Using OptiView Console

Introduction

The OptiView™ Console application (also referred to as "the application") provides you with the ability to monitor the performance of your Ethernet enterprise network, generate reports, map your network configuration, and notify you of problems with your network devices. With the integration of OptiView Console software agents and Fluke Networks OptiView hardware agents, you can quickly and easily get detailed information about your complete enterprise network from your desktop.

The application is a Microsoft Windows based software tool that provides Network Supervision™ capabilities for network engineers, LAN administrators, and network technicians who maintain local area networks. By deploying software agents or Fluke Networks OptiView™ analyzers serving as hardware agents on the broadcast domains of your network, the application allows you to monitor your complete network, generate network configuration maps and performance reports, and troubleshoot LAN segments that may consist of servers, routers, switches, printers, managed hubs, and clients (hosts and other network devices). You can also use the application to monitor and control Fluke Networks diagnostic tools (such as an OptiView™ analyzer or OneTouch™ Series II network assistant) that may be located on your network.

The application uses a Viewer/Agent configuration:

- The **Viewer** is the main user interface of the application and provides access to the data collected by the agents on the network. Only one viewer is necessary to monitor the performance of your enterprise network, however, multiple viewers can be installed (with the purchase of additional software licenses) so other network professionals can monitor the network.

- The **Service Manager** allows you to configure and start the four services (Agent, Analysis, Import, and Notification) that comprise the OptiView Console application. All data is stored in an MSDE database and the Viewer is used to show the results.

  – The **Agent Service** is used to discover information about the network. Information discovered by the Agent is stored in a Microsoft SQL Server Desktop Engine (MSDE) database.

  – The **Analysis Service** runs algorithms on the information stored in each database and determines network configuration, error conditions, and other network information.

- The **Import Service** stores information discovered by hardware agents in a separate MSDE database for each agent.
- The **Notification Service** flags error or performance conditions discovered on your network and can be configured to generate email, email to pager, and SNMP traps to alert network administrators.

PC requirements

Processor speed and memory

The minimum requirement to run the application is a Windows based PC with a 400 MHz Pentium processor and 384 Mbytes of system memory. However, you may find this minimum requirement does not give satisfactory performance for medium-to-large networks that have many trended interfaces. A PC with a 2 GHz Pentium processor and 1 Gbyte of system memory running the master viewer and agent will perform satisfactorily for most medium-to-large networks. It is also recommended that the PC is dedicated to the task, i.e. not running other applications. Remote viewers running on a desktop PC can be used in a server/client scenario to allow multiple users to monitor network performance.

Disk space

The minimum requirement is 500 Mbytes of disk space. Factors that affect the amount of disk space required for a particular installation include network size (number of hosts and especially number of switches), the number of trended interfaces, the frequency of archives, and the number of agents that are archived.

All information for the application is stored in Microsoft SQL Server Desktop Engine (MSDE) databases. There is a separate database for each agent (software or hardware) as well as a master agent database (OVCMaster) containing information about discovered agents and notification information. Each agent database contains discovery and analysis data and notification setup information.

The size of each agent database is dependent on the number of discovered hosts in the broadcast domain, the number of interfaces on each host, and the number of trended interfaces. A software agent database can exceed 100 Mbytes if the number of trended interfaces is large. Hardware agent databases will be smaller (approx. 30 Mbytes) because of fewer trended interfaces. The master agent database will be significantly smaller than agent databases, typically less than 5 Mbytes. Software agent databases are always stored on the PC that is running the agent (remote agent databases are stored on the remote PC), whereas hardware agent databases are stored on the PC that is running the master agent.

Archived databases typically have a 5:1 reduction in size, so an archived database that was 100 Mbytes will use about 20 Mbytes of disk space. Archived databases are always stored on the PC that is running the master agent. The accumulation of archived databases can consume a significant amount of disk space depending on the number of agents being used and how frequently archives are scheduled. You can move archived databases to another machine for backup, but they must be restored to the \Program Files\Fluke Networks\OptiView\Console \Database\Archive directory in order to access them from the master viewer.

Here are some examples of disk space usage:

Note: *While the estimates used here are generous, the amount of disk space needed for any given network may be quite different.*

Typical configuration: 3 SW Agents trending 100 interfaces each + 1 HW Agent, 1000 hosts total	
Average weekly viewer database size	5 MB
Average weekly database size per SW agent	30 MB
Average weekly database size per HW agent	30 MB
Average current database disk usage	(30 * 3 + 30 + 5) = 125 MB
Size of each archive set	125 MB / 5 = 25 MB
Disk usage after one year	125 MB + (25 MB * 52) = **1.43 GB**

Large configuration: 10 SW Agents trending 500 interfaces each + 5 HW Agents, 10K hosts total	
Average weekly viewer database size	5 MB
Average weekly database size per SW agent	100 MB
Average weekly database size per HW agent	30 MB
Average current database disk usage	(100 * 10 + 30 * 5 + 5) = 1.16 GB
Size of each archive set	1.16 GB / 5 = 231 MB
Disk usage after one year	1.16 GB + (231 MB * 52) = **13.2 GB**

Unzipping archived databases will increase the amount of disk space required. You can remove unzipped archived databases by deleting the data sources beginning with “A_” in the **Manage Data Sources** dialog. Access the dialog box by selecting the **Manage** button on the **Database/Address** tab of the Service Manager.

Network bandwidth

The OptiView Console application uses a minimum amount of network bandwidth, even on medium-to-large networks. There are several factors that affect network utilization:

Note: *A 100MHz network is the basis for estimates given below.*

- **Network discovery** – Immediately upon starting the Agent Service, network discovery begins. Broadcast pings are sent to the local broadcast domain and depending on the number of hosts that respond, there will typically be a small spike (up to 1%) in network utilization for a medium-sized (200–1000 nodes) broadcast domain. After the ping broadcast, a series of directed queries are sent to individual hosts to gain more information about each host and other devices about which the host may have information. For more information about how the application's network discovery works, refer to the application's online help topic, *The Agent's Device Discovery and Problem Reporting Processes*. After the initial discovery has completed, the cycle is repeated every 1.5 hours (default). The user can increase the rediscovery interval up to a maximum of 24 hours.

In some circumstances, network discovery may cause a high utilization rate for a switch or frame loss on specific devices. The high utilization effect has been observed with extremely large switches that respond rapidly to SNMP queries. If either of these situations occurs on your network, you can clear the **Maximum Discovery Speed** checkbox on the **Advanced** tab of the Service Manager. This will slow down the rate of discovery, but will have no effect on the information that is discovered.

- **Key device and utilization source polling** – Approximately every 40 seconds a Ping is sent to each identified key device to verify its status. Approximately every 2 minutes, each utilization source is sent an SNMP query to verify its status. Because these are sequential events, they have minimal impact on network utilization.
- **Remote software agents** – When the Viewer requests data from a remote software agent, you may see up to a 2% spike in network utilization for a medium to large network. Again, this is dependent on the size of the remote broadcast domain and particularly, the number of trended interfaces. The number of remote agents has minimal impact on network utilization because agent data is sequentially refreshed in the viewer.
- **Hardware agents** – Hardware agents have less impact on network utilization than software agents because they support fewer trended interfaces.

Agents

The application uses agents to discover information about the network. Each agent will discover information about the broadcast domain in which it resides. (A broadcast domain is defined as a LAN with a common address space, which is demarcated from other broadcast domains by routers.) By deploying an agent in each broadcast domain of your network, you can get a complete view of your enterprise network. You can use the application's Viewer to identify all of the agents on your network and to select each agent and view the collected data, generate maps and reports, set up notification events, view trending data, view the problem log, and look at individual device details. The application supports two kinds of agents:

- **Software agents** are included with the application. A master agent is installed with the application but additional remote agents can be installed on PCs located in each broadcast domain. Each remote agent is then directed to the master agent.
- **Hardware agents** are Fluke Networks analyzers used as discovery agents. The application can import and analyze data collected by a hardware agent and present it in the Viewer just like it can from its software agents. The application automatically discovers hardware agents in the same local broadcast domain as the master agent up to 10 hops away as specified by the user.

There are some differences between the operation of hardware and software agents:

- Hardware Agents report a different set of errors to the problem log.
- Because the OptiView Console application is only *reporting* the errors discovered by a hardware agent, hardware agent errors cannot be deleted from the Problem Log.
- Key devices in OptiView Workgroup Analyzers and OptiView Integrated Network Analyzers are user specified, while they are defined by device type in software agents. You can define key devices on the analyzer and they will be reported on the **Key Devices** tab of the viewer.
- Hardware agents can trend a single device (with up to 32 interfaces) at a time.
- Software agents can trend up to a maximum of 500 interfaces (250 recommended).

Remote agents

You can use the OptiView Console application to discover and monitor your complete enterprise network by installing the viewer and master agent in one broadcast domain and then deploying a remote agent (hardware or software) in every other broadcast domain on the network.

Software agents

Using a remote software agent involves installing it on a PC that is located on a remote broadcast domain and "pointing" the agent at the PC that is running the master agent.

Installing a remote software agent is very similar to installing the complete application (viewer and master agent); you just select **Agent Only** during the installation process. The first time you run the remote agent, you will be prompted to enter the IP address of the PC that is running the master agent. On each PC running a remote agent, there must be an account (with administrator privileges) that has the same user name and password as the logon account of the PC that is running the master agent. The account on the remote PC only has to exist, it does not have to be the logon account for the remote PC.

Hardware agents

Certain Fluke Networks tools (e.g. the OptiView™ Integrated Network Analyzer or the OptiView™ Workgroup Analyzer) can be used as hardware agents. The application will automatically find hardware agents on your network and present them in the **Overview** tab of the Viewer. If the password feature is being utilized on a hardware agent, then the password must be entered in the **Security** tab of the Service Manager of the application.

By default, the application will find Fluke Networks tools that are within one hop (router) of the PC that is running the application. You can increase the number of hops that the application will use on the **Advanced** tab of the Service Manager. In addition, you can "point" any OptiView analyzer at the OptiView Console application by entering the IP address of the computer that is running the application in the **OptiView Console** field of the analyzer's **Security** tab.

How to access remote software agents

1. On the PC that is running the master viewer and agent, select the **Startup...** button on the **Service** tab of the Service Manager.

2. If you want the agent and other services to start automatically each time Windows is started, then select the **Automatic** radio button. Otherwise, select the **Manual** radio button.

3. In the **Log On As:** area, select the **This Account:** radio button. Enter an account name that matches a valid account on the PC that is running the remote agent. There must be an account on the remote PC that is the same as the log on account for the master viewer and agent. There are two requirements for both accounts:

   – Both accounts must have administrator privileges.

   – Both accounts must have the same password.

Notes

- *The PC running the remote agent does not have to be logged on with the same account name/password as the master PC; the account just has to exist on the remote PC.*

- *You can use the User Accounts selection in Windows Control Panel to create user accounts.*

- *For clarity in this discussion, the PC that is running the master viewer/agent is referred to as the master PC. Other PCs are referred to as a remote PC.*

User names and passwords

There are several issues regarding access to remote software agents and the use of remote viewers. If you are not using remote software agents or remote viewers, then it does not matter what user name/password the application is running under (the user name must have administrator privileges). However, there are a number of scenarios where it is critical that the appropriate user name/password is used on the PC that is running the master viewer/agent and on PCs that are running a remote viewer or a remote software agent.

Note: *This discussion pertains to remote software agents only. If the password is set for a hardware agent, that password must be entered on the Security tab of the Service Manager. Nothing else is necessary for the application to access hardware agents.*

There are two user names/passwords of concern to the user of the OptiView Console application:

- The master PC logon account – this is the account with which the user logs on.

- The account that is used by the services – this is the account set in the **Service** dialog box of the Service Manager.

Note: *To set the user name/password for the services, select the* ***Startup...*** *button on the* ***Service Tab*** *of the Service Manager. Select* ***This Account:*** *in the* ***Log On As:*** *area and enter the user name and password.*

In order to use remote agents, the services on the master PC must be logged on to a user account, not the default system account. Use the **Startup…** button to set the user account. For many users, the services will be set to the same account as the logon account of the PC. However, for a system with multiple network administrators, it is reasonable to expect that there may be multiple user names for the master PC logon account with a single Services account. ***Note:*** *The Agent service on the remote PC can use the default* ***System Account****. It is not necessary to set a User Account.*

In summary, any accounts used on the master PC that need access to a remote PC must exist on the remote PC. Also, any account used by a remote viewer PC must exist on the PC at which the remote viewer is pointed. Passwords must match and all accounts must have administrator privileges.

The examples given below address various situations:

Example – master viewer/agent and one or more remote agents (single user)

The user logged on to the master PC with user name *OVCUser* and password *OVCTest*. The user name must have administrator privileges. The services are also using the same user name/password.

The remote PC must have an account *OVCUser* with password *OVCTest*. The account must have administrator privileges. The remote PC can be logged on as a different user, as long as the *OVCTest* account exists on the remote PC.

Example – master viewer/agent and one or more remote agents (multiple users)

There are four user names:

- *OVCUser1* with password *OVCTest1*
- *OVCUser2* with password *OVCTest2*
- *OVCUser3* with password *OVCTest3*
- The services account is *OVCServices* with password *Services*

All accounts must have administrator privileges.

In order for all three users to view the results of the remote software agent and for the master services, the remote PC must have all four accounts with matching passwords and administrator privileges. The remote PC can be logged on as a different user, as long as the accounts exist on the remote PC.

Domain authentication

If the user accounts authenticate to domains, the rules are a little more complex, but still straightforward. There must be an account on the remote PC that has the same domain/account name and password as the login accounts and/or service accounts on the master PC. For example, the user logged on to the master PC has user name *OVCUser*. This account is logged into domain *DomainA*. In order to access the database on the remote PC, there must be an account on the remote PC for user name *DomainA\OVCUser*. Again, the user name *DomainA\OVCUser* must have the same password and administrator privileges.

Remote viewer

With the purchase of a license, you can install an additional viewer on a remote PC and direct the viewer to read the master database. You can then perform all the same functions on the remote viewer as the master viewer with the exception that you cannot restore and view archived databases.

The first time that you run the remote viewer, you will have to enter the IP address or computer name of the PC that is running the agent whose database you want to see. You can direct the viewer to look at different agent databases by selecting **Set Master Database...** from the **File** menu of the viewer Menu Bar and entering a new IP address or computer name.

In order to use a remote viewer, an account with the same user name and password as the logon account of the remote viewer PC must exist on the master PC. The account must have administrator privileges. The master PC can be logged on as a different user, as long as the account exists on the master PC.

Example – remote viewer

A remote viewer is installed and directed to a PC running the master agent/viewer. The remote PC is logged on as *RemoteUser* with a password of *Viewer*.

The master PC must have an account *RemoteUser* with password *Viewer*. The account must have administrator privileges. A different user name can be used to log on to the master PC, as long as the *RemoteUser* account exists on the master PC. The services account user name/password on the master PC does not affect the remote viewer.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 6/2003 2097355 D-ENG-N Rev A