Global Information Assurance Certification Paper

Centralized Monitoring of Distributed Systems

Edward Finneran

A GIAC GCUX practical

giac certification version 1.9
(administrivia version 2.5b)

Formatting of this document is deliberately bland in a uniform Arial 12 point font, to comply with GIAC requirements. Screenshots of proprietary products have been not been used, to avoid copyright questions.

Abstract/Summary

This practical will address a mechanism to provide centralized monitoring of distributed systems. In particular, it will describe how the Hewlett Packard (HP) product known as VantagePoint Operations or Openview Operations, using agents running on the distributed systems to be monitored, can report events that you define to be of interest to a centralized monitoring facility.

The product provides certain out-of-the-box monitoring across various UNIX, Linux, and Windows OSes, with extensions available for MVS and others. However, the true power of the product is that it allows each site to customize its definitions of events that are of interest, and what actions the product will take in response to them. Since the uses of the product are so varied and unique to each site, this document attempts to strike a balance between describing the overall capabilities of VPO/OVO and in-depth examples of how they could be used for specific purposes such as monitoring of syslog and sulog.

This document will describe:

- what functionality is available with VPO/OVO and why it might be useful for security and operational monitoring
- specific steps to get the VPO/OVO environment installed
- some detailed examples of how that functionality can be used for selected security and operational monitoring functions including installation and configuration
- some other potential uses of the product that readers could examine to see if they could be helpful at their sites (e.g. monitoring of hardware consoles through terminal servers, in combination with VPO/OVO), in less detail
- specific considerations when systems to be monitored are on the other side of firewalls from the management server

What this document won't describe:

- The online documentation for VPO/OVO, which is available on the Hewlett-Packard http://docs.hp.com website, runs to around 3,700 pages (!), plus another 2,800+ pages for the underlying Openview Network Node Manager software. While this document will describe one specific example of an installation configured to do some specific monitoring, obviously it is not a replacement for a manual set exceeding 6,500 pages. It would be ill-advised for anyone to attempt to use solely this document to install the product and configure it.
- Every possible type of security test for which this product could be used. Many examples will be provided, but you'll need to decide what types of security checks are appropriate for your site. A practical can only scratch the surface of what is possible with the product, but it can give you a sense of what is possible and how difficult it might be.

1. VPO/OVO overall functionality

1.1 VPO/OVO architectural description

VPO/OVO is an HP product, with licenses both for centralized management servers and tiered pricing for the agents that run on the systems to be managed. The cost may make this most appropriate for a medium-sized enterprise and up, and less likely to be the best solution for small companies with few servers, unless they have very stringent requirements for monitoring and security. The purchase of agent licenses in tiers makes it easy to redeploy an agent from one machine to another in the same tier.

VPO/OVO is architected with one or more centralized management servers, plus agents that run on the systems to be monitored (managed nodes). VPO/OVO is a member of the HP Openview family, which is an umbrella of products that are used for various purposes. VPO/OVO specifically includes the Network Node Manager product that performs network management, which most people mean when they refer to Openview.

VPO/OVO can retrieve information from several sources:

- logfile encapsulation, where the manager defines patterns for the agent to look for in logfiles on the managed node
- monitors, where the agent will run a script or process periodically, and examine a numerical result against predefined threshold values
- information sent by scripts or applications explicitly to VPO/OVO (opcmsg)
- SNMP traps where unsolicited inbound SNMP traps deliver information
- SNMP thresholds where mib values are polled periodically
- on HP's legacy MPE/ix operating system, a console interceptor that tracks messages to the MPE/iX console facility

Once an event occurs that you've defined in VPO/OVO to be of interest, a message is generated by whichever local agent detected it. It then forwards it to a management server, where it is stored in a database and displayed to any users of the product who are configured to see that category of messages (i.e. Security versus OS versus Job, etc.) for that machine. A message stays visible in the message browser until it is acknowledged by an operator, when it is sent to a history category.

The full multi-volume manual set for VPO/OVO, which is extensive, is available online from Hewlett-Packard at http::://www.docs.hp.com under the Network and Systems Management category. [1] Clearly someone considering the product would need to familiarize themselves with it before attempting an implementation.

[1] Hewlett-Packard website http://www.docs.hp.com

1.2. How VPO/OVO can help with security monitoring

VPO/OVO provides a significant advantage from a security perspective not only by being able to monitor a variety of security-related aspects of system functions, but also by transmitting that information quickly off of the machine to a management server. This makes it more difficult for an intruder to cover their tracks, even if they remove information from the log files on a machine under attack. The information has potentially already been sent by the agent to the management server, and already been flagged for an operator or security team member's attention.

The mechanism that the VPO/OVO agent uses to transmit this information to the management server is also not a generic syslog protocol. Individuals launching attacks against UNIX host tend to be familiar with syslog, and attempt to circumvent information it logs. Once on the management server, VPO/OVO stores its messages in an Oracle database, not flat files. This means an attacker would need to compromise the management server as well as the managed node, plus possess a second skill set to compromise the VPO/OVO information.

A configuration using a management server located on a corporate network inside a well-configured firewall can also receive and alert on information from more vulnerable machines on a DMZ – providing the alerting function in a more secure location where it would be much more difficult for an attacker to reach.

The view that VPO/OVO can provide by integrating information of different flavors (logfiles, monitors, SNMP, etc.), from multiple sources (VPO agents, application information from opcmsg, SNMP traps from any SNMP-enabled device) can alert staff to a pattern of activity that might not be easily detectable through other means. For example, odd alerts from a particular managed node, combined with syslog or SNMP information from network-based devices about suspicious network traffic can quickly show a pattern that indicates an attack is in progress.

At the release of OVO version 7, the list of operating systems, which can be managed by OVO, is:
AIX 4.3.1, 4.3.2, and 5.1.
HP-UX 10.20, 11.00, and 11.11 (11i)
IRIX 6.2, 6.4, and 6.5
RedHat Linux 6.2, 7.0, and 7.1
SuSE Linux 6.2, 6.3, 6.4, 7.0, 7.1, and 7.2
MPE/iX 6.0, 6.5, and 7.0 (with an HP-UX-based management server only)
Netware 4.1, 4.11, 4.11 SFT III, 5.0, 5.1
ptx 4.4.10, 4.5.3
SINIX Reliant SNI RM200, RM300, RM400, RM600

Solaris 2.6, 7, 8 (Solaris 9 was added as a certified managed node after the release of OVO 7)
Tru64 4.0F, 4.0G, 5.0A, 5.1
Windows NT 4.0 SP4, Sp5 or SP6a (nt server, workstation, and enterprise edition)
Windows 2000 5.0, SP1 or SP2 (professional, server, advanced server, data center families)[2]

Additional platforms can be added by HP via patches in between major releases of VPO/OVO, so you should check with HP for the latest list.

1.3 HP VPO/OVO licensing

Although license loading is not performed until later in the procedure, redeeming them ahead of time ensures that you won't encounter any problems when you're in the middle of the installation.

HP licensing is provided by the web site http://www.webware.hp.com. You will need the HP sales order number for the purchase that was made that included the VPO/OVO licenses, and may include other HP items on the same order. When a license is purchased, part of the documentation that arrives with the license is paperwork that provides the sales order number and directs you to the website to activate it.[3]

You provide the sales order number, and the web site will list the available VPO/OVO licenses that have not yet been redeemed and their quantity. By clicking on a license and proceeding to redeem it, the web site will provide you with a 24-character license code that you can later load into the VPO/OVO product. You'll need to provide the hostname of the management server, the operating system it runs (HP-UX or Solaris, including the version) and the IP address to tie the license to. This is the address of the management server you will load the license on, so it's important to think through your IP addressing ahead of time. It will be displayed on the web page, which you can save via your browser, and also emailed to you. It is important to save this information permanently in case you ever need to reload it from scratch for some reason.[4]

The management server does the validation of licenses for all machines in its domain – so if you buy 100 managed nodes licenses, you can redeem all of them for a single IP address for a single management server, and it takes care of ensuring that only the appropriate number of managed nodes are installed. This allows you the flexibility to push an agent out from that management server in the

[2] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, pages 51-52.
[3] Hewlett-Packard website http://www.webware.hp.com
[4] Hewlett-Packard website http://www.webware.hp.com

morning to one managed node for testing, and then in the afternoon deinstall it from that node and push it out to a different node instead. HP supports the use of Serviceguard (HP-UX) and Sun Cluster (Solaris) to provide failover for the management server, which would involve a traditional clustered mobile IP address that would shift between multiple servers – if using one of these techniques you want to make sure you redeem the licenses for that IP address, and not the stationary IP address of one of the hosts. Later you would configure VPO/OVO to use that IP address as the one it will communicate on.[5]

You'll need the license for the management server, plus a valid license of the appropriate tier (zero through four) for however many other systems you want to manage. Systems capable of running multiple OS images at the same time, such as HP Superdome, IBM Regatta, or Sun F12Ks, etc. are slightly more complicated. They are covered by a single VPO/OVO license from a purchase standpoint. When that license is redeemed, a license for a single OS image would be created, but customers then need to send a licensing request form to the HP licensing authority to request additional license keys based on how many additional OS images there are running on the licensed hardware.[6]

[5] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Appendix A

[6] HP Openview Tiering Matrix, page 1, reference 5 in that document

2.0 Installing the VPO/OVO product set

2.1 Installing the management server

The first step in setting up a VPO/OVO monitoring environment is to install the software on the management server. Then a typical installation would use the management server to 'push' the installation of agent software onto the managed nodes.

Currently, HP supports the management server function on HP-UX and Solaris. If an HP MPE/iX legacy node is involved, HP requires the management server to run on HP-UX.

2.1.1 Oracle

VPO/OVO requires Oracle as its database to hold messages and various configuration information. An existing Oracle database can be used, either local to the management server, or on a remote host. If an existing Oracle installation is not available, a specific license for "HP Oracle for Openview" can be purchased from HP that will fulfill the requirements of VPO/OVO. Access to this database is centralized to the management server for all functions, and is not directly accessed by the agents. The process to enable an existing Oracle database instance for use by VPO is expanded below.

2.1.1.1 Configuring an existing Oracle instance for use by VPO/OVO

As released VPO/OVO version 7 requires Oracle 8.1.7.0 (32 bit). (HP may introduce support for later versions of Oracle via patches. http://www.itrc.hp.com and http://www.openview.hp.com are excellent places to check for the latest VPO/OVO patches)
Ensure that the Oracle installation that you plan to use is set to be compatible with version 8.1.7 by adding a line

compatible = 8.1.7.0.0

to the configuration file for this Oracle instance, namely

$ORACLE_HOME/dbs/init<instance>.ora

and stop and restart the Oracle instance if this line was not already present.[7]

(Once installed, when VPO/OVO processes that need connection to the Oracle database start, they will examine the environment they are starting in to determine if ORACLE_HOME, ORACLE_SID, NLS_LANG are set, in which case they are used, otherwise the processes will examine the file /etc/opt/OV/share/conf/ovdbconf which is specific to VPO/OVO to determine the

[7] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, pages 50 and 59

value to use.)[8] For the purposes of this installation, if you don't normally set ORACLE_HOME, ORACLE_BASE, ORACLE_TERM for the root user, set them now in the context of the process you will be using to perform the installation to whatever you currently set them to in the context of the Oracle user that runs the instance. set NLS_LANG, ORA_NLS33, and add the Oracle binary directory to the path of your current process, if not already included:
export NLS_LANG=american_america.WE8ISO8859P15
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
export PATH=$PATH:/$ORACLE_HOME/bin
if SHLIB_PATH is unset, set it to $ORACLE_HOME/lib – if it is set, add $ORACLE_HOME/lib to it.
export SHLIB_PATH=$SHLIB_PATH:$ORACLE_HOME/lib [9]

2.1.1 VPO/OVO

2.1.2 Installing the management server binaries

A slightly different procedure applies to an HP-UX versus Solaris management server installation, so there are separate manuals for each OS. The Solaris installation, for example, would install an HP lightweight DCE facility if no dce installation exists (Solaris does not provide one by default). HP-UX has one built in so it is not required.[10] This will describe using an HP-UX machine as the management server.

2.1.2.1 prerequisites

The prerequisite software that must exist on the HP-UX machine that will become the management service includes the following filesets:

- DCE-Core.DCE-CORE-RUN, version 1.7 or higher (installed as part of HP-UX)
- DCE-KT-Tools (hp-ux 11.0 only. Could be installed from HP-UX Application CD-ROMS, or from the VPO/OVO CD-ROM, where it should be selected automatically as a dependency when the VPO/OVO management server is installed).
- InternetSrvcs.INETSVCS-RUN (part of HP-UX Core OS)
- X11.X11R6-SHLIBS (part of HP-UX Core OS)
- X11 (part of HP-UX Core OS)
- CDE.CDE-DTTERM, CDE.CDE-HELP-RUN, CDE.CDE-RUN (part of HP-UX Core OS)

[8] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, page 119
[9] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, which pertains to OVO version 7], page 62
[10] HP Openview VantagePoint Operations for Sun Solaris Installation Guide for the Management Server

- OVSNMPAgent.MASTER, OVSNMPAgent.SUBAGT-HPUNIX, OVSNMPAgent.SNMP-ENG-A-MAN (available on the same VPO/OVO CD-ROMs)[11]

The installation of the product requires the following amount of available disk space in these new directories that the installation will create for you:
/opt/OV 510MB
/etc/opt/OV 16MB
/var/opt/OV 320MB
which swinstall, the standard HP-UX tool for installing software, will verify for you, and a guideline of 600MB of initial space in the Oracle database that VPO/OVO will use to store its message and configuration data. The total amount of space needed in the database will be directly related to how many systems you plan to place under VPO/OVO monitoring, and how many messages they generate.

The HP Openview VantagePoint Operations for HP-UX Installation Guide for the Management Server shows the pre-requisite patches needed on the management server at the time the guide was written. Check the release notes for the latest information. Up to date information about consolidated patches and point patches is available from http://www.hp.com/go/openview and via the traditional contract-based http://www.itrc.hp.com that people may already be familiar with for other HP support.

2.1.2.2 specific detailed instructions for installing the management server

On HP-UX, the distribution CD would be mounted normally via:
umask 027
mkdir /mymountpoint
mount –r –F cdfs /dev/<special file for your cd drive> /mymountpoint [12]

The actual installation of the VPO/OVO product would be accomplished by using the HP swinstall utility. This is the normal way to install any software on an HP-UX machine. A VPO/OVO installation product that includes the software for all supported OS agent platforms is called ITOEngOraAll. You can launch swinstall in either a character cell terminal or Motif environment and the appropriate interface will load. (A Motif interface will be required later to perform configuration.). The following describes the normal use of swinstall on HP-UX to select and install a product.

Launch swinstall and point it at the CD (you can also simply launch swinstall with no parameters and use the gui to point it at the CD):
swinstall –s /mymountpoint

[11] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, which pertains to OVO version 7], page 45-47
[12] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, page 72

The swinstall interface will launch. It uses a fairly standard menu interface. In the Motif version of the interface, the usual pull-down method is used. In the character-cell interface, if it is an ANSI terminal emulation being used, options are selected by hitting tab to activate the top menu bar, and then using arrow keys to navigate the menus.

By pre-specifying the location of the software depot on the command line, the software will interrogate the depot and show all the different bundles and products that are available from the depot. In this case, it would include VPO/OVO, regular Network Node Manager by itself, documentation sets, etc.

To install the VPO/OVO Management server software, select from the View menu the “change software view item” item and the “start with products” subitem. This will cause the display of software to start with product collections of filesets in the depot. The software that you want to select is named ITOEngOraAll (navigate to the item with arrows and use space bar in character cell, mouse click in Motif).

Select from the Actions menu the “Mark for Install” item. The “Marked for Install” column will turn to Yes for this item.[13]

Begin to install the software by selecting the Install item from the Actions menu. This standard analysis phase of swinstall will examine the software selected and ensure that the prerequisites needed by the installation exist, among other things. When the analysis phase finishes, select Logfile to examine the log of the analysis activity to ensure that it completed without errors. Select OK to proceed to install the software without further interaction. Once the installation phase has finished, it is prudent to again select logfile to examine the portion pertaining to the installation to ensure everything was successful.

Exit swinstall by selecting exit from the File menu.[14]. Unmount the cd via umount /mymountpoint.

2.1.3 specific detailed instructions on configuring VPO/OVO

Now that the software actually resides on the management server, it needs to be configured to run in your environment, and needs information about the Oracle installation that it should use for its data, as follows.

2.1.3.1 core detailed configuration instructions

[13] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, page 73
[14] HP swinstall utility

Ensure that your DISPLAY environment variable is set so properly for a Motif display (i.e. to a UNIX workstation, a Linux PC, a Windows PC with Reflection X software, etc.)
The opcconfig utility is an over-8000 line script provided by HP to perform the task of configuring the VPO/OVO product to operate in the specific environment into which it is being installed. run the opcconfig utility via:
/opt/OV/bin/OpC/install/opcconfig

It will prompt for various pieces of information to perform the configuration operation and then proceed to complete it without further intervention:
- First is whether to have the utility proceed to configure the Oracle database with the appropriate schema for VPO/OVO's use. Enter y to have it perform the configuration.
- It will prompt for the password for the Oracle system user if one exists – otherwise, hit enter to have it create one.
- It will prompt for your choice for the password for the Oracle opc_op user, which is the id that will be used for most VPO/OVO Oracle communication.
- It will prompt for your choice for the password for the Oracle opc_report user, which you can use for read-only reporting against the VPO/OVO data in Oracle.
- It will prompt for whether you wish to integrate startup of the database into the startup sequence for the system; enter y to have it automatically add this startup to the system startup sequence.
    - It will prompt for your choice of directories to hold the data and index directories for the VPO/OVO data. Enter a location that has sufficient space to hold the oracle database data tables and indices. Size will be based on how many nodes you plan to manage and how many messages you expect your systems to generate. See the installation guide for guidelines on space/system and space/message.
    - It will prompt for your choice of the Oracle environment variables ORACLE_BASE, ORACLE_HOME and ORACLE_SID (frequently openview).
    - It will prompt for the UNIX id that runs the Oracle instance.

opcconfig then proceeds to create the schema and load an initial base configuration without further intervention.

Once it has been configured, VPO/OVO is now installed and enabled with a minimal configuration. The last action of the script is to launch the VPO/OVO Motif gui (via the opc command)
In the authentication panel that pops up, the user id for the administrative user is opc_adm, and the initial password is set to OpC_adm. This will launch the VPO/OVO interface, as seen by the administrator, for the first time.
[this entire section derived from [15]].

[15] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8, which pertains to OVO version 7], page 79-81

2.1.3.2 specific instructions on loading licenses

Loading the licenses you retrieve from HP earlier is done via
/opt/OV/bin/OpC/install/opclic –add –force ABCD EFGH IJKL MNOP QRST UVWX “Message that came with the license”
where the 24-character license is what you received from HP in email and via your browser.

Currently loaded licenses can be reported via the
opclic –list
and
opclic –report
commands.

The report option will allow you to verify as you deploy agents that you won’t be running out of licenses, or alert you it’s time to purchase additional licenses if you want to deploy more managed nodes.

2.1.4 Agents

2.1.4.1 Agent architecture

The initial state of VPO/OVO is that the node bank, which contains an icon for each system that will have an agent, either directly, or in groups, will have only the icon for the management server. All other servers that will run a VPO/OVO must be added to the node bank and an agent pushed out to them.

Now that VPO/OVO is running, the agent software on the machine running the management server must also be pushed out. It functions basically the same as all other agents, with only one slight difference to enable reception of SNMP traps for forwarding them into VPO/OVO.

The architecture of an agent includes a “control agent” process, which takes care of the job of starting all the other components of the agent, that need to start. If on the management server, templates have been assigned to this node and distributed to the agent, the control agent will start the necessary components to enable that functionality. For example, if monitoring of any logfile has been assigned to this agent, the control agent will start the opcle logfile encapsulator process. If opcmsg for direct transmission of messages to the management server upon request has been enabled, the control agent will start the opcmsgi message interceptor process.

Agents are started and stopped via the opcagt command (not by running the control agent process directly – opcagt takes care of that for you), using either the –start, -stop or –kill options. –stop will actually leave the control agent running, whereas –kill will stop it as well. Stopping an agent means that a

remote command from the management server can request the control agent to reactivate the rest of the agent process via opcragt (opc remote agent) commands.

Again, the list of OS's that can run an VPO/OVO agent as of the release of version 7 includes: AIX, HP-UX, Irix, Linux (RedHat and SUSE), MPE/iX, Netware, ptx, Sinix reliant, Solaris, Tru64 UNIX, and Windows NT and 2000. [table 1-13] [16]

Agents employ a storage and forward mechanism for their messages so that if an agent is functioning and detects an event, but the management server is not running for some reason, the message will be queued for delivery when the management server restarts, so no data is lost.

2.1.4.2 distributing an agent

The default selection is to modify the startup/shutdown sequences of the node in order to shutdown the agent during the shutdown of the node and to restart it as root during the startup sequence of the node.

2.1.4.2.1 security for the agent

Distributing an agent automatically is done through the administrator's gui, which was started above.

The agent typically runs as root on the managed node so that it can monitor everything that happens on the node. Security to perform the installation of the agent can either be performed by typing in the root password when prompted by the installation dialog, or by enabling .rhosts access to the remote node as root from the root account on the management server.

This is the standard mechanism to accomplish an installation, aside from a manual installation option described in 2.1.4.2.4, which is available for a subset of all the operating systems supported by VPO/OVO. These are the only options available in VPO 6 and earlier. This will be described first, since it is available to all versions, but the ssh-based method that HP introduced in OVO 7 is more secure, and is described subsequently.

There is an Advanced Security optional add-on product for encrypted communication at all times between the agent and management server, which is not a function of the base VPO/OVO product. It would be most appropriate for very high security environments.

2.1.4.2.2 agent installation via traditional method

[16] HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, Edition 8

The default installation process when not configured to use ssh will use remsh/rsh Berkeley services to accomplish the distribution of the agent. It will use either a previously established .rhosts access or if that is not available, then the provided root password to execute remote commands on the managed node to accomplish the installation.

During the traditional process, the agent software is ftp'ed to the managed node as root and unpacked in a temporary directory, so ftp access must be enabled for root. Examine the file of users not allowed to be the recipient of an inbound ftp operation (such as /etc/ftpusers) to ensure that root is not listed. ftp access is only needed during the default agent installation process. If using this mechanism, in order to enable remsh/rsh access, services such as shell login and exec may need to be re-enabled in the inetd.conf of the managed node if the node has been hardened to shut them off. This can be accomplished by uncommenting the shell login and exec entries in /etc/inetd.conf on most UNIXes (even if just a link to another location, as on Solaris), then sending the inetd daemon a HUP signal (assuming the host is running inetd) for it to reexamine its config file, installing the agent, removing the entries and resignalling inetd to remove the services again. If the host has been sufficiently hardened to not run inetd, or it is undesirable to enable services of this type, choosing the ssh installation option is probably a better choice.

One option for increasing security for the agent itself is that once the agent is installed, if the monitoring the agent needs to perform can be accomplished via a less privileged id than root, it can be configured to run under a different login id. The command
opcswitchuser user group
can be used to transfer ownership of all agent-related config files to a different id. The agent would be killed (stopped including the control agent) via /opt/OV/bin/OpC/opcagt –kill prior to doing this, and restarted after via /opt/OV/bin/OpC/opcagt –start afterwards. It is up to the system administrator to ensure that any work the agent is requested to do can be performed by the user the agent is now running under. For example, if the agent is to be used to monitor the syslog, and it is readable by the alternate user or group selected, this will work. Monitoring the sulog logfile, however, for example, is typically only readable by root, so it's permissions would need to be adjusted in order to work successfully with a non-root agent, perhaps by creating a specific group that the agent id would belong to, and setting the group ownership of any file that is to be monitored to that group, with read access enabled.

2.1.4.2.3 installation sequence for the management server's agent

Using the gui started at the end of section 2.1.3.2, select the from the Actions menu the Agents item and the Install SW & Config subitem to open the window to carry out this process. In the list of the nodes to operate on, on the right, type

in the fully qualified name (including domain name) of the node running the management server, and click Add so that it appears in the list of machines to operate on. On the left side, choose Software. Click OK. A window will open in which the installation script runs. The installation will proceed largely unattended other than prompting for the root password if needed (or the password to a different account if the node's properties in the node bank have been modified to install via a different id). At this point, since the first agent we want to install resides on the same machine as the management server, no authentication is required.

2.1.4.2.3 prerequisites for installation using ssh

If you are already running OVO version 7 (most companies are still in the process of upgrading from VPO 6), and the operating systems of the managed nodes you are running are supported by HP for an ssh-based installation, it may be the better choice.

Passwordless access not requiring a passphrase from the root login on the management server to the root login on the managed node needs to be set up in order for this option to work. The node can be updated to set ssh as the installation mechanism by selecting the node in the node bank and selecting Node/Modify, and selecting SSH installation in the window, which appears after clicking on Communications Options. The passwordless root connection via ssh can be disabled if not needed for other purposes after the completion of the installation.[17]

HP provides a free download of a pre-packaged and supported ssh from http://software.hp.com. If you have a support agreement with HP for HP-UX, they will provide free support for ssh. The product as they package it is called HP-UX Secure Shell. Versions are available for both the hp-ux 11.0 and 11.i versions of the operating system. Check whether you have Secure Shell installed by:

swlist –l fileset Secure_Shell

If you have it, it will return information showing the Secure_Shell fileset and its version number. If you do not, it will return any error that the software was not installed on the host.

If you need to install it, determine which version of hp-ux you are running by issuing:
uname –r
so that you can specify the correct version when downloaded it from the HP website. HP-UX 11.0 reports 11.00, while 11i will report 11.11 (on PA-RISC CPUs).

[17] HP OpenView VantagePoint Operations Administrator's Reference Guide, volume I, edition 6, pages 59-61

If you are running 11i, there is an additional facility available from the same site that provides superior random number generation, which can make ssh less susceptible to attacks that use the predictability of previous random number generation. HP Secure Shell will take advantage of the specialized random number generator automatically if it is installed.

To install these products, you can re-use the swinstall instructions provided in section 2.1.2.2, and simply selecting the appropriate software rather then the VPO software specified in that section. No CD mounting would be required, clearly. For this type of depot containing only one product, when you launch swinstall pointed at the depot, you will only have the single software available for selection and subsequent installation.

To launch swinstall and point it at the file you downloaded for either ssh or the random number generator (say, T1471AA_A.03.50.00_HP-UX_B.11.00_32+64.depot for ssh),issue:
swinstall –s /pathwhereyouputthefile/ T1471AA_A.03.50.00_HP-UX_B.11.00_32+64.depot
(the path MUST be fully qualified).

HP's prepackaged ssh implementation is a flavor of OpenSSH, but installs and storages its configuration information under /opt/ssh, for an installation which is more consistent with other HP products. Additionally, command line options can be passed to the sshd process at boot time by adding them into /etc/rc.config.d/sshd by defining them in the SSHD_ARGS environment variable, and restarting sshd via
/sbin/init.d/secsh stop && /sbin/init.d/secsh start

No modification should be needed for VPO/OVO to use it, provided we set up key-based ssh2 style authentication -- .rhosts and .shosts style authentication, and ssh1, are disabled by default with the HP installation.

To enable root-level access without a passphrase from the management server to the managed node using a dsa-style key pair, as root issue:
/opt/ssh/bin/ssh-keygen –t dsa
You will be prompted for the name of the file in which to save the key – the default is a file called id_dsa in a (potentially new) directory called .ssh under the home directory of the root user. The key pair is composed of a file called id_dsa with the private key and id_dsa.pub with the public key. For VPO/OVO purposes, enter no passphrase when prompted.

In the case of managed node also running HP Secure Shell, copy the resulting id_dsa.pub to a (potentially new) .ssh directory on the managed node into a file called authorized_keys2. This is the OpenSSH convention, on which HP Secure

Shell is based. If this file already exists, append the contents of id_dsa.pub to it, to avoid overwriting existing keys.

Test the key-based ssh configuration by attempting to connect as root from the management server to the managed node:
/opt/ssh/bin/ssh <nodename>
It should log you in without prompting for further authentication, based on the exchange of the private key from the management with the public key on the managed node to authenticate you.

Note that in some security environments, leaving a capability to go from one system to another as root without additional challenge would not be a wise idea. You may wish to disable this access by removing the key that you added from the authorized_keys2 file on the managed node after the installation of the agent is complete.

2.1.4.2.4 installing on additional nodes

Add other nodes to be managed to the node bank via the Actions menu, Node item, Add subitem to open the add node window. Provide the fully qualified hostname of the node, the and the operating system on which it runs. Select 'controlled' to configure the node to run a full agent. If ssh installation is desired, click the Communications Options button to open the subwindow, and select the SSH Installation option and click OK in the subwindow. Click OK in the main window. Once added to the node bank, use the process from 2.1.4.2.2 above to install the software for all additional nodes.

If a managed node will be located on the other side of a firewall from the management server, set the communication protocol to DCE TCP instead of DCE UDP in the communication options subwindow, and set Polling Type to RPC Only in the main window. Changing the communication type after the installation of an agent would require a reinstallation of the agent, so it's preferable to do it now.[18]

A full-blown OS installation on the managed nodes is usually not required for a VPO/OVO agent to function correctly. A "minimal" HP-UX installation, and a "core" Solaris installation, as defined by HP and Sun, are sufficient. Check the Administrator's Reference manual for the flavor of operating system on which you wish to install an agent.

2.1.4.2.4 manual installation

[18] HP OpenView Operations for UNIX, Firewall Configuration White Paper

Rather than the automatic installation triggered from the installation gui, if circumstances dictate that even passwordless/passphraseless ssh and remsh/rsh/ftp access are not available or not desirable between the management server and the managed node, a manual agent installation process is available for some OSes (including at least HP-UX, Solaris, Linux and Windows). The compressed tar package of the agent software can be transferred to the node through other means (tape, etc.), and then a manual process followed to install it and activate it. This circumvents the need for extra access between the management server and the managed node in order to perform the agent installation beyond that needed for normal agent operation.

3.0 configuring monitoring

Now that agents are installed on some systems for monitoring, the events that are of interest can be defined

VPO/OVO out of the box comes with several basic 'templates' for each OS. A template is a definition that pertains to a single source of information. It includes the fully qualified path to the logfile that will be watched by this template. If there are multiple logfiles on the agent node that you want to monitor, say the syslogd log, the su log, etc. there would be a separate template for each logfile.

A template can apply to numerous machines, so the definition of what patterns to look for in a particular logfile can be done once, and then assigned to as many machines as desired. Assigning the template to the node, and then notifying the agent will cause the agent to add that template to the list of activities it carries out locally. Only when a pattern match occurs does the agent notify the management server of a message, keeping network traffic to a minimum. It follows the principle of central definitions, distributing analysis and processing, and centralized reporting.

Since different UNIXes store their syslogs in different locations (/var/adm/syslog/syslog.log for HP-UX, /var/adm/syslog for AIX, /var/adm/messages for Solaris, and /var/log/messages for Linux), a different template would be required for each OS.

HP supplies a category of templates for several operating systems of pre-built templates. The template is subject to replacement in future versions of OVO, so the best approach is to take their default as a starting point, and make your own site-specific copy that you can customize with the events that you care about without worrying that they will be overlaid with the next version of the product. If you also save a copy of the current HP-provided one under a unique name (e.g. copy HP UX syslog to HP UX syslog vpo 6), when the product is later upgraded, you can compare the new HP UX syslog to the vpo 6 version to see if any new and interesting conditions have been added by HP that you might want to add to your site-specific version.

Some of the things that HP provides default logfile-based templates for include syslog, su, cron logfile, and bad logins. Some monitors (numerical thresholds) include cpu utilization, swap utilization, mail queue length, and whether certain daemons are running, such as inetd, sendmail and syslogd. These vary slightly across the different supported OSes.

3.1 pattern matching for logfiles

Templates are maintained either by the overall VPO/OVO administrator, or logins within the product can be created to allow individuals to maintain templates only,

and not have access to other functions that only the administrator can perform, like installing agents, determining which templates are assigned to each machine, which operators see which messages, etc. Those functions will be described later.

Through the motif administrator gui, templates can be maintained by the administrator by selecting the templates pulldown from the administrator's interface. For logins created specifically to maintain templates, that view constitutes the entirety of their interface and no selection is required.

A hierarchical display of templates and groups of templates appears in the template window.

3.1.1 sulog monitoring

If we examine the default template for HP-UX as provided by HP, and in particular "Logfile:Su (10.x/11.x HP-UX)[19] and examine the conditions it contains, there are three. By default, all conditions in the template are sent with a message group of "Security", so any VPO/OVO user who is configured to see security messages for the group this managed node resides in will see the message.

3.1.1.1 predefined conditions for sulog

Condition number 1 is an example of a suppress condition, where if that pattern is detected in the sulog it will explicitly be ignored by VPO/OVO. The pattern defined for the agent to search for is "SU <*> + <@.tty> root-Oracle"[20] This would ignore any lines appended to the sulog that result from a successful su from root to oracle, being something that happens normally.

Condition number 2 is a match condition, where once this pattern is detected by the agent, a message will be created in VPO/OVO in response. The pattern listed for this first condition is "SU <*> - <@.tty> <*.from>-<*.to>. The message text that will be displayed to the user is "Bad switch user to <to> by <from>"[21]. The text from the somewhat cryptic line from the su log is parsed, and if it matches the specified pattern, the tty, from and to fields are captured, and inserted into the text shown to the VPO/OVO user. The severity of this message is "warning".

In this case, of a bad su switch from one user to another, the OS will log that fact to the logfile, the VPO/OVO agent will parse the added line, find that it matches this condition, and send the chosen text, which is configured to include elements from the matched pattern, to the VPO/OVO user community via the Security message group (described later).

---

[19] HP VantagePoint Operations software, version 6
[20] HP VantagePoint Operations software, version 6, Logfile Su (10.x/11.x HP-UX).
[21] HP VantagePoint Operations software, version 6, Logfile Su (10.x/11.x HP-UX)

Condition number 3 is a match condition as well, with a search pattern of "SU <*> + <@.tty> <*.from>-<*.to>"[22], indicating a failed su attempt from the user captured in the "from" field to the user id in the "to" field. The severity of this message is unchanged, which defaults to the global setting for the template, which is "normal".

3.1.1.2 customizing sulog messages.

Since GIAC Enterprises has more stringent security requirements than some companies, let's modify the sulog monitoring template to customize it.

Su's that involve the root account as a destination are of more concern than su's in general, so let's add additional conditions for monitoring of these events.

Selecting the "Bad su" condition in the condition window, and selecting Copy…, creates a duplicate of that condition. We can change the name of the condition from "Bad su" to "Bad su to root". Change the section of the pattern match from "<*.from>-<*.to>"[23] to "<*.from>-root". In the message text that will be shown to the operator, change the <to> text where the variable target of the su would have been filled in for the generic case via "Bad switch user to root by <from>". Change the severity from warning to minor.

To add specific instructions to the condition that results from a bad su attempt, click on Instructions. In the instructions window, enter the text that you want presented to operators, so in this case for the root user bad su, "An attempt has been made to su to the root account that was unsuccessful. Please contact the system administrator for this system to determine if this was legitimate." OK the condition to add it to the conditions for the template. It will be added as condition 4 to the template. Select it, and click Up twice to move it to position two.

Since conditions are examined sequentially for any line added to the logfile, by placing the more specific root bad su condition above the generic bad su condition, bad root-targeted su's will first match the root condition and be caught there, whereas all other su's will continue to be examined by the other conditions, and be caught by the generic bad su condition.

Now that the original bad su condition no longer applies to root, we can make the instructions for the condition more specific. A bad su from one user to another might have been caused by a user mistyping a password, so a single event may not be sufficient at your site to warrant any action. Other sites may require a minimum response of a phone call to ask the user if they attempted to su from their account to the other one. Instructions could say "If more than 2 bad su messages for the same account occur within an hour, please initiate contact with that user to determine if they were attempting to use the account. "

[22] HP VantagePoint Operations software, version 6, Logfile Su (10.x/11.x HP-UX)
[23] HP VantagePoint Operations software, version 6, Logfile Su (10.x/11.x HP-UX)

If GIAC Enterprises does not consider successful su's to non-root accounts to be of concern, additional customization could be done along the same lines as above for the bad su. We can clone a "Succeeded su" condition to add a more specific "Succeeded su – root" condition using the same techniques. Once done, and promoted above the default "Succeeded su" condition, we could modify the now-generic "Succeeded su" condition by clicking on the "On Server log only (put directly into history log)" checkbox. This will cause the message to be created and sent to the management server, but VPO/OVO will acknowledge it automatically and not show it to any operators. The value of this is to make the information available in history for further detail – if an operator sees suspicious patterns of a several su's on a machine, by opening the history browser via view/history on the message browser window they can also see the successful non-root generated messages which by themselves may not normally be deemed of interest.

3.1.1.3 other logfiles

Additional logfile templates can be defined for as many logfiles are deemed to have interesting messages in them.

For example, a template could watch /var/log/xferlog for wu-ftp related messages so that wu ftp doesn't have to be configured to send its messages to the system syslog and clutter it up with ftp messages.

3.1.1.4 actions

Each message can also be configured with an automatic, and/or an operator-initiated action. The command to be issued is entered on the condition definition screen. Automated actions are triggered locally as soon as the agent detects the event – it doesn't wait for the event to be transmitted to the management server. An operator-initiated action results when an operator who is authorized to initiate actions clicks on the button in their opc gui.

In this way, VPO/OVO can even be configured to automatically defend a system against the known signature of an attach – a particular message in the syslog, for example could trigger an action to shut down a vulnerable daemon, isolate the machine from the network, or even shut down a vulnerable host in extreme cases.

3.2 SNMP traps

A template can also be defined that is of the 'SNMP trap' variety. This allows the specification of specific SNMP trap values, which when received by the operating system on the management server, will trigger VPO/OVO messages. Since

SNMP isn't usually the first choice for monitoring host computers, I'll describe this in less detail.

SNMP (Simple network management protocol) is available from a great many types of devices. Its origin was for the management of network devices, such as hubs, switches, routers, etc., but has expanded into management of network-attached hosts as well. More complex network devices may provide a syslog-forwarding type of facility, but a great many network devices provide only SNMP-based alerts for events of interest, which makes it a potentially valuable source of information. A "trap" is an unsolicited message sent by the device to a defined snmp trap destination address.

SNMP as a protocol is not particularly secure, so if SNMP traps are to be used, it is imperative that the person responsible for VPO/OVO, and in particular the Network Node Manager subcomponent which is largely beyond the scope of this document, stay aware of any current SNMP-based vulnerabilities that could be used against the management server, and apply relevant HP patches to close those vulnerabilities. You can subscribe at the HP support website, http://www.itrc.hp.com, for security-related bulletins by email, even if you don't have an HP support contract.

Since the management server for VPO/OVO is a superset of the Openview Network Node Manager functionality, many sites use the Openview system as their trap destination for various network devices. By doing this, the information is available for processing in the traditional Openview Network Node Manager interface, in addition to being available in VPO/OVO for message integration.

This allows a single view, the Message Browser, to display information from VPO/OVO managed nodes with agents, plus all other network devices that may or may not have agents, including routers, switches, etc.

The method to accomplish this would be to define a template of type 'trap' rather than logfile or one of the others – a predefined template is available for some out of the box event interpretation.

3.3 threshold monitors and numerical monitoring

3.3.1 host-based threshold monitors

Threshold monitors are templates that are specifically designed to be sensitive to conditions that are numerical in nature. Some examples of monitors that come with VPO/OVO includes swap utilization and cpu utilization, which actually return percentage information.

Multiple conditions can be defined for a single threshold monitor template. For example, for swap utilization, a normal severity message could be generated

when it exceeds 80%, a minor severity message at 85%, major at 90%, and critical at 95%. Monitors can be configured to only re-alert when the value has dropped back down and risen past the configured threshold another time, or to alert continuously every time the threshold is checked (say, every 5 minutes).

Site-specific threshold monitor scripts can be written to do any site-customized function, and then use the opcmon program to transmit the numeric value of that threshold monitor to the agent. In this way any criteria that is either 0/1 or numerical in nature can be checked, such as queues for pop3 or sendmail, etc.

New monitors can also be created that run an out of the box VPO/OVO script that checks for the existence of a particular process using a 0/1 paradigm to reflect whether it is detected with a threshold set at 0.5 to catch the transition.

The monitor called “Syslogd” executes the 445-line vp_chk.sh monitor script (both monitor and script provided by default with VPO/OVO by HP), passing it the arguments of
syslogd Syslogd
The vp_chk.sh script performs a check, as appropriate to the operating system it’s running on, to determine if a process with the name of the first argument (syslogd) is running or not. It will return the number of copies of the process with that name to the monitor whose name is passed as a second argument (Syslogd).

The monitor called Syslogd is configured by default to be sensitive to when the value returned by the vp_chk.sh crosses a threshold of 0.5. Since the normal value returned by the script would be 1 to represent a single syslogd process running, the transition of the returned value to 0 to indicate that it is no longer running would trip this threshold.

The condition is configured to send a message to all VPO/OVO operators who are configured to be able to see the “OS” group for this server. Additionally, the local agent will also run an action script (also provided by HP) called st_syslogd.sh that will cause the syslog daemon to be restarted.

This is very useful from a security perspective to prevent an intruder from stopping the syslog daemon in order to prevent their activities from being logged by the syslog daemon, either locally, or forwarded via syslog mechanisms to a central repository. In this case, not only will the syslog daemon be restarted, but an operator will be notified that it needed to be restarted, which could trigger an investigation, which might catch an intruder in the act.

3.3.2 SNMP-based threshold monitors

Another variety of threshold monitor can poll SNMP MIB values and apply the same type of numeric thresholding to the results. This allows VPO/OVO to

monitor the health of a great variety of network devices and specialized equipment that could not run a VPO/OVO agent, but are capable of providing information via SNMP mib queries. Since the scope of this document is to manage distributed hosts, not network equipment, it is not described in detail here.

3.4 making templates effective

Once the templates are defined the way that we want them at GIAC Enterprises, there are two actions needed to activate them for monitoring.

3.4.1 assigning templates

The first action is to define to VPO/OVO which managed nodes should use which templates. By choosing the Actions/Node/Assign templates pulldown in the administrator's gui, a template assignment window will open, showing all currently assigned templates.

Assign our modified sulog log template to all nodes by clicking on Add. In the add configuration window that opens, type the names of the nodes to which we want to assign this template and click the Add button so that they appear in the list of nodes to which to assign the template. Click the Open Template Window button and select the modified sulog template in the template hierarchy that opens. In the first window, click Get Template Selections. Click OK. The newly assigned template will appear in the list of assigned templates.[24]

3.4.2 distributing templates

Similar to distributing software, select the Actions/Agents/Install SW & Config selection to open the window to carry out this process. In the list of the nodes to operate on, on the right, type in the fully qualified name (including domain name) of the nodes that need to be notified of their new template assignment, and click Add so that it appears in the list of machines to operate on. On the left side, choose Templates. Click OK.

Essentially the management server transmits a request to the agent for it to come to the management server to pick up newly defined templates. This process will occur in the background. You should see for each node that needed a copy of the template, a message in the message browser that says that templates have been successfully distributed for that node.

Monitoring is now effective for those templates on those nodes.

3.5 displaying and acting on messages

[24] HP OpenView VantagePoint Operations for UNIX Concepts Guide, edition 6, page 291

When an operator logs into VPO/OVO by issuing the opc command on the management server, they are challenged for their VPO/OVO login id. This is in addition to the UNIX login needed to launch the command. A java-based interface is also available that can even run on PCs and connect to the management server, that will be the predominant interface going forward.

The view presented to the operator once logged in consists of several windows that can be opened.

The Managed Node bank shows all the nodes (or groups of nodes, if layout groups have been employed) that are visible to this operator.

The Message Groups window shows all the categories that those message can fall into (Security, Job, OS, etc.).

The Application Bank shows any application icons that have been defined to be available to this operator.

The heart of the interface is the Message Browser window. This will show any messages that have not yet been acknowledged from all the nodes and message groups this operator is responsible for as defined by the administrator.

The attributes of a message are:

- node (machine that the message pertains to)
- severity
- flags (whether an automatic action been defined for this message, and was it successful or failed)
- object (the object on the managed node that this message pertains to – varies by message.)
- message text – body of the message, as defined by the administrator as the text to be used when this condition is detected

3.6 severities

The available severities that can be attached to messages are: Critical (red), major (orange), minor (yellow), warning (teal), normal (green), and unknown (blue). Two other colors pertain to messages that have been 'owned' by an operator for further investigation – pink (owned by this operator login) and white (owned by a different operator login than this one). Using the motif operator interface, if a critical message arrives, the message group window pops to the foreground so that the message is not missed. In a multi-desktop pane CDE environment, the message group window will even pop up across desktop panes so that even if the current focus is not the pane in which the VPO/OVO windows are open, an operator will still be notified of a critical message.

3.7 groupings

3.7.1 layout groups

When adding nodes to the node bank, in order to organize the nodes and avoid having the node bank becoming over cluttered, the nodes can be grouped according to site preferences. If nodes are grouped, then when messages pertaining to nodes in the group are received, the icon for the group will change color depending on the most severe message received for the nodes in the group.

3.7.2 message groups

Each template is configured, either at the template level for all conditions, or at the individual condition level, to send a resulting message to a particular message group. Some built-in message groups in the VPO/OVO product include Security, OS and Job. Additional message groups can be added to the message group bank, and used for new conditions, and for modifications to existing conditions. Sites may wish to subdivide some existing message groups to better map events and messages to their organizational structure, or their escalation process.

3.7.3 node groups

In order to establish which nodes are seen by which operators, nodes are placed in node groups. To place a node in a particular node group, open the node group bank window by selecting that pulldown from the Windows menu.

In this case you'll see the predefined hp-ux group (that contains the management server).

GIAC Enterprises wishes to classify nodes by internal versus DMZ-resident machines. Create a new node group by selecting actions/create node group. Enter DMZ as the node group name, and OK. Select the just-created DMZ node group icon and select actions/modify. In the window that opens, type in the fully qualified name of a DMZ host and click Add to display it in the list of systems to add to the node group. Click OK.

3.8 operators

3.8.1. configuring an operator login and responsibilities

Select User Bank from the Windows menu of the administrator gui. Select Actions/add new user. Enter the VPO/OVO user's name and password that they will use to login to VPO/OVO.

Click Responsibilities to open the matrix that will define what message groups for which node groups this operator sees.

The visibility of messages is assigned to an operator or profile by checking and unchecking the intersection of all message groups versus node groups. Message groups appear down the left vertical axis versus node groups across the top horizontal axis. Individual intersections (i.e. Security messages for nodes in the hp ux node group only) can be turned on by checking that intersection, or an entire row (e.g. Security messages for all nodes across all groups) or column (all messages for any node in the hp ux group) can also be selected.

For this operator, whom we want to make sure sees Security messages for DMZ nodes (perhaps because he or she concentrates on managing DMZ nodes), ensure that the intersection of the Security message group with the DMZ node group is selected. Click OK here and in the add user window.

3.8.2 operator view

When this operator logs into the VPO/OVO application via the opc command (motif version), they are challenged for the password entered by the administrator above. Once authenticated, the opc interface consists of several Motif windows that can be opened: Managed Nodes, Message Groups, Application Desktop and Message Browser.

Managed Nodes will display icons for all the nodes (or layout groups of nodes) for which this operator is responsible.

Application Desktop will show any icons that have been pre-defined by the administrator and granted to this operator to be able to execute. This is a way for operator to trigger pre-defined actions safely as other users, etc.

Message Groups is the display of all the categories into which messages will fall (Security, OS, Job, etc.)

The Message Browser window is the key to the operator interface. It is here that events detected by the agents, once filtered by this operator's definition of message groups and node groups, are displayed.

When a message arrives, additional information can be displayed by clicking on the details button.

On thing this will show is the time the message was received on the managed node, and the time when it was received at the management server. If the management server has been running all the time, this should be very shortly after it was created on the managed node. It is helpful for this reason, as well as for forensic purposes in general, to have the time synchronized across all the nodes that will participate in the VPO/OVO management environment. ntp is an excellent solution for this, but is outside our current scope.

3.9 other techniques

Now that we've covered the mechanism to get templates distributed to nodes, and monitored from a central location, there are some additional techniques that can add value.

3.9.1 syslog forwarding, including network devices

Monitoring of logfiles created by the syslogd daemon can be a powerful technique when combined with syslog forwarding. Network entities, whether other hosts that do not run a VPO/OVO agent, or devices such as routers, can be added to VPO/OVO as "nodes for external events". This means that messages that pertain to that network device will be delivered into the VPO/OVO environment through an agent on another node.

Using this technique, routers and other devices can be configured to forward their syslog messages to nodes running agents. syslog typically includes the node name of the system originating the message when logging it on the destination host. The template watching that syslog logfile can pick up the machine that the message pertains to from the correct field in the file and use that node as the node to log the message against. The icon for the node for external events will be the one to turn the appropriate color to reflect the severity of the message, not the node whose agent actually transmitted the message to VPO/OVO.

SNMP messages can also be configured into VPO/OVO through the trap interceptor that can also pertain to the node for external events, so both SNMP and syslog events from network devices can be alerted on in VPO/OVO.

3.9.2 using terminal servers for console messages

One technique that can be tremendously useful is to capture console messages from one node onto another node.

One example of this is for 'regular' machines that have serial interfaces that can serve as a console port, traditionally with a dumb terminal attached. By attaching that serial port to a lantronix terminal server, and establishing an unattended telnet session from a host that will server as the consolidator of console information (the management server makes an excellent candidate for this), any information from the serial port can be captured into a logfile for that host.

Newer models of terminal servers now include ssh functionality, so even the capturing of that serial port information can be encrypted across the network.

By configuring a VPO/OVO template pointed at the console output for a host, it is possible to set the node that any messages from that template pertain to be the node whose console it is – rather than the node onto which that output is consolidated.

In this way, if a VPO/OVO template is defined to look for events in the console output that are serious, or perhaps reflect the fact that the machine has crashed or is rebooting, messages can be generated in the VPO/OVO environment that relate to that machine – even though that machine is not currently up and not running an agent.

4.0 configuring for firewalls and intermediate security needs

http://www.docs.hp.com and the VPO/OVO manual set provide the HP OpenView Operations for UNIX, Firewall Configuration White Paper on how to configure VPO/OVO to operate when there is a firewall between the management server and the managed node. It would be highly undesirable to place the management server on the Internet outside the protection of a well-configured corporate network firewall. Placing a managed node on a DMZ is often necessary for the functioning of the applications they are designed to run, so opening additional communication into the internal corporate network, while bearing a small additional risk, may be more than offset by the functionality that the VPO/OVO agent can provide to alert on potential security intrusions.

Additional security measures can be taken with the base VPO/OVO product to allow it to work through a firewall, and also to enable additional security by activating other IP-centric protections such as IP Filter by providing those predictable port connections rather than random ones.

Since the communications between the management server and most nodes uses the DCE (or NCS variant) protocols, there is typically a range of ports that must be opened between the management server and the managed nodes on the other side of the firewall. On a normal internal network configuration where the ports used by the agent on the managed node are not of as great a concern, both the management server and the agent processes will dynamically select DCE endpoint ports upon startup, as installed by default. The dced daemon on each end of the connection provides the endpoint mapping so that the opposite end of the conversation can send its communication to the right port.

The port ranges and firewall rules in the HP OpenView Operations for UNIX, Firewall Configuration White Paper use 12001-12051 for management server ports and 13001-13030 for managed nodes ports. These are customizable to your site, provided the firewall rules are adjusted to match. If using checkpoint firewall-1 as your firewall, read section 4.4.

4.1 management server restrictions

The management server can be configured to restrict various portions of its functions to use specified ports. By adding the following information from the HP OpenView Operations for UNIX, Firewall Configuration White Paper to the file /opt/OV/bin/OpC/install/opcsvinfo and restarting the management server processes, they will bind themselves to the specified ports, rather than using random port numbers.

```
# Note the use of restrict to procs to make the following setting only
# apply to that particular process ONLY. Consequently, make any modifications
to  this file
# BEFORE the following section, not after
OPC_HPDCE_CLIENT_DISC_TIME 5

OPC_RESTRICT_TO_PROCS opcdispm
OPC_COMM_PORT_RANGE 12000

OPC_RESTRICT_TO_PROCS opcmsgrd
OPC_COMM_PORT_RANGE 12001

OPC_RESTRICT_TO_PROCS opcdistm
OPC_COMM_PORT_RANGE 12002

OPC_RESTRICT_TO_PROCS opccmm
OPC_COMM_PORT_RANGE 12003

OPC_RESTRICT_TO_PROCS opcforwm
OPC_COMM_PORT_RANGE 12004-12005

OPC_RESTRICT_TO_PROCS ovoareqsdr
OPC_COMM_PORT_RANGE 12006-12040

OPC_RESTRICT_TO_PROCS opcragt
OPC_COMM_PORT_RANGE 12041-12050

OPC_RESTRICT_TO_PROCS opctss
OPC_COMM_PORT_RANGE 12051-12060

OPC_RESTRICT_TO_PROCS opcvterm
OPC_COMM_PORT_RANGE 12061

ovstop ovoacomm && ovstart opc
```

4.2 agent restrictions

You can cause the agent to restrict the port numbers it used to a predictable range by adding the following information from the HP OpenView Operations for UNIX, Firewall Configuration White Paper to the opcinfo file, which on most UNIXes is located at /opt/OV/bin/OpC/install/opcinfo.

Note the use of restrict to procs to make the following setting only
apply to that particular process ONLY. Consequently, make any modifications to this file
BEFORE the following section, not after
OPC_DIST_MODE DIST_RPC
OPC_RPC_ONLY TRUE

OPC_RESTRICT_TO_PROCS opcctla
OPC_COMM_PORT_RANGE 13001

OPC_RESTRICT_TO_PROCS opcdista
OPC_COMM_PORT_RANGE 13002-13003

OPC_RESTRICT_TO_PROCS opcmsga
OPC_COMM_PORT_RANGE 13004-13006

OPC_RESTRICT_TO_PROCS opccma
OPC_COMM_PORT_RANGE 13007

Restart the agent via opcagt –kill && opcagt -start

4.3 firewall rules

Although implementing firewall rule definitions vary somewhat by vendor, they typically can be set to allow specific source/destination IP address and port combinations.

To match the above ports selected for the management server and managed nodes, add rules that allow the following[25]:

1) from: management server to:managed_nodes protocol:tcp source_port:12006-12040 and 12041-12050 destination:135
2) from managed nodes to: management server protocol:tcp source port:13002-13003 and 13004-13006 destination:135
3) from: management server to:managed_nodes protocol:tcp source_port:12006-12040 destination:13001 and 13007]
4) from: management server to:managed_nodes protocol:tcp source_port: 12041-12050 destination:13001
5) from managed nodes to: management server protocol:tcp source port:13002-13003 destination:12002
6) from managed nodes to: management server protocol:tcp source port:13004-13006 destination:12001 and 12003

[25] HP OpenView Operations for UNIX, Firewall Configuration White Paper

4.4 verifying restrictions

to verify that both the management server and the managed nodes have restricted themselves as desired, you can use the command
rpccp show mapping
to see what ports are advertised in the local dced/rpcd's endpoint map. The port numbers should match what you specified above.

You can also verify remote successful endpoint mapping communication from the management server to a managed node by issuing:
rpccp show mapping ncacn_ip_tcp:hostname
(the rpccp command is linked to from /usr/bin on HP-UX, so it is in most super-user's paths. On Solaris, the equivalent as provided by the VPO/OVO delivered HP lightweight DCE is in /opt/OV/dce/bin/rpccp.sh as a wrapper to the rpccp in the same directory.

4.4 checkpoint content filtering

When using checkpoint firewall-1 4.1 service pack 4 or later between management server and managed node, it is possible to use content filtering instead of, or in addition to, the port restrictions listed above. Content filtering for VPO/OVO agents examines the actual content of the packets communication back and forth through the firewall to ensure the UUID number matches the expected number for that destination.

For basic content filtering, enable the following rules[26]:

1) from: management server to: managed node service: DCE-RPC
2) from: managed node to: management server service: DCE-RPC
3) from:managed node to:management server service:HP-OpCdistm
4) from:managed node to:management server service:HP-OpCmsgrd-std
5) from:managed node to:management server service:HP-OpCmsgrd-coa
6) from: management server to:managed node service: HP-OpCctla
7) from: management server to:managed node service: HP-OpCctla-cfgpush
8) from: management server to:managed node service: HP-OpCctla-bulk

4.4.1 Adding ports restriction to content filtering

In order to use BOTH mechanisms to filter communication through the checkpoint firewall on both content and ports, change the predefined services, above to include the ports listed in 4.3 by "editing the match field in the services properties for the OVO Services"[27]:

[26] HP OpenView Operations for UNIX, Firewall Configuration White Paper
[27] HP OpenView Operations for UNIX, Firewall Configuration White Paper

the DCE-RPC services would be modify to look like:
(dport=DCERPC_PORT), dcerpc_uuid_ex (IID1, IID2, IID3, IID4)

while the other rules would look like:
((dport <= high_port, dport >= lo_port), dcerpc_uuid_ex (II D1, IID2, IID3, IID4)
where lo_port to high_port is the range of ports for that rule.

4.5 restricting the protocol of the underlying dce/rpcd installation

VPO/OVO used dced to perform the endpoint mapping to find the remote end of the conversation. It is possible to restrict dced/rpcd to only advertise certain IP addresses in its functionality, and also to only listen to tcp packets and not udp.

rpcd (an endpoint mapper that does not require a full fledged dce cell) is including in the base HP-UX operating system. Since Solaris does not provide a dced/rpcd, the VPO/OVO agent installation provides one specifically for the agents use.

It is possible to cause rpcd on UX to listen only to tcp communications by modifying the file /sbin/init.d/Rpcd to change the line
/opt/dce/sbin/rpcd
to
/opt/dce/sbin/rpcd ncacn_ip_tcp

and then stopping and restarting it via
/sbin/init.d/Rpcd stop && /sbin/init.d/Rpcd start

On the provided Solaris dced, the same can be achieved by modifying the /etc/rc2.d/S70Hplwdce script to change:
daemonrunning $DCELOCAL/bin/dced –b
to
daemonrunning $DCELOCAL/bin/dced –b ncacn_ip_tcp

In the case of hosts with multiple IP address where it is desirable to restrict the ports that dced/rpcd will advertise, define the variable
RPC_SUPPORTED_NETADDRS="w.x.y.z"
export RPC_SUPPORTED_NETADDRS
in each script above, prior to the line that launches the daemon, to define the single IP address on this host that it will advertise.

Not that this does NOT restrict the addresses to which dced/rpcd will bind – it would be highly desirable to use a separate facility such as IP filter, as well as the above defined firewall rules to disallow communication to port 135 via undesirable interfaces.

4.6 installation

Although in a higher security environment like a DMZ it would be somewhat unusual to allow sufficient network access to allow an automatic 'push' of the agent software, firewall rules can be added to allow it. A more typical installation would use the manual installation method for those OSes' agents that support it.

If desired, traditional installation to a UNIX node would require[28]:

1) from: management server to: managed node protocol: icmp
2) from: managed node to:management server protocol:icmp
3) from: management server to: managed node protocol:tcp from: any to:21
4) from: managed node to: management server protocol:tcp from:20 to:any
5) from: management server to: managed node protocol:tcp from: any to:512

[28] HP OpenView Operations for UNIX, Firewall Configuration White Paper

5.0 summary

Near real-time event monitoring can certainly be one important tool in securing distributed systems against security breaches. VPO/OVO can enforce consistent detection mechanisms across a large number of nodes, with a minimum of additional effort as the number of monitored nodes increases.

This document has only scratched the surface of what VPO/OVO can do. Ideally this document has provided you with some food for thought on how you might be able to use it in protecting your own systems.

6.0 references

HP website http:://www.docs.hp.com

HP website http://www.webware.hp.com

HP OpenView VantagePoint Operations for HP-UX Installation Guide for the Management Server, edition 8

HP Openview Tiering Matrix, page 1, reference 5 in that document.

HP swinstall software utility

HP Openview VantagePoint Operations for Sun Solaris Installation Guide for the Management Server

HP website http://www.hp.com/go/openview

HP website http://www.itrc.hp.com

HP OpenView VantagePoint Operations Administrator's Reference Guide, volume I, edition 6

HP OpenView VantagePoint Operations software, Logfile: SU (10.x/11.X HP-UX) template

HP OpenView VantagePoint Operations for UNIX Concepts Guide, edition 6

HP OpenView Operations for UNIX, Firewall Configuration White Paper

this is version 2.0 of this document.

Last Updated: May 25th, 2017

Upcoming Training

SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**