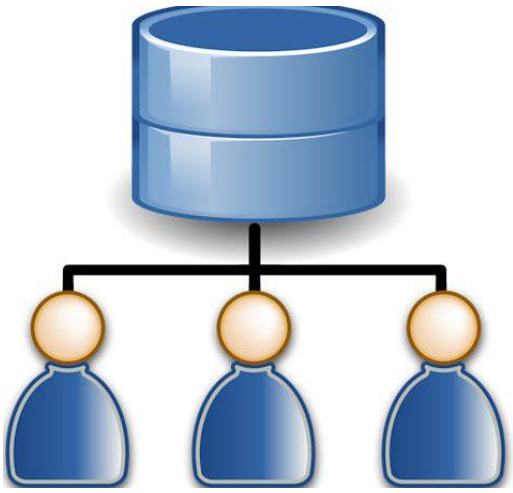
Integrating LANGuardian with Active Directory using WMI



Integrating LANGuardian with Active Directory allows you to search network activity by user name as well as IP address. It is ideal for environments where DHCP is used. You need to complete these five steps to enable the integration.

1. Create an AD account which your LANGuardian will use for logging onto domain
2. Assign WMI permissions to this user
3. Add user to ***Performance Log Users*** and ***Event Log Readers*** groups
4. Check access rights using ***wbemtest*** application
5. Configure AD integration on LANGuardian

1. Create a standard user logon for LANGuardian

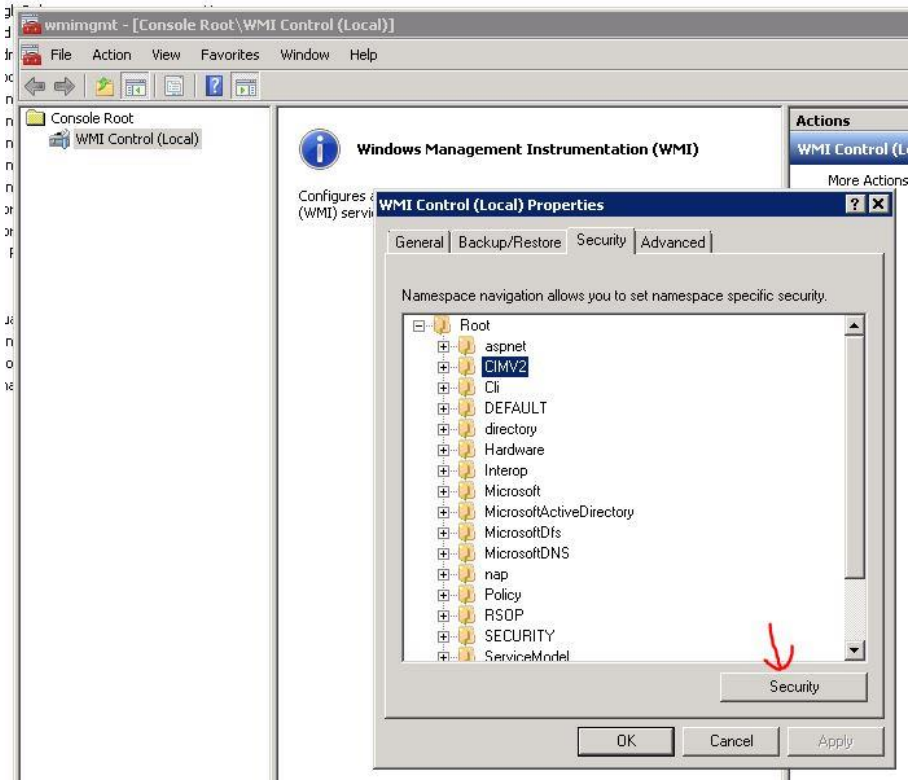
You can use an existing account for AD integration, but for the purposes of this guide, we are going to create a new one called LANGuardian. This account does not need to be an administrator or in the domain admins group, but it does need extra permissions which are described below.

We recommend that the account is set with a password which does not expire as there is no facility within the LANGuardian GUI to set AD passwords.

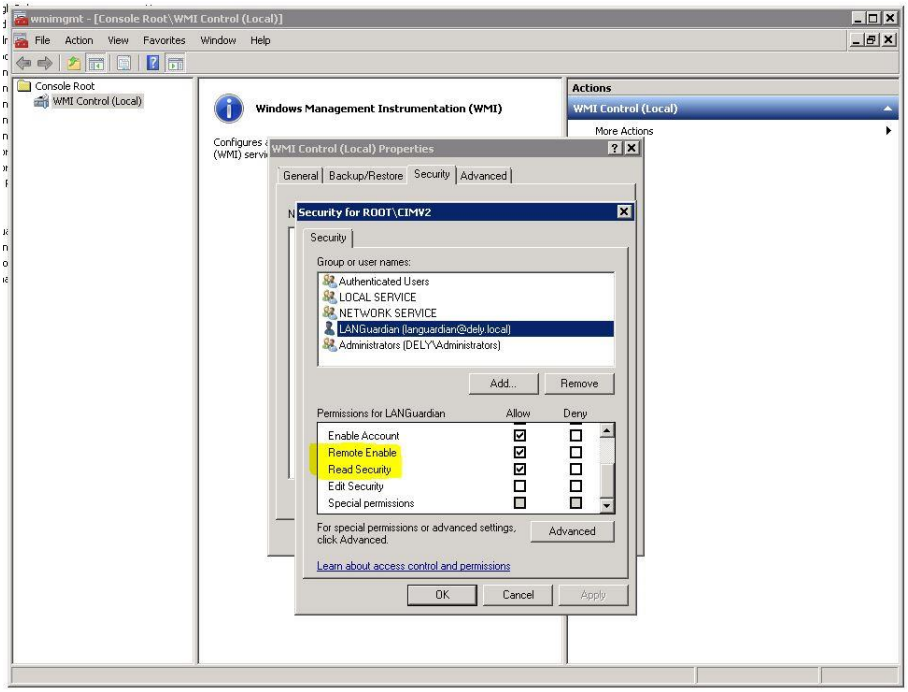
2. Assign WMI permissions

You need to logon to each domain controller and grant specific WMI permissions to the new user.

Click on start\run and type in ***wmimgmt.msc.*** In the WMI Management window, right click on the WMI Control sub menu and select Properties. Under Security Tab select CIMV2 and click on the Security button in the bottom right corner.

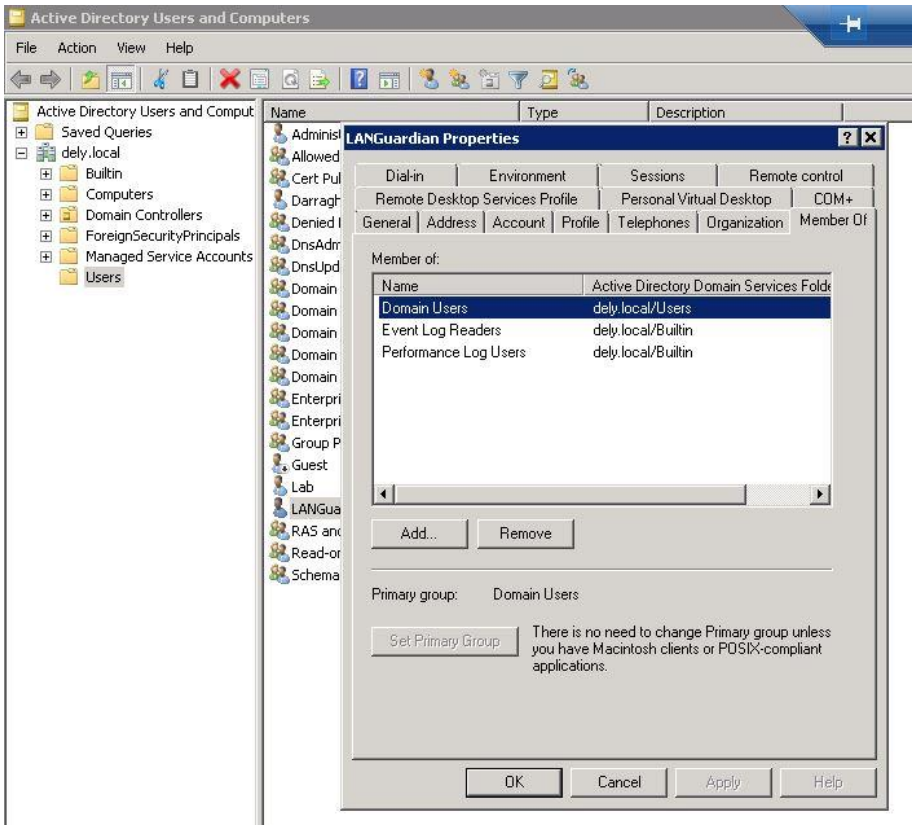


Add the LANGuardian AD account and verify that Enable Account, Remote Enable and Read Security is Allowed, if not, enable those permissions and apply your settings.



3. Add user to *Performance Log Users* and *Event Log Readers* groups

Use the *Active Directory Users and Computers* application to add the LANGuardian AD account to the groups: Performance Log Users and Event Log Readers.



4. Check configuration and permission using the *wbemtest* application

Test the WMI configuration and permissions using the native Windows tool WBEMTEST from your desktop

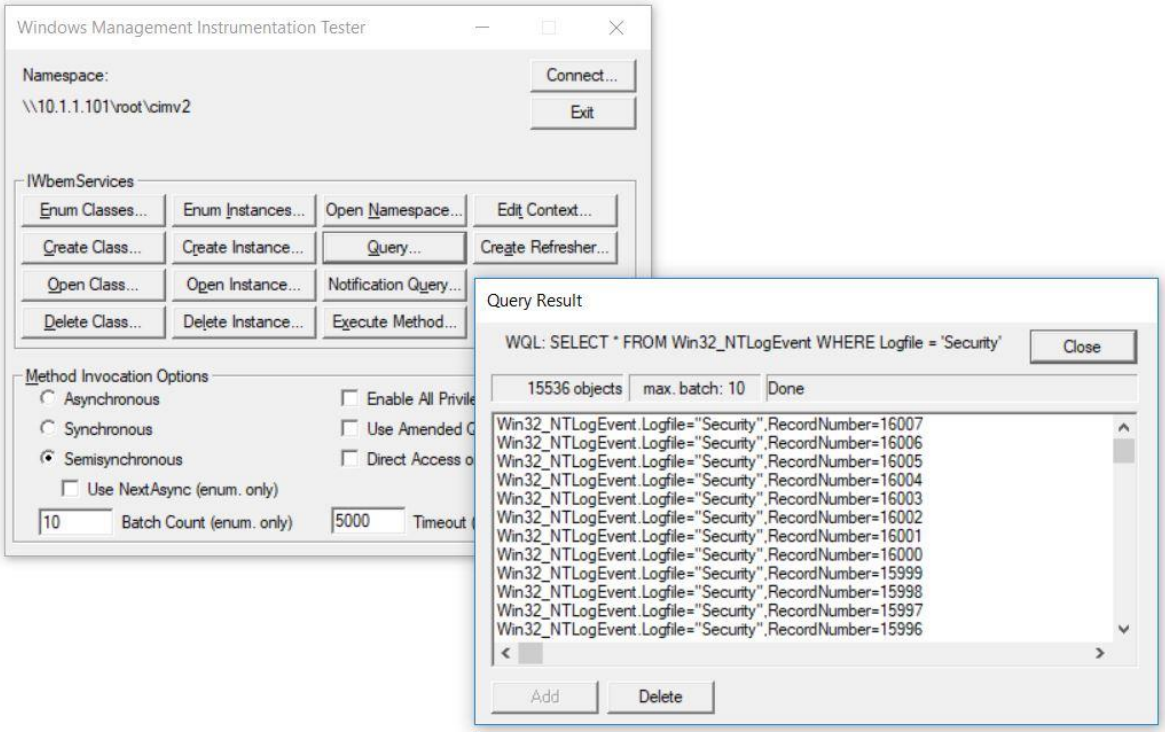
1. Click on run and type in wbemtest on a Windows 7 or 10 system
2. Click on connect and type in \\x.x.x.x\root\cimv2 into the namespace field where x.x.x.x is the IP address of a domain controller
3. Use the LANGuardian AD account with password and click on connect
4. If the account has permissions to connect via WMI you should not see any error messages

If the steps above fail add the LANGuardian user account to the domain group *Performance Log Users* and try running the test again. If this fails then try the test using the Administrator account to see if the server is blocking all remote WMI connections.

Optionally click on Query and type in:

SELECT * FROM Win32_NTLogEvent WHERE Logfile = 'Security' AND EventCode = '4624'

This command verifies that the account can run a query and see the user logon events. If you do not get any data back from the query you may not be auditing user logon events or the LANGuardian AD account is not in the *Event Log Readers* group.



5. Configure AD integration on LANGuardian

Logon to the LANGuardian GUI and click on the gear symbol top left then settings \ Identity \ Active Directory. Click on add domain and enter the IP address of one domain controller together with the LANGuardian AD account.

View our video guide: How to setup Active Directory integration using WMI

https://www.netfort.com/blog/integrating-languardian-with-active-directory-using-wmi/ -wplu5b8e9adac5cbf