

Re: XP SP2 and ports required to view a remote event log

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.setup_deployment/2004-12/0113.html

From: Torgeir Bakken \ (MVP) (Torgeir.Bakken-spam_at_hydro.com)

Date: 12/02/04

Date: Thu, 02 Dec 2004 01:14:06 +0100

FastEddie wrote:

> *I need to know what ports are required to be opened on a XP SP2
> computer to remotely view its event log.*

Hi

E.g. WMI (or more correctly RPC/DCOM) uses TCP ports 135 and 445 as well as dynamically-assigned ports above 1024.

So for Windows XP SP2 with an enabled firewall, to handle this, you need to enable "Allow remote administration exception" for the firewall.

This can be done with gpedit.msc for a local computer, or push it out with a AD GPO if possible. You can also use the command line tool netsh.exe to do this, see further down for how.

From PolicySettings.xls available here:

Group Policy Settings Reference for Windows XP Professional Service Pack 2

<http://www.microsoft.com/downloads/details.aspx?familyid=ef3a35c0-19b9-4acc-b5be-9b7dab13108e&displaylang>

<quote>

Administrative Templates\Network\Network Connections\Windows Firewall
\<some> Profile

Windows Firewall: Allow remote administration exception

Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). This policy setting also allows SVCHOST.EXE and LSASS.EXE to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned

ports, typically in the range of 1024 to 1034. If you enable this policy setting, Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. You must specify the IP addresses or subnets from which these incoming messages are allowed. If you disable or do not configure this policy setting, Windows Firewall does not open TCP port 135 or 445. Also, Windows Firewall prevents SVCHOST.EXE and LSASS.EXE from receiving unsolicited incoming messages, and prevents hosted services from opening additional dynamically–assigned ports. Because disabling this policy setting does not block TCP port 445, it does not conflict with the Windows Firewall: Allow file and printer sharing exception policy setting. Note: Malicious users often attempt to attack networks and computers using RPC and DCOM. We recommend that you contact the manufacturers of your critical programs to determine if they are hosted by SVCHOST.exe or LSASS.exe or if they require RPC and DCOM communication. If they do not, then do not enable this policy setting. Note: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (the message sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow file and printer sharing exception, Windows Firewall: Allow remote administration exception, and Windows Firewall: Define port exceptions.

</quote>

Using netsh.exe, you can configure this from command line as well, like this:

```
netsh.exe firewall set service type=remoteadmin mode=enable scope=subnet profile=domain
```

If not a domain computer, you need to change to 'profile=standard' (or 'profile=all'). Scope can also be set to 'custom' and then you can add ip ranges to the command line as well.

The netsh.exe syntax is documented in WF_XPSP2.doc.

WF_XPSP2.doc "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" is downloadable from

<http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1>

--

torgeir, Microsoft MVP Scripting and WMI, Porsgrunn Norway
Administration scripting examples and an ONLINE version of
the 1328 page Scripting Guide:
<http://www.microsoft.com/technet/scriptcenter/default.aspx>