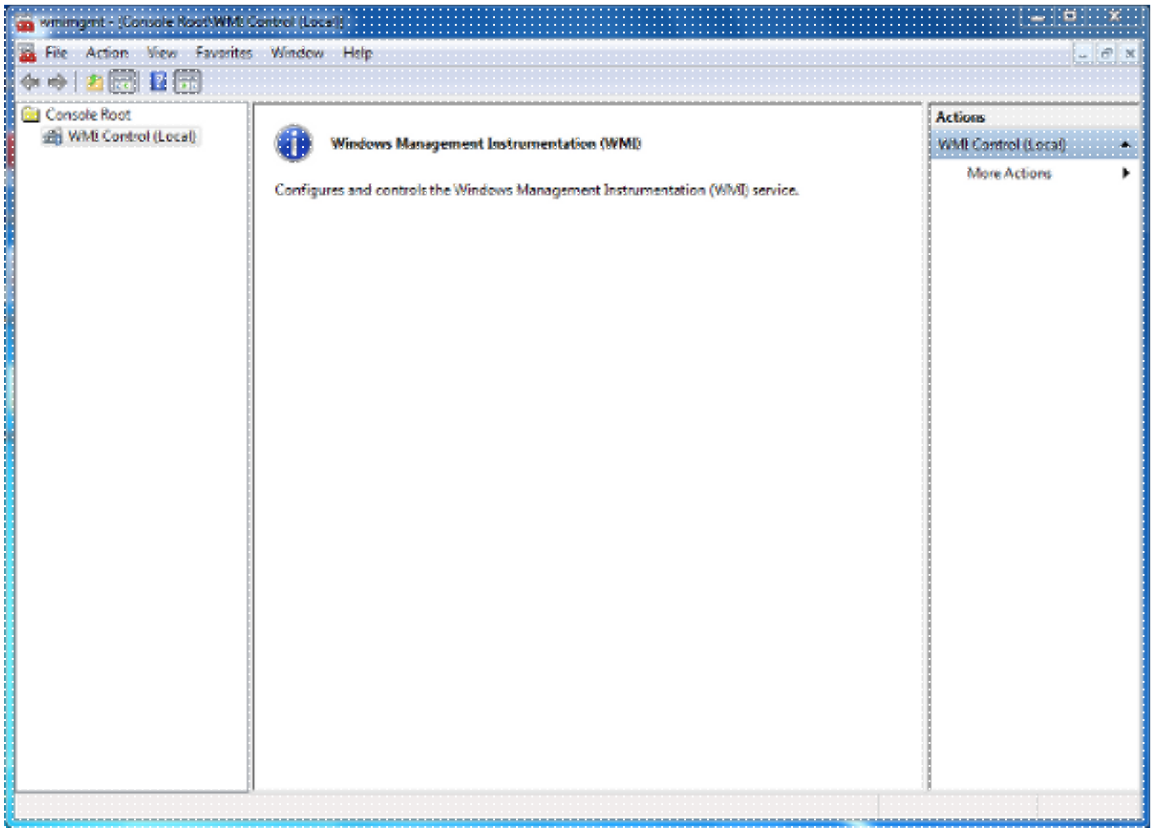
First, an administrator must create a new AD user specifically for User Agent access. If this new user is not a member of the domain administrators group (and they should not be), the user might have to be explicitly granted permission to access the Windows Management Instrumentation (WMI) security logs. In order to grant permission, complete these steps:

1. Open the WMI Control Console:

    a. On the AD server, choose the **Start** menu.

b. Click **Run** and enter **wmimgmt.msc**.

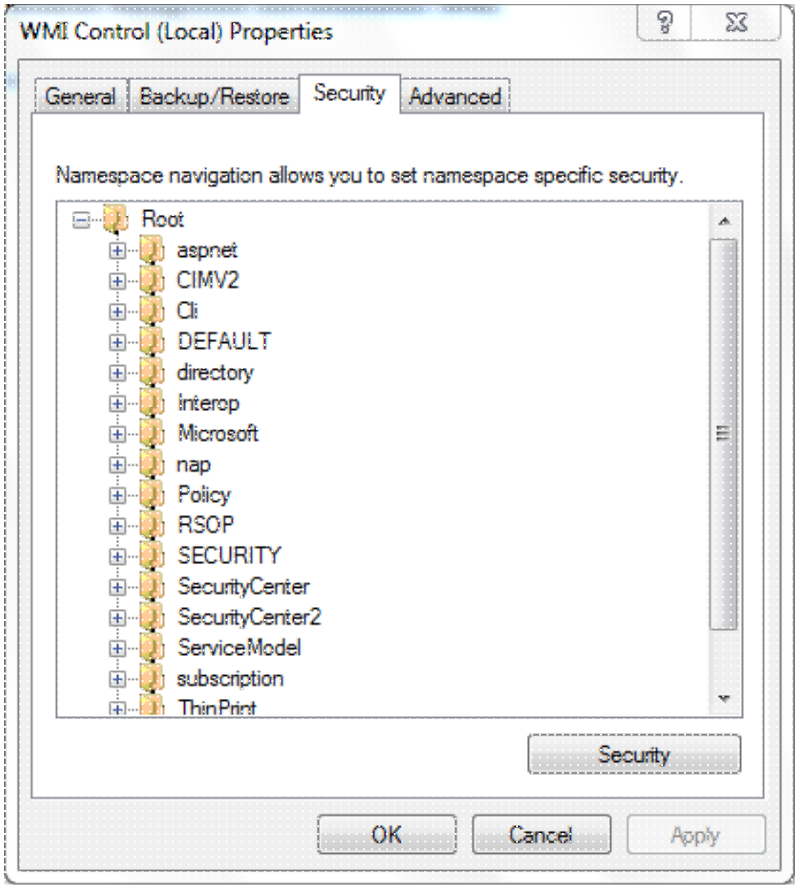
c. Click **OK**. The WMI Control Console appears.



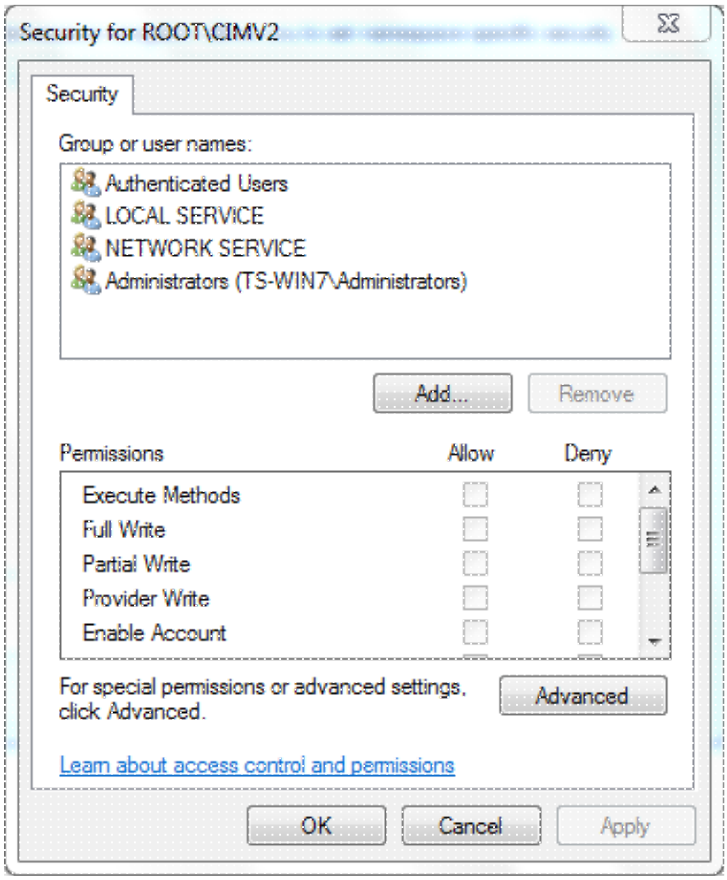
2. On the WMI console tree, right-click **WMI Control** and then click **Properties**.

3. Click the **Security** tab.

4. Select the namespace for which you want to give a user or group access (**`Root\CIMV2`**), and then click **Security**.



5. In the Security dialog box, click **Add**.



6. In the Select Users, Computers, or Groups dialog box, enter the name of the object (user or group) that you want to add. Click **Check Names** in order to verify your entry and then click **OK**. You might have to change the location or click **Advanced** in order to query for objects. See the Context-sensitive help (**?**) for more detail.

7. In the Security dialog box, in the Permissions section, choose **Allow** or **Deny** in order to grant permissions to the new user or group (easiest to give all permissions). The user must be given at least the **Remote Enable** permission.

8. Click **Apply** in order to save changes. Close the window.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

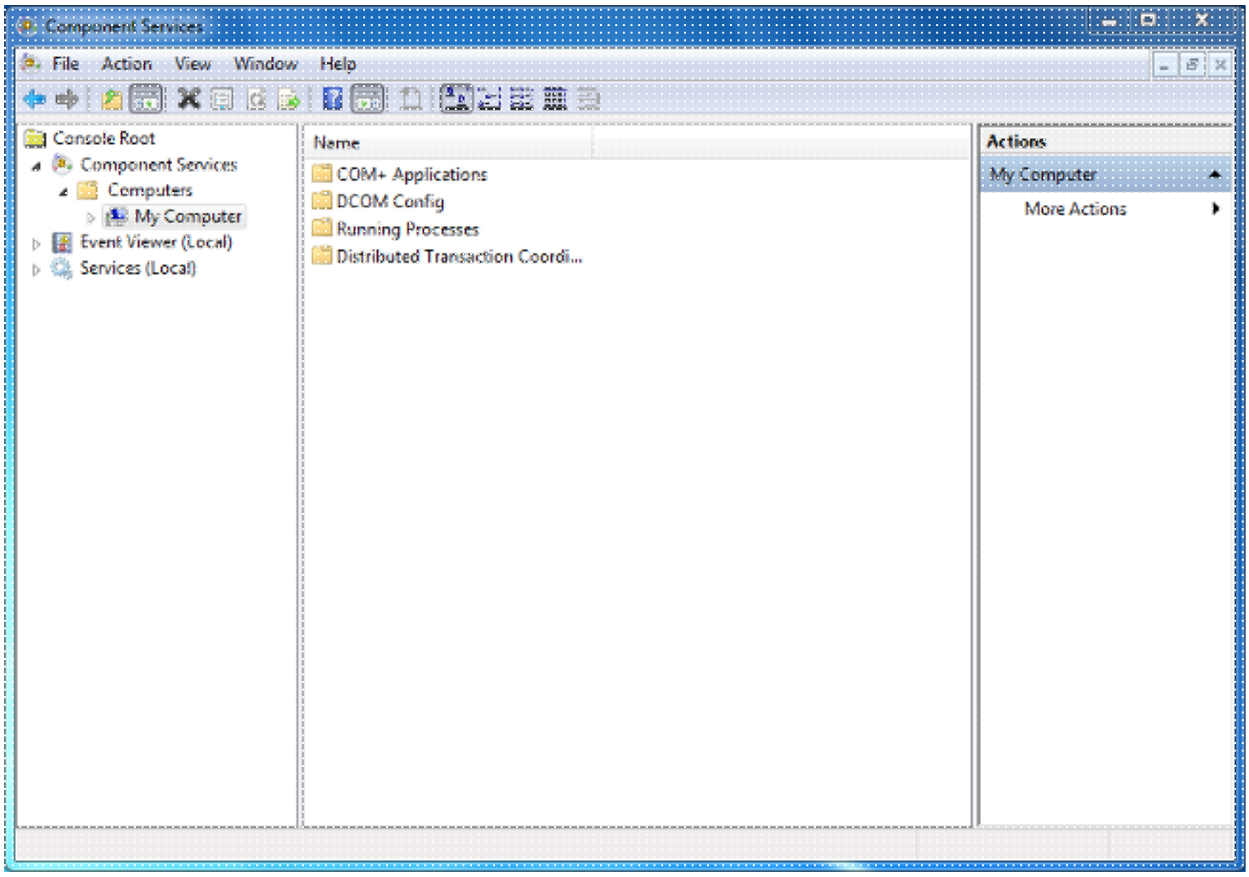
This section provides information you can use to troubleshoot your configuration.

If an issue persists after the configuration changes, update the Distributed Component Object Model (DCOM) settings in order to allow remote access:

1. Choose the **Start** menu.

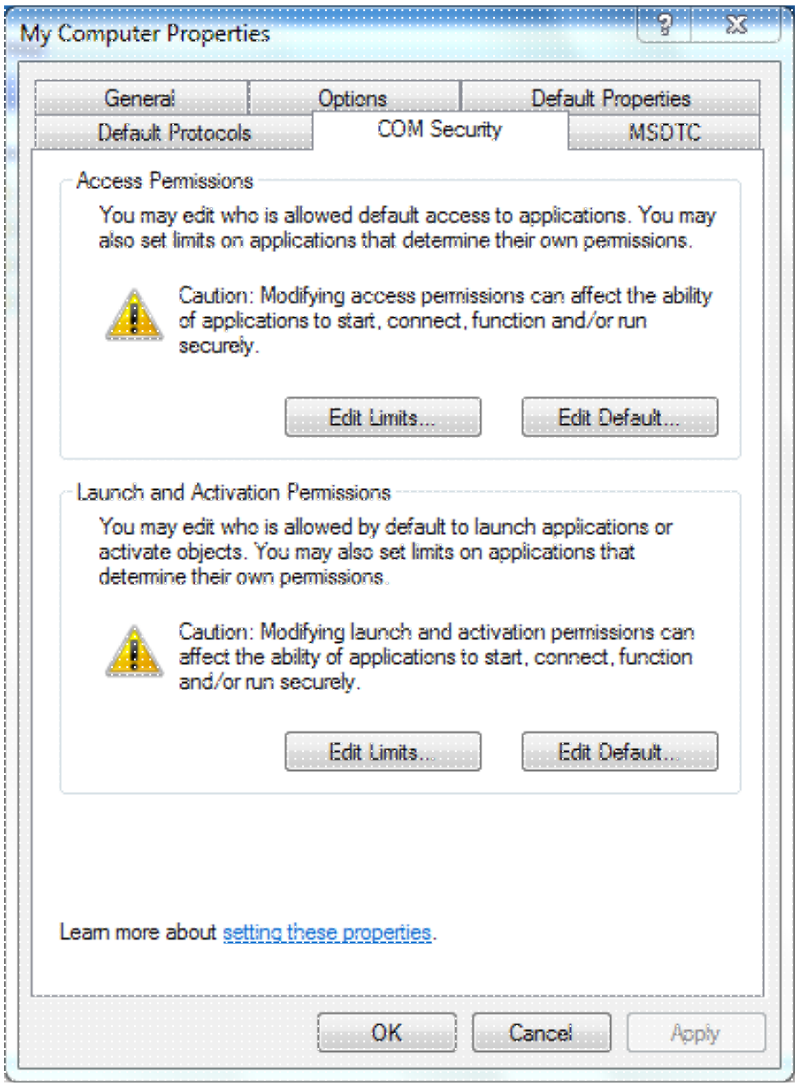
2. Click **Run** and enter **DCOMCNFG**.

3. Click **OK**. The Component Services dialog box appears.



4. In the Component Services dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer** and choose **Properties**.

5. In the My Computer Properties dialog box, click the **COM Security** tab.



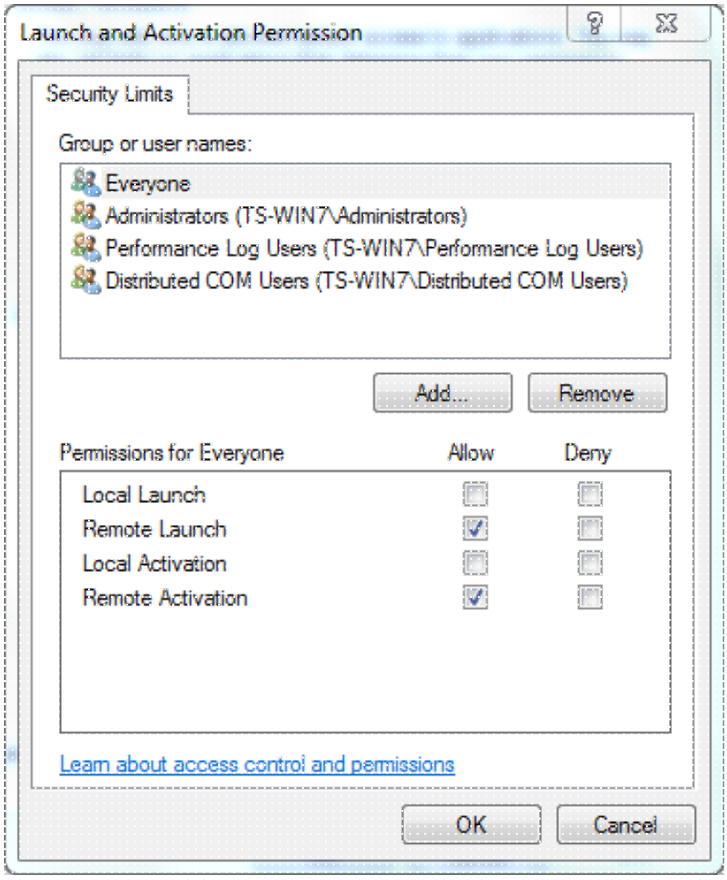
6. Under Launch and Activation Permissions, click **Edit Limits**.

7. In the Launch and Activation Permission dialog box, complete these steps if your name or your group does not appear in the Groups or user names list:

    a. In the Launch and Activation Permission dialog box, click **Add**.

    b. In the Select Users, Computers, or Groups dialog box, enter your name and the group in the Enter the object names to select field, and then click **OK**.

8. In the Launch and Activation Permission dialog box, select your user and group in the **Group or user names** section.



9. In the Allow column under Permissions for User, check the **Remote Launch** and **Remote Activation** check boxes, and then click **OK**.

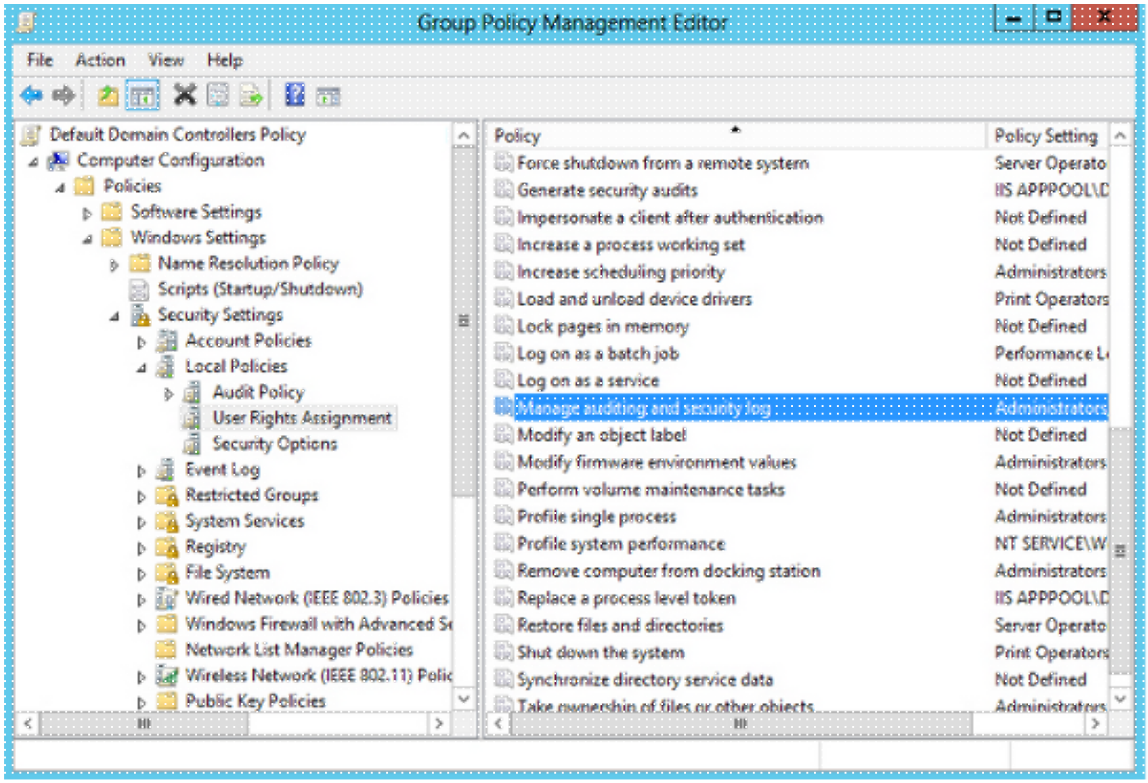
   Note: A user name must have rights to query for user login data on an AD server. In order to authenticate with a user via proxy, enter a fully qualified user name. By default, the domain for the account you used to log into the computer where you installed the agent auto-populates the Domain field. If a user you supply is a member of a different domain, update the domain for the user credentials supplied.
10. If the problem persists, on the Domain Controller try to add the user in the Manage auditing and security log policy. In order to add the user, complete these steps:

    a. Choose the **Group Policy Management Editor**.

    b. Choose **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.

    c. Choose **Manage auditing and security log**.

    d. Add the user.



Updated: Jun 05, 2015 Document ID: 118637