

Knowledge Base Article: Article 216

How to use a domain user account for NSI WMI Centralized Server v10

Date: November 5th, 2010

Problem:

When NSI WMI Centralized Server is attached to a domain and you want to collect WMI information from servers attached to the same domain, you have to use a domain user account et configure additional parameters on each remote server on which you want to collect WMI information.

The Microsoft Developer Network (MSDN) describe this process in an article where the subject is "User Account Control and WMI" at http://msdn.microsoft.com/en-us/library/aa826699(VS.85).aspx

1. Create a domain user

Create a domain user WMIUser that belongs to the domain users group.

2. Grand DCOM rights to this user

Start Component services management from Administration tools:



www.clickndecide.com



Right click on computer, select properties the COM Security, the screen below should appear:

1y Computer Properties 🛛 🔹 👔 🗙
General Options Default Properties Default Protocols COM Security MSDTC
Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.
Edit Limits
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.
affect the ability of applications to start, connect, function and/or run securely.
Edit Limits Edit <u>D</u> efault
Learn more about <u>setting these properties</u> .
OK Cancel Apply





Access Permissions

Click on "Edit Limits...", add WMIUser and enable Local / Remote Launch as below:

Access Permission		? ×
Security Limits		
Group or user names:		
Everyone WHIUser (WMIUser@fla.loca WMIUser (WMIUser@fla.loca && Performance Log Users (FLA- && Distributed COM Users (FLA-I && ANONYMOUS LOGON	al) -NSI2008-64\Perf NSI2008-64\Distri	ormance Log buted COM
	Add	<u>R</u> emove
Permissions for WMIUser	Allow	Deny
Local Access Remote Access	N	
Learn about access control and permissions		
	OK	Cancel



Click&DECIDE Business Application Intelligence | FAQ

Launch and Activation Permissions

Click on "Edit Limits...", add WMIUser, enable Local / Remote Launch and Local / Remote Activation as below:

Launch and Activation Permissio	n	? ×
Security Limits		
Group or user names: & Everyone & WMIUser (WMIUser@fla.loca & Administrators (FLA-NSI2008-	al) 64\Administrators	.)
Reformance Log Users (FLA- & Distributed COM Users (FLA-)	-NS12008-64\Perf NS12008-64\Distri	ormance Log buted COM
	A <u>d</u> d	<u>R</u> emove
Permissions for WMIUser	Allow	Deny
Local Launch Remote Launch Local Activation Remote Activation	3 3 3 3	
Learn about access control and permissions		
	OK	Cancel





3. Grand WMI namespaces rights to this user

Start Computer management from Administration tools:







Right click on WMI Control, select Properties, and then Security. Expand the Root node, select CIMV2 and the screen below should appear:

WMI Control Properties	? ×
General Backup/Restore Security Advanced	
Namespace navigation allows you to set namespace specific security.	
Root Root ONV2 OINV2	
The State of the	-
<u>S</u> ecurity	
OK Cancel App!	y





Click on Security, add WMIUser and enable "Remote Enable" as below:

Security for ROOT\CIMV2		×
Security		
<u>G</u> roup or user names:		
& Authenticated Users		
& LOCAL SERVICE		
& NETWORK SERVICE		
WMIUser (WMIUser@fla.loc	al)	
Administrators (FLA-NSI2008-	-64\Administrators	:)
	A <u>d</u> d	<u>R</u> emove
Permissions for WMIUser	Allow	Deny
Provider Write		
Enable Account		
Remote Enable	\checkmark	
Read Security		
Edit Security		
For special permissions or advance click Advanced.	ed settings,	Advanced
Learn about access control and p	ermissions	
OK	Cancel	Apply



Click&DECIDE Business Application Intelligence | FAQ

Then click on Advanced, then edit permission for WMIUser and select "this namespace and subnamespaces" as below:

Permission Entry for CIMV2		×
Object		
Name: WMIUser (WMIUser@fla.local)		⊆hange
Apply to: This namespace and subnar	nespaces	•
Permissions:	Allow	Deny
Execute Methods Full Write Partial Write Provider Write Enable Account Remote Enable Read Security Edit Security		
Apply these permissions to objects ar containers within this container only <u>Managing permissions</u>	nd/or	Clear All
	ОК	Cancel





Then do the same for DEFAULT as you did for CIMV2.

WMI Control Properties	? ×
General Backup/Restore Security Advanced	
	- 1
Namespace navigation allows you to set namespace specific security.	_
E Root	▲
E CIMV2	
Herop	
E Policy	
🗄 👜 😥 RSOP	
🗄 🕀 BECURITY	
💿 😥 ServiceModel	
🗄 🕀 🕀 subscription	_
🗄 🔑 WebAdministration	- I I
	<u> </u>
<u>S</u> ecurity	
OK Cancel Aor	du I

4. Add the domain user to the local administrator group

Add WMIUser to the local administrator group of the server.

5. Windows 2008 UAC special consideration

The process describe in the MSDN article "Securing a Remote WMI Connection" at <u>http://msdn.microsoft.com/en-us/library/aa393266(v=VS.85).aspx</u> should work even the UAC is enable Windows 2008 server.

Unfortunately, this process is not enough if UAC is enabled on a Windows 2008 on which you want to get WMI information and if NSI WMI Centralized Server runs also Windows 2008. To make it working properly the registry entry below should be added

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] "LocalAccountTokenFilterPolicy"=dword:00000001

But if the NSI WMI Centralized Server runs Windows 2003, this entry is not mandatory. So, we can conclude the UAC of the Windows 2008 on which we want to get WMI information is involved only if the server which spied this information runs Windows 2008.

6. Reboot to apply all changes

