ManageEngine
EventLog Analyzer

WMI log collection using a non-admin domain user

To collect WMI logs from a domain controller in EventLog Analyer, it is necessary to add a domain admin account of that domain in it. Alternatively, you can create a user account in Active Directory with sufficient permissions to collect WMI logs from the Domain Controller, and add that account in EventLog Analyzer.

This document provides step-by-step instructions to create a domain user account in Active Directory and assign permissions to collect WMI logs from a domain controller.

Outline

- Create a non-admin domain user in Active Directory.
- Add the user to Performance Log Users and Distributed COM Users group.
- Create a new group policy in the Group Policy management console.
- Assign rights to the created user.
- Enforce the created Group Policy.
- Update the Group Policy on the WMI client and server.
- Grant WMI Namespace Security Rights to the created user.
- Grant COM permissions to the created user.
- For log collection, use this user's credentials in the EventLog Analyzer web-console.

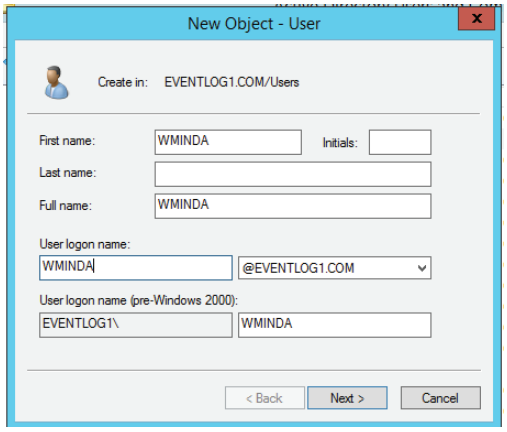
Steps

1. Create a non-admin domain user in Active Directory

a. Navigate to **Active Directory Users and Computers.**

b. Click on **Users** → **New** → **User.**

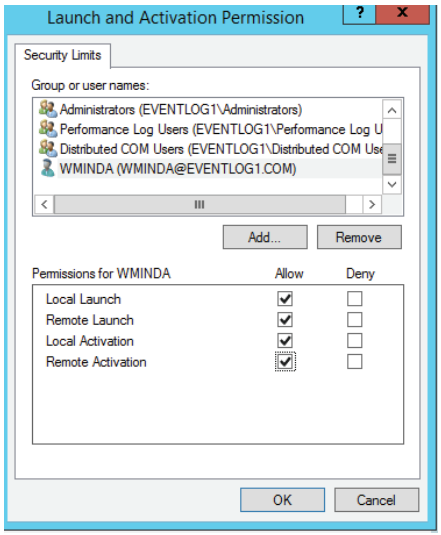
c. Enter the user details such as first name, last name, logon name, and password in the window that opens and create the user.



2. Add the created user to the Performance Log Users and Distributed COM Users group

Right-click on the created user and click **Add to a group.** The user needs to be added to the following groups.

- Performance Log Users
- Distributed COM Users



3. Create a new Group Policy in the Group Policy Management console.

4. Assign rights to the created user

a. Right click on the created Group Policy and click Edit.

b. The **Group Policy Management Editor** will open. Navigate to Computer **Configurations → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.**

c. **Right-click on the specific right** and click on **Properties.**

Rights to be granted

- Act as part of the operating system
- Log on as a batch job
- Log on as a service
- Replace a process level token
- Manage Auditing and Security Log Properties

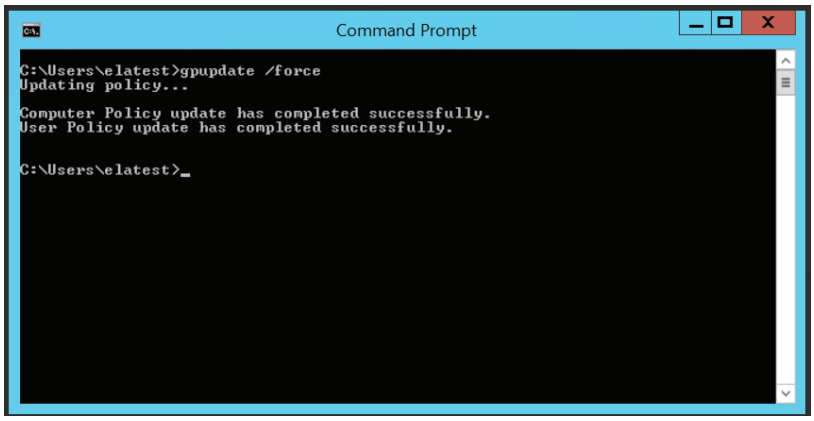
d. Enable the **Define these policy settings,** click on **Add User or Group,** select the **created user** and click **Apply.**

5. Enforce the created Group Policy

In the left pane, right-click on the created Group Policy and click **Enforce**.

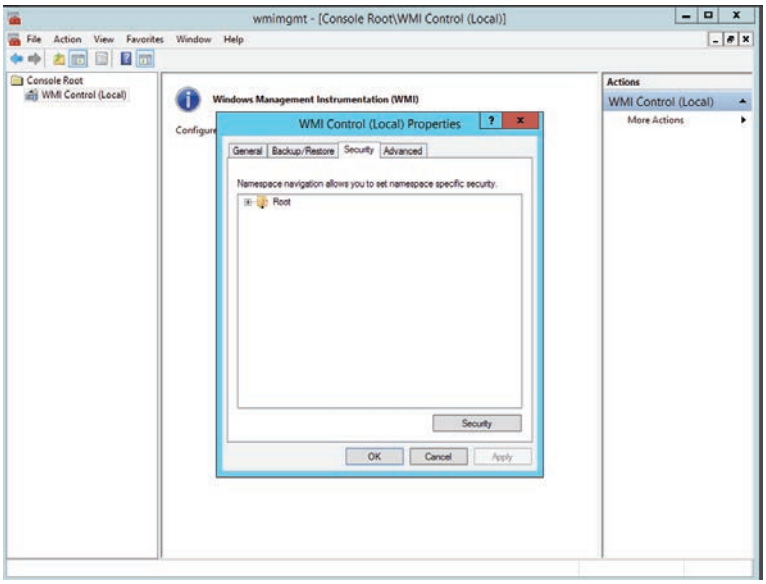
6. Update the created Group Policy on the WMI client and server

Open **Command Prompt** as an administrator in both the client and server, and run the command below.



7. Grant WMI Namespace Security Rights to the created user

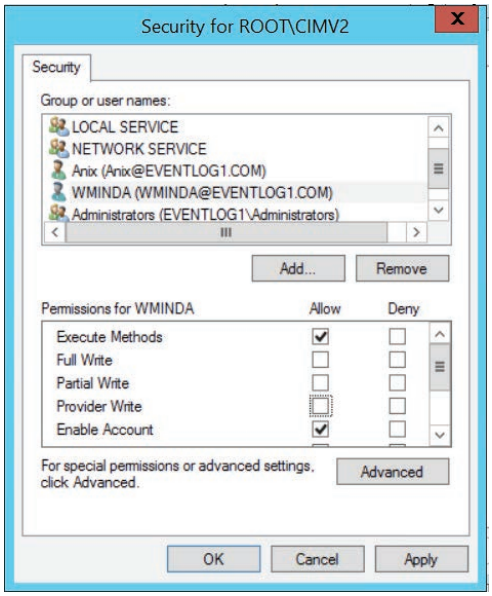
a. In the Domain Controller from which the logs are to be collected, open the **Run command** and type **wmimgmt.msc** to open the **WMI Management Console**.



b. Right-click on **WMI Control(Local)** and click on **Properties.**

c. In the **WMI Control Properties** popup that opens, click on the **Security tab.**

d. In the Security tab, **expand the Root NameSpace** and select **CIMV2 Namespace.**



e. Click the **Security** button that appears on the bottom right corner to open the Security for ROOT\CIMV2.

f. Click **Add** and select the created user.

g. The user now needs to be granted permissions. To do this, click on the user and check the **Allow boxes** for the permissions below.

i Execute Methods

ii Enable Account

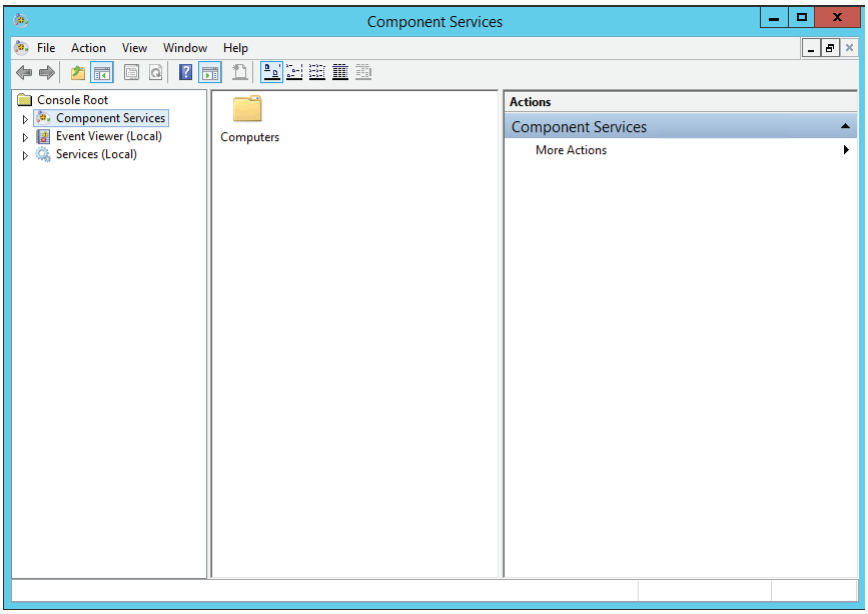
iii Remote Enable

iv Read Security

h. **Apply the changes** and click **OK** to exit the WMI Management console.

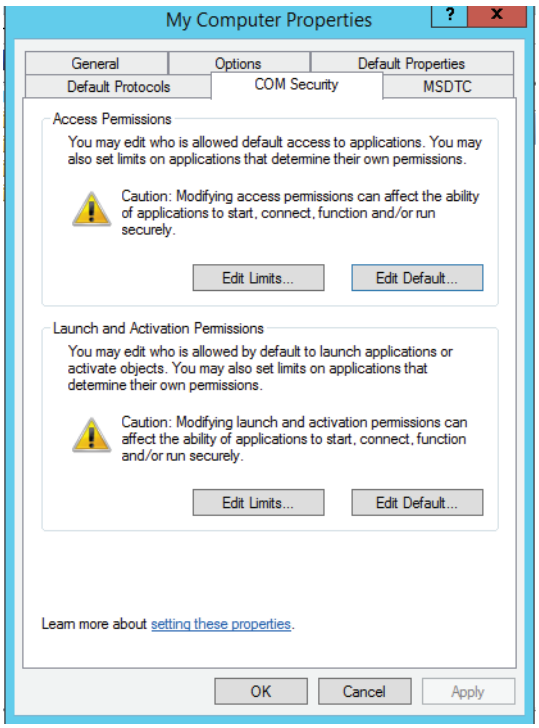
8. Grant COM permissions to the created user

a. In the Domain Controller from which the logs are to be collected, navigate to **Start → Administrative Tools → Component Services.**

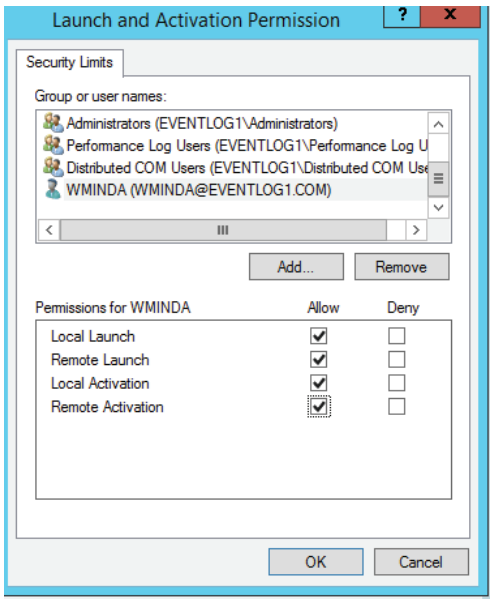


b. Expand the Computers folder, navigate to **My Computer → Properties → COM SECURITY.**

c. Under **Access Permissions,** click on **Edit Limits** and **add the created user** by clicking **Add. Grant all the permissions** and click **OK.**



d. Under **Launch and Activation Permissions,** click on **Edit Limits** and **add the created user** by clicking Add. **Grant all the permissions** and click **OK.**



Once you grant all the above mentioned permissions, the created non-admin user will be able to collect logs from a domain controller.

9. For log collection, use this user's credentials in the EventLog Analyzer web-console.