

McAfee Enterprise Security Manager

Polling Windows Event Logs using a Non-Admin Account

June 28, 2012

Important Note:

The information contained in this document is confidential and proprietary.

Please do not re-distribute without permission.

2 Introduction

This guide will provide information on how to use a non-admin account to poll Windows 2003 and 2008 Event Logs via WMI using a non-administrator account which can then be utilized by McAfee Enterprise Security Manager.

3 Configuring a non-Admin for WMI

3.1 Creating the user/group, assigning security policies and permissions

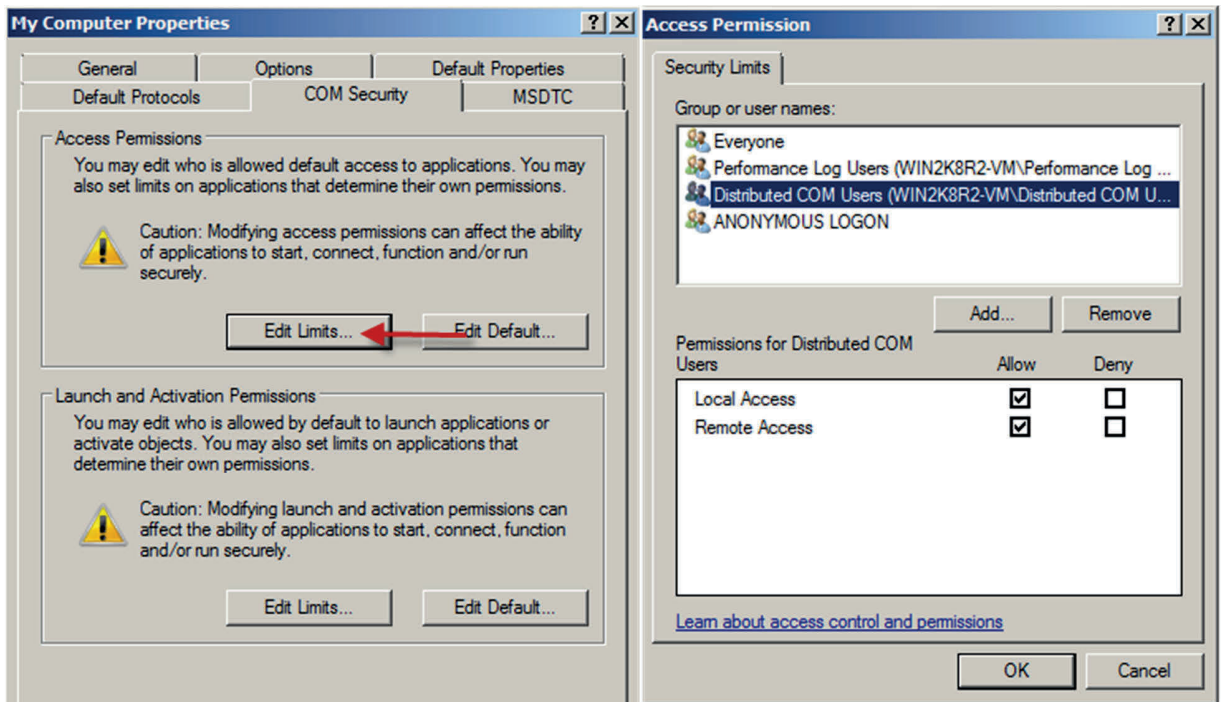
1. Create a domain user account to be used for log collection.
2. Create a domain group that will receive all of the rights that WMI Collection user needs.
 - a. Note: Make sure you assign all rights to a group and not directly to a user.
3. Put the WMI Collection user into the newly created group.
4. Put the newly created WMI Collection user into the following domain groups:
 - a. Performance Log Users
 - b. Distributed COM Users
5. Run one of the following three Microsoft Management Console (MMC) snap-ins:
 - a. Local Security Policy snap-in (secpol.msc) for member servers, or
 - b. Default Domain Security Policy snap-in (dmpol.msc) if you wish to configure these settings domain-wide as a GPO, or
 - c. Default Domain Controller Security Settings snap-in (dcpol.msc) if you wish to assign the rights only on domain controllers.
6. Windows 2008 Server R2, open Group Policy management (gpmc.msc).
 - i. Right click Default Domain Controller Policy, click Edit.
7. Once the snap-in has started, expand **Security Settings, Local Policies, User Rights Assignment**.
8. Assign your new group at least the following rights:
 - a. Act as part of the operating system
 - b. Log on as a batch job
 - c. Log on as a service
 - d. Replace a process level token
9. Close the Policy Settings Utility.

Distributed Component Object Model rights assignments

Configure DCOM security for the WMI collection group.

1. Click **Start, Administrative Tools, Component Services**.
2. Expand **Console Root, Computers, My Computer**. Right-click **My Computer** and select **Properties**.
3. In the window that appears, click the **COM Security** tab.

4. Under **Access Permissions**, click **Edit Limits**.
5. Review that the **Distributed COM Users** group has all items checked under **Allow**.



6. Once you've reviewed the presence of **Distributed COM Users**, click **OK** to save your changes and return to the COM Security tab.
7. Under **Launch and Activation Permissions**, click **Edit Limits**.
8. In the list of groups and permissions, ensure that the **Distributed COM Users** group has all items checked under **Allow**.

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/208131107110006106>