HOW TO CONFIGURE WMI ACCESS ON WINDOWS FOR A NON ADMIN USER

Hi,If you, like me have to configure WMI access on Windows servers for a non admin user in order for Zenoss to read the eventlog etc, read on...

Introduction

Zenoss is able to read & query Windows servers via WMI in order to obtain Eventlog information. Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems. WMI also supplies management data to other parts of the operating system and products like zenoss. For security purposes you can use a limited domain user account to access the WMI infrastructure and relevant components. The domain user acount has rights to only access the appropriate areas of the server to obtain information for Zenoss.As the main objective is read & query the Windows event logs via WMI. Modifications to the windows server security will need to have access granted to the specific account (zenwmi) at 4 different levels in order for Zenoss to function correctly and obtain the event log information the Windows team requires to be displayed in Zenoss.The following information describes the 4 levels or areas that require acess to be configured for the specific user. These 4 requirements are all needed and are in logical order as one follows on to the next as shown in this diagram attached .

1. DCOM

DCOM stands for Distributed COM and COM stands for Component Object Model (COM). COM is the standard method for communication between client/server apps and highlevel APIs for Windows developers. DCOM users Remote Procedure Call to expose COM objects on a computer to remote clients on other computers.Prior to XP SP2 (and the introduction of these 2 DCOM security settings), it was difficult for an administrator to assess or control which COM objects were available to remote users and this is even more important since COM objects can allow anonymous access. Each COM object has its own ACL and you would have had to look at each COM object's ACL to determine if remote access were allowed and to whom. This policy and DCOM: Machine Access Restrictions In Security Descriptor Definition Language (SDDL) syntax put a system wide access check that all DCOM clients (local or remote) must pass before hitting the individual COM object's ACLs. This system-wide DCOM check is like share permissions on a shared folder. Many files may be accessible through a given network share and each file may have it's own unique permissions but you must first pass the share level permissions before the file permissions are checked.Security in WMI is related to connecting to a WMI namespace. WMI uses DCOM to handle remote calls. One reason for failure to connect to a remote computer is due to a DCOM failure, Therefore, this is the first access that must be granted to the specific user and happily can be granted by adding the user to the local or domain distributed COM users group on the Server. There is a domain GPO which adds the domain user to the relevant grounds need by Zenoss. Specific user access can be granted by following & applying the following link.http://msdn.microsoft.com/en-us/library/aa393266.aspx

2. WMI

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM)

industry standard to represent systems, applications, networks, devices, and other managed components. CIM is developed and maintained by the Distributed Management Task Force (DMTF). The ability to obtain management data from remote computers is what makes WMI useful. Remote WMI connections are made through DCOM.WMI provides a uniform interface for any local or remote applications or scripts that obtain management data from a computer system, a network, or an enterprise. The uniform interface is designed such that WMI client applications and scripts do not have to call a wide variety of operating system application programming interfaces (APIs). Many APIs cannot be called by automation clients like scripts or Visual Basic applications. Other APIs do not make calls to remote computers.To obtain data from WMI, an application like Zenoss accesses WMI Classes or provides data to WMI by writing a WMI provider.

Namespace Access Settings

You can change the access to a WMI namespace using the WMI Control or programmatically.

Term	Description
Execute Methods	Permits the user to execute methods defined on WMI classes. Corresponds to the WBEM_METHOD_EXECUTE access permission constant.
Full Write	Permits full read, write, and delete access to WMI classes and class instances, both static and dynamic. Corresponds to the WBEM_FULL_WRITE_REP access permission constant.
Partial Write	Permits write access to static WMI class instances. Corresponds to the WBEM_PARTIAL_WRITE_REP access permission constant.
Provider Write	Permits write access to dynamic WMI class instances. Corresponds to the WBEM_WRITE_PROVIDER access permission constant.
Enable Account	Permits read access to WMI class instances. Corresponds to the WBEM_ENABLE access permission constant.
Remote Enable	Permits access to the namespace by remote computers. Corresponds to the WBEM_REMOTE_ACCESS access permission constant.
Read Security	Permits read-only access to DACL settings. Corresponds to the READ_CONTROL access permission constant.
Edit Security	Permits write access to DACL settings. Corresponds to the WRITE_DAC access permission constant.

This is the second access requirement that is needed for Zenoss. For the DMSI Windows team, the zenwmi domain user is manually given Remote Enable & Enable Account permissions to the CIMV2 class. This is done by a user written program, WMISecurity that can be run at the command prompt.The syntax is as follows: WmiSecurity.exe /C="%computername%" /A /N=Root/CIMV2 /M=" DOMAIN\USER:REMOTEACCESS" /R Specific user access can be granted by following & applying the following link.http://technet.microsoft.com/en-us/library/cc787533%28WS.10%29.aspx

3. Service Control Manager

The service control manager (SCM) is started at system boot. It is a remote procedure call (RPC) server, so that service configuration and service control programs can manipulate services on remote machines. SCM maintains a database of the installed services and driver services that allow the operating system to start successfully, and provides a unified and secure means of controlling them. The database, which is stored in the Windows system registry, includes configuration and security information about each service or driver service.System administrators should use the Services snap-in or the sc.exe command-line tool

to query or configure services.The service functions provide an interface for the following tasks performed by the SCM:Maintaining the database of installed services.Starting services and driver services either upon system startup or upon demand.Enumerating installed services and driver services.Maintaining status information for running services and driver services.Transmitting control requests to running services.Locking and unlocking the service database.Zenoss requires access to this manager in order to scan the machine for which windows services are installed on it and subsequently provide status information on the event page besides gaining access to the eventlog (which is a service). This is the third access requirement which needs to be modified for Zenoss. This is configured by command line (sc.exe) and is also included in the tasks section of the automatic network install. Specific user access is the only method of configuration for this type of access & can be granted by following & applying the following link.http://support.microsoft.com/kb/907460The command line used for Windows servers is:sc sdset SCMANAGER D:(A;;CC;;;AU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPRC;;;S-1-5-21-1248577188-10479689-3873521419-99999)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

4. Event Log Permissions

Finally to read and list the Windows events in Zenoss event page, the user defined in the properties of Zenoss Orangiser has to be given rights to read the log. Unfortuntely as you have just read, you are not able to just add the rights to the event log and be done with it, the above modifications needed to have been actioned beforehand. The easiest way to perfom this task for the hundreds of Windows servers at Sopra was to create a domain wide GPO.A policy setting determines which user accounts have access to log files and what usage rights are granted. Individual setting may be specified for each of the Application, Security, Setup, and System event log channels. For Zenoss each Log must by modified in order the the ZenEventlog connection is UP.Enabling this setting allows you to enter a security descriptor for the log file. The security descriptor controls who can read, write, or clear the event log. You enter the security descriptor using Security Definition Description Language (SDDL) as we have read above. The following link explains how to add specific user access to the Eventlog via a GPOhttp://support.microsoft.com/default.aspx/kb/323076The structure of the Eventlog key is as follows: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application,Security,System,CustomLogNote that domain controllers record events in the Directory service and File Replication service logs and DNS servers record events in the DNS server.CustomSD Restricts access to the event log. This value is of type REG_SZ. The format used is Security Descriptor Definition Language (SDDL). Construct an ACL that grants one or more of the following rights: Read (0x0001) Write (0x0002) Clear (0x0004) To be a syntactically valid SDDL, the CustomSD value must specify an owner and a group owner (for example, O:BAG:SY), but the owner and group owner are not used. If CustomSD is set to a wrong value, an event is fired in the System event log when the event log service starts, and the event log gets a default security descriptor which is identical to the original CustomSD value for the Application log. SACLs are not supported.The SDDL permissions used for Windows servers is:O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x1;;;S-1-5-21-1248577188-10479689-3873521419-99999)

Error Summary

I have figured out the following after lots of trial and error. It is a logical process, almost like walking through one security door after another to get to the windows Eventlog. If you see the following ZenWin or ZenEventlog errors in the event page you need to check the relevant section or link to determine where the fault lies.Component: ZenWinMessage: Could not read the status of Windows services (NT_STATUS_ACCESS_DENIED). Check your username/password settings and verify network connectivity.Component: ZenEventlogMessage: Could not read the Windows event log (NT_STATUS_ACCESS_DENIED). Check your username/password settings and verify network connectivity.This error relates to the DCOM Permissions & is resolved by implementing http://

msdn.microsoft.com/en-us/library/aa393266.aspx, check that the ZenWMI user is a member of the Distributed COM users group on the server.Component: ZenWinMessage: Could not read the status of Windows services (NT code 0x80041003). Check your username/password settings and verify network connectivityconnectivity.Component: ZenEventlogMessage: Could not read the Windows event log (NT code 0x80041003). Check your username/password settings and verify network connectivityThis error relates to the WMI Permissions & is resolved by implementing http://technet.microsoft.com/en-us/library/cc787533.aspx, Check to see that the ZenWMI users has Enable Account & Remote Enable access to the CIMV2 namespace in WMI Control on the serverComponent: ZenWinMessage: Could not read the status of Windows services (NT code 0x80041001). Check your username/password settings and verify network connectivityThis error relates to the SCM Permissions & is resolved by implementing http://support.microsoft.com/kb/907460, check to see if the ZenWMI user Unique SID has been added to the SCM SSDL, type "sc sdhow scmanager", if not copy and pase the above command, once this is done you should get a cleared "zenwin wmi connection is up" messageComponent: ZenWinMessage: Could not read the status of Windows services (NT code 0xc002001b). Check your username/password settings and verify network connectivity.Component: ZenEventlogMessage: Could not read the Windows event log (NT code 0xc002001b). Check your username/password settings and verify network connectivity.This error relates to the Eventlog Permissions & is resolved by implementing http://support.microsoft.com/kb/323076, As this is set by GPO, check to see if the GPO was correctly enforced and use the regisitry editior to check that the above SDDL is present, goto HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\"LOG" and read the Custom SD string value, once this is modified correctly, you should get a cleared "zeneventlog wmi connection is up" message

Other Errors

Component: ZenEventlogMessage: Could not read the Windows event log (ExecNotificationQuery (WBEM_E_ACCESS_DENIED)). Check your username/password settings and verify network connectivity.This usually relates to an missing EventLog permission and that the SSDL has not been applied to all the event logs, application system, security, etc.Component: ZenPerfwmiMessage: Could not read the WMI value (NT code 0x80010105). Check your username/password settings and verify network connectivity.I forget.. will have to recall how I fixed it... I think it was due to the "users" group being removed the right to log onto the computer in the local policy..Component: ZenPerfwmiMessage: Could not read the WMI value (NT code 0x80041010). Check your username/password settings and verify network connectivity.This usually relates to a missing WMI namespace, check that Service pack 2 is installed,or recreate/reset the WMI namespaces.The command winnts2k\system32\wbem\wmiadap.exe /f will often restore missing WMI performance counters.Sources:http://msdn.microsoft.com/en-us/library/aa392740%28VS.85%29.aspxhttp://support.microsoft.com/kb/820847http://msdn.microsoft.com/en-us/library/aa394528%28VS.85%29.aspx

Final thanks to all the forum members for their help and input over time.

Alzoo