HP OpenView Smart Plug-In (SPI) for OpenVMS User's Guide

June 2004

This guide is intended for new users who have recently installed the HP OpenView Smart Plug-In software on their OpenVMS Version 7.3-1 or later systems.

Revision/Update Information: This is a revised manual.

Hewlett-Packard Company
Palo Alto, California

This document was prepared using DECdocument, Version 3.3-1b.

Contents

Figures

Tables

1 Overview

HP OpenView is a comprehensive, modular portfolio of software solutions for managing and optimizing business services over IT, voice, and data infrastructures. To summarize, OpenView can help you to:

- Provide better service with fewer resources
- Maintain system up time

The primary functions of OpenView are to monitor resources and to report events based on the outcome of its monitoring.

OpenView Products

In their breadth and depth, OpenView products offer solutions across the enterprise to include fault, performance, network, systems and servers, applications, web services, and storage management.

Note that for heterogeneous environments, OpenView enterprise management does not replace OpenVMS system management point products.

The following table briefly describes some HP OpenView products.

OpenView Product	Description
Network Node Manager (NNM)	Provides a map of the network and a means to pinpoint problems and network bottlenecks quickly. Uses SNMP for data collection and events.
OpenView Operations (OVO) Monitors	OVO Monitor activities: • Control and report on the health of the enterprise across boundaries “through a single pane of glass.” • Automatically collect, correlate, and respond to thousands of events from network devices, systems, databases, and applications. • Include **native agents** that are loaded onto systems to collect data, filter events, and perform actions automatically. • Include **Smart Plug-Ins (SPIs)** to manage applications and databases (for example, Oracle®, SAP, Exchange).
OpenView Storage Area Manager (OVSAM)	Centralizes and simplifies storage area management across distributed multivendor repositories and efficiently manages availability, performance, and growth.
Storage Data Protector (OmniBack)	Provides centralized and automated data protection and recovery.

2 OpenView Installation on OpenVMS Systems

The HP OpenView Smart Plug-In (SPI) software for OpenVMS comes as a POLYCENTER Software Installation kit. If you have an OpenVMS Cluster, you need to install the OpenView agent and the SPI on each individual cluster member even if all members boot from the same system disk. (The reason for this is that files are copied into the specific root of each cluster member.)

Files Installed

The installation procedure places the following files on your OpenVMS system:

- SYS$STARTUP:VMSSPI$STARTUP.COM
- SYS$STARTUP:VMSSPI$SHUTDOWN.COM
- OVO$CONTRIB:VMSSPI$SHUTDOWN.EXE
- OVO$CONTRIB:VMSSPI$SYSTEM.EXE
- OVO$CONTRIB:VMSSPI$SYSTEM.COM
- OVO$CONTRIB:VMSSPI$PERFORMANCE.EXE
- OVO$CONTRIB:VMSSPI$PERFORMANCE.COM
- OVO$CONTRIB:VMSSPI$SECURITY.EXE
- OVO$CONTRIB:VMSSPI$SECURITY.COM
- OVO$CONTRIB:VMSSPI$CONFIGURE_SYSTEM.EXE
- OVO$CONTRIB:VMSSPI$DEVICES.EXE
- OVO$CONTRIB:VMSSPI.TAR

Configuration Work

You can start OpenVMS Smart Plug-Ins (SPIs) “out-of-the-box.” However, to obtain the best results, you need to do some configuration work. The first time you start up the SPI, the configuration utility that scans your system and cluster members generates a configuration file. You can modify this configuration as described in Section 3.

Note that this configuration utility obtains the best results when you install the OpenView Agent and SPI on each individual cluster member first.

Post-Installation Requirements

After installing the SPI, perform the following steps:

1. Modify the site-specific startup command file, SYS$MANAGER:SYSTARTUP_VMS.COM. After starting all layered products, add the following commands to the end of this file:

```
$ @sys$startup:ovo$startup
$ @sys$startup:vmsspi$startup
```

2. Modify the site-specific shutdown command file, SYS$MANAGER:SYSHUTDWN.COM. Before stopping any layered product, add the following commands to the beginning of SYS$MANAGER:SYSTARTUP_VMS.COM:

```
$ @sys$manager:vmsspi$shutdown
$ @sys$manager:ovo$shutdown
```

3 OpenView Customizations

Prior to starting the OpenVMS SPI, you need to make a number of customizations within OpenView. It is essential to define the OpenVMS Message Group and to load all templates that the SPI uses.

You usually complete these steps when you perform your initial installation and configuration. Follow the steps in this section only if you need to reload your templates or policies. (Configuration Work explains how to customize SPIs.)

Within OpenView, perform tasks in the following order:

1. Add the OpenVMS nodes and clusters you want to monitor; the README instructions explain how to do this. (An OpenVMS Cluster is defined as a node for external events. See Section 6.3.1 for more information.)
2. To distribute the templates to the OpenVMS nodes, use the graphical user interface (GUI), or enter the following command:

   ```
   # opcragt -distrib -templates -force <vms_hostname>
   ```

   For <*vms_hostname*>, enter the TCP/IP hostname of the OpenVMS system that is to be managed and that has the OpenView agents already installed.
3. **Caution**: If you intend to run the SPI on multiple nodes in a cluster, you must define all cluster members within OpenView at one time, and push the templates to all nodes. You must do this prior to starting the VMSSPI software on those nodes. Failing to do so might result in missing event messages on items that are monitored on the cluster level.

   Do not start the SPI on any node before you have pushed the templates from the OpenView Server to the OpenVMS managed node.

4 SPI for OpenVMS Functionality

The SPI for OpenVMS consists of the following modules:

Module	Description
SYSTEM	Reports on a number of system-related items such as processes, disks, shadow sets, queues, and so on.
PERFORMANCE	Reports on system and process resource utilization.
SECURITY	Reports in real-time on security events that the AUDIT_SERVER process detects.

The work performed in modules is described in the following sections.

4.1 Work of the SYSTEM Module

The OpenView SYSTEM module is activated at regular time intervals (usually each minute) and reports on the items shown in the following table:

What Is Monitored	The SYSTEM module...
Changes in the error count	Checks at regular time intervals if the error count on CPU, memory, and devices has changed. Note that upon startup of this SPI, no messages are sent regarding the current error count on devices. However, reporting is always done on the CPU and memory error count.
OpenVMS Cluster changes	Sends a notification whenever a node is added to or removed from an OpenVMS Cluster.
Process availability	Reports on the availability of processes. A process is defined by its OpenVMS process name and its UIC. Note the following: • Specification of the UIC is optional. If you do specify the UIC, use the identifier format or numeric format. • The process name can contain the asterisk (*) and/or percent sign (%) wildcard. • You can also check for a minimum number of occurrences if the process name contains the asterisk (*) and/or percent sign (%) wildcard. • Process availability can be checked clusterwide. • You can also restrict process availability checks during predefined periods.
Disks	Reports on the status and free space of disks. A disk is specified by its physical name or its logical volume name. For each disk, the SYSTEM SPI determines the following: • What is the status of the disk? (Is the disk correctly mounted and accessible?) • Is the disk write-locked? • Is there free space on the disk? Monitoring of free space on clusterwide mounted disks is done on a clusterwide basis. Disk state and write lock monitoring are done on a per-node basis. Monitoring of a disk can be restricted to specific periods of time.
Queue manager status	Checks the status of the queue manager or managers and reports if the status is different from “Running.”

What Is Monitored	The SYSTEM module...
Batch queue status	Reports on the status of batch queues and the number of retained and pending jobs on batch queues. The preferred status of a batch queue can be either "Started" (indicated by a status of "Idle", "Available", or "Busy") or "Stopped," during different time periods. The SYSTEM module checks that this preferred status corresponds to the actual status of the batch queue. Batch queue monitoring is usually performed on a clusterwide basis.
Print queue status	Reports on the status of print queues and the number of pending and retained jobs on print queues. Print queue monitoring is usually performed on a clusterwide basis.
Batch jobs	Reports on the availability of batch jobs. A batch job is defined by its job name, user name, and batch queue name. Corollaries to this definition are the following: • The job name can contain wildcards. • The batch queue can be a generic queue or an execution queue. • If a generic queue has been specified, and the job is currently running on one of the execution queues, the job is considered to be present. Batch job monitoring, which is usually performed clusterwide, can be restricted to certain time periods.
Shadow sets	Reports on the availability of shadow sets and the status of their members, including missing members, unexpected members, and copy and merge operations. Monitoring can be restricted to certain time periods. Clusterwide mounted shadow sets are usually monitored on a clusterwide basis.
System intruders	Reports on system intruders.

4.2 Work of the PERFORMANCE Module

The work of the OpenView PERFORMANCE module is to monitor resources whose usage affects system and process performance. The following table details the work done by the PERFORMANCE module.

What Is Monitored	The PERFORMANCE module...
CPU utilization	Reports on CPU utilization. The value reported is the actual CPU utilization over total CPU capacity times 100. This value is calculated over a period of 10 minutes. (All CPUs fully used equals 100%.)
Memory utilization	Reports on memory utilization. The value reported is the average percentage of memory utilization over a period of 5 minutes.
Page file utilization	Reports on the free space in the system page file or files. The value reported is the percentage of free space in the page file or files.
Swap file utilization	Reports on the free space in the system swap file or files. The value reported is the percentage of free space in the swap file or files.
Buffered I/O count	Reports on the total number of buffered I/Os per second, for the entire system. The value reported is the average BIO rate over a period of 5 minutes.
Direct I/O count	Reports on the total number of direct I/Os per second, for the entire system. The value reported is the average DIO rate over a period of 5 minutes.
Processes in COM or COMO state	Reports on the average number of processes in COM or COMO state over a period of 5 minutes.

What Is Monitored	The PERFORMANCE module...
Total number of processes	Reports on the current number of processes on the system. The value reported is the average number of processes over the value of the SYSGEN parameter MAXPROCESSCNT times 100. This value is calculated over a period of 5 minutes.
Non-paged pool expansions	Reports on the number of expansions of the non-paged dynamic memory and on the number of times the system failed to expand non-paged dynamic memory. Note that this item is available only on OpenVMS Version 7.3-2 and higher.
System page faults	Reports on the average number of system page faults per second, over a period of five minutes.
Resource hash table utilization	Reports on the total number of resources on the system, compared to the value of the SYSGEN parameter RESHASHTBL times 100. The average utilization is calculated over a period of 5 minutes.
LAN device utilization	Reports on the Ethernet device throughput of selected LAN devices. The value reported is the line utilization to the line speed times 100 for the last minute.
Looping processes	Continuously looks for processes that use high amounts of CPU but do not do any I/O. A process is flagged as "seems to be looping" if it uses a minimum of 25% of one CPU and does not do any I/O during a period of at least 2 minutes.
Active CPUs	Sends a notification message when it detects a stopped CPU on the system
Processes in special states	Sends a notification if processes are in a state other than LEF, LEFO, CEF, HIB, HIBO, COM and CUR. The PERFORMANCE module takes multiple samples of the state of each process, and notification is sent only if a process is in the same special state for a minimum of 1 minute.
Disk I/O	Reports on the following items for selected disks: • The DIO rate on the disk. The value reported is the average number of DIOs made to this disk per second, over a time period of 10 minutes. • The queue length on the disk. The value reported is the average queue length per second on this disk, over a time period of 10 minutes. • Hot files on the disk. The PERFORMANCE module reports on the files on which the highest number of DIOs per second are made.
Process quota utilization	Reports on the quota utilization of each process on the system. A message is sent when a process is detected whose utilization of one of its quotas reaches its limit. The PERFORMANCE module checks on the following quotas: ASTLM, BIOLM, DIOLM, BYTLM, ENQLM, FILLM, PGFLQUOTA, PRCLM, and TQELM.

4.3 Work of the SECURITY Module

The AUDIT_SERVER process records security-relevant activity as it occurs on the system, that is, any activity related to user access to the system or a protected object within the system, including the following:

- Logins, logouts, and login failures.
- Changes to the user authorization, rights list, and network proxy files.
- Access to protected objects such as files, devices, global sections, queues, and so on.
- Changes to the security attributes of protected objects.

The AUDIT_SERVER usually writes security event messages to the locations shown in the following table.

Location	Description
Security audit log file	Security events are written in binary format to this clusterwide log file. Each record contains details related to the event and can be examined using the ANALYZE/AUDIT utility. The SET AUDIT/AUDIT command allows you to specify which security events are to be written to the audit log file.
Security operator terminals	These are terminals that are enabled to receive OPCOM security class messages, allowing the system manager to monitor users' activity in real time. The SET AUDIT/ALARM command allows you to specify which security events are to be written to operator terminals.

The SECURITY module allows you to monitor security events in a continuous but simplified manner. System managers can quickly detect suspicious security events, which they can then examine further using the ANALYZE/AUDIT utility.

The operator terminal and the security audit log file are the primary destinations for security event messages. An additional feature of the security auditing facility is a **listener mailbox**, which you can create to receive a binary copy of all security-auditing messages.

The security SPI does the following:

1. Creates and reads the listener mailbox.
2. Processes the auditing information. The AUDIT_SERVER writes all monitored security items to the listener mailbox; this information is summarized in a one-line message.
3. Sends a message to the OpenView server. This one-line message is sent to OpenView.

The messages written to the listener mailbox are the ones that result from entering the SET AUDIT/ALARM and/or SET AUDIT/AUDIT commands. HP recommends that certain security events be enabled for auditing; for example:

```
$ set audit/audit/enable=(acl, -
                  authorization, -
                  breakin:(all), -
                  logfailure:(all), -
                  file_access:failure:(read,write,execute,delete,control),
                  login:(dialup))
```

Use the SHOW AUDIT command to check the security events that are enabled for monitoring on your system.

5 VMSSPI Logicals

You might find the following logical names useful when you implement the OpenVMS SPI in an OpenVMS Cluster with multiple system disks. You can define these logicals in the file SYS$STARTUP:VMSSPI$LOGICALS.COM.

Note that the installation procedure does not create this file. However, VMSSPI$STARTUP.COM does check whether this file exists and, if it does, executes it.

The following sections describe VMSSPI logicals.

5.1 VMSSPI$DATA Logical

On a standalone system or in an OpenVMS Cluster with a single system disk, the OpenVMS SPIs use the configuration file that is in SYS$COMMON:[SYSMGR]. The name of the file is VMSSPI$CONFIGURATION.DAT. The SPIs ideally work with a configuration file that is common to all cluster members; therefore, the usual location for the file is SYS$COMMON:[SYSMGR].

For OpenVMS Clusters with multiple system disks, place the configuration file in a directory that all cluster members can access.

Follow these steps to create the VMSSPI$DATA logical:

1. Create a directory on a disk that is common to all members, and define the logical VMSSPI$DATA so that it points to this directory. For example:

   ```
   $ DEFINE/SYSTEM/EXECUTIVE_MODE VMSSPI$DATA DISK$COMMON:[VMSSPI]
   ```

   In this example, the logical name VMSSPI$DATA points to the [VMSPI] directory on a disk mounted clusterwide with the DISK$COMMON logical volume name.

2. Create the file VMSSPI$CONFIGURATION.DAT in this directory. You can do this by using the utility VMSSPI$CONFIGURE_SYSTEM or by copying a previously created configuration file from SYS$MANAGER to VMSSPI$DATA.

5.2 VMSSPI$NO_CLUSTER_CHECKS

OpenVMS SYSTEM SPIs usually run on every member in an OpenVMS Cluster. Only one of the instances performs clusterwide monitoring, which includes clusterwide processes, clusterwide mounted disks and shadow sets, and anything related to queues. The cluster member where the System SPI performs this clusterwide monitoring can be any node in the cluster.

In some situations, you might not want to perform clusterwide monitoring on one particular cluster member, which is the case with the quorum system of a multisite disaster-tolerant cluster. This quorum system usually does not mount any cross-datacenter shadow sets and does not have access to the queue file. In a situation like this, disable the clusterwide monitoring on this node by entering the following command prior to starting the SPIs:

```
$ DEFINE/SYSTEM VMSSPI$NO_CLUSTER_CHECKS TRUE
```

6 SPI Configuration File

The SPIs need a configuration file that contains the definition of the items to monitor. In an OpenVMS Cluster, the configuration file must be common to all nodes. The name of the configuration file is VMSSPI$CONFIGURATION.DAT.

If the logical VMSSPI$DATA has been defined, the SPIs look in the directory pointed to by this logical name. If the logical name has not been defined, the configuration file must reside in SYS$COMMON:[SYSMGR].

6.1 Generating the Configuration File

You can easily generate an initial version of the configuration file by running the utility OVO$CONTRIB:VMSSPI$CONFIGURE_SYSTEM.EXE. When you run this utility, a configuration file is generated based on the current present processes, mounted disks and shadow sets, batch and print queues, and batch jobs.

The generated configuration file allows out of the box monitoring of the OpenVMS system and OpenVMS Clusters. To obtain optimal results, however, the system manager needs to edit this file.

6.2 Reconfiguring Dynamically

If changes are made to the VMSSPI$CONFIGURATION.DAT file, the OpenVMS SYSTEM SPI automatically registers these changes. New items that are added to this file are monitored, and all messages related to items that are removed from this file are also removed from the OVO message browser.

Note that the PERFORMANCE and SECURITY SPIs need to be restarted to put changes made in the configuration file into effect.

6.3 Editing the Configuration File

In the configuration file, you need to add entries for the following:

- Cluster name information
- Time interval for performing checks
- Restricted periods for monitoring
- Enabling intrusion detection
- Processes to be monitored
- Disks to be monitored
- Batch queues to be monitored
- Print queues to be monitored
- Batch jobs to be monitored
- Shadow sets to be monitored
- LAN devices to monitor
- Process quota thresholds
- Security filter settings

These configuration file entries are explained in the following sections.

6.3.1 Entering Cluster Name Information

If you have an OpenVMS Cluster, specify the name of the cluster. This name is usually the cluster alias, but if no such alias is defined, specify any appropriate name for the cluster in the following format:

```
CLUSTERNAME clustername
```

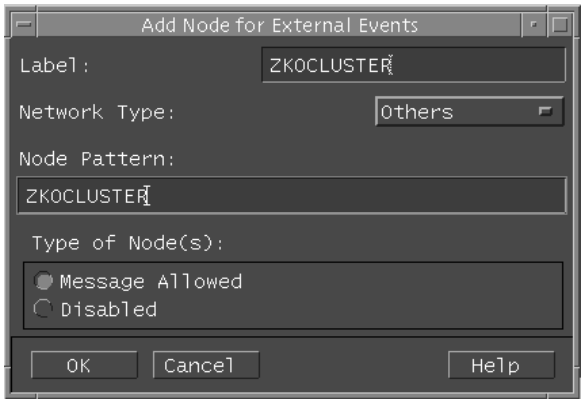
For *clustername*, enter the name of the group of systems you are monitoring.

Next, you must define a node for external events in OpenView. To do this, enter *clustername* as the name of the node.

Follow these steps:

1. Start the Node Bank window, and select Actions –> Node –> Add for External Events. The last of these is shown in Figure 1.

Figure 1 Add Node for External Events



2. In the Add Node for External Events window, for the Label and Node Pattern, enter the name of the cluster.
3. Set Network Type to “Others.”
4. For the Type of Node(s), set Message Allowed.
5. After selecting OK to define this node for external events, move the icon into the Node Groups. (Usually, you would place it in the node group containing your individual OpenVMS Cluster members.)
6. Perform a reload on the OVO Message Browser.

6.3.2 Defining the Time Interval Between Two Consecutive Checks

The OpenVMS System SPI performs all defined checks at regular time intervals. You can modify the time between two consecutive checks.

To define this interval, enter a value after the INTERVAL command in the configuration file:

```
INTERVAL value
```

For *value*, enter an integer to specifiy the number of seconds between two consecutive checks. The default interval is 60 seconds.

6.3.3 Defining Periods to Restrict Monitoring

You can restrict the monitoring of items to certain time periods. The default generated configuration file defines two default periods: ALWAYS and NEVER.

You can define your own periods by adding the following statements to the configuration file. These periods can then be used in other definitions in the configuration file.

```
PERIOD name_of_period  /MONDAY=(BEGIN=hour,END=hour) -
                       /TUESDAY=(BEGIN=hour,END=hour) -
                       /WEDNESDAY=(BEGIN=hour,END=hour) -
                       /THURSDAY=(BEGIN=hour,END=hour) -
                       /FRIDAY=(BEGIN=hour,END=hour) -
                       /SATURDAY=(BEGIN=hour,END=hour) -
                       /SUNDAY=(BEGIN=hour,END=hour) -
                       /WORKDAY=(BEGIN=hour,END=hour) -
                       /EVERYDAY=(BEGIN=hour,END=hour) -
                       /WEEKEND=(BEGIN=hour,END=hour)
```

Example:

```
 PERIOD workhours      /WORKDAY=(BEGIN=08:30,END=12:00) -
                       /WORKDAY=(BEGIN=13:00,END=17:15) -
                       /SATURDAY=(BEGIN=09:00,END=12:30)
```

This example uses the /WORKDAY qualifier twice to specify two different periods during a regular work day.

6.3.4 Defining a Process to Monitor

In the configuration file, you can define all the processes to monitor. For each process, specify the PROCESS verb, followed by the OpenVMS process name and one or more optional qualifiers:

```
PROCESS "process_name"  [/UIC="uic"] -
                        [/PERIOD=period] -
                        [/OCCURRENCES=n] -
                        [/CLUSTER_WIDE] -
                        [/NODES=(...)]
```

The *process_name* is the OpenVMS process name, which can have a maximum of 15 characters. It can contain the asterisk (*) and percent (%) wildcards. Also note that process names are casesensitive. If the process name contains lowercase letters, be sure to place double quotes (" ") around it.

Table 1 describes qualifiers you can use with PROCESS.

Table 1 PROCESS Qualifiers

Qualifier	Description
/UIC	Can be specified in different formats, such as SYSTEM, [SYSTEM], or [1,4]. Specifying the UIC is not mandatory. However, if you have two processes with the same name that run with UICs in different groups, specifying the UIC distinguishes one from the other.
/PERIOD	One of the periods defined earlier in the file. If the period is not defined, ALWAYS is assumed.
/OCCURRENCES	If the process name contains wildcards, you might want to specify the number of occurrences required for this process, if you have more than one process on your system or cluster with the same fixed name portion and a variable name portion. The default is 1.
/CLUSTER_WIDE	Specifying the qualifier /CLUSTER_WIDE indicates that the process should be present on at least one of the nodes of the cluster.
/NODES	Specifies the cluster members on which the process should be present.

The qualifiers /CLUSTER_WIDE and /NODES are mutually exclusive. If neither of these qualifiers is present, the process should be available on each node in the cluster.

Examples:

```
PROCESS ERRFMT /UIC="[1,6]" /PERIOD=ALWAYS
PROCESS ORA* /UIC=ORACLE8 /OCCURRENCES=10
PROCESS QUEUE_MANAGER /UIC=SYSTEM /CLUSTER_WIDE
```

These examples define three processes to be monitored by the SYSTEM SPI.

6.3.5 Defining Disks to Monitor

In the configuration file, you can define all the disks to be monitored. For each disk, specify the DISK verb, followed by the disk specification, and one or more of the following optional qualifiers:

```
DISK disk_name   [/PERIOD=period] -
                 [/CRITICAL=threshold] -
                 [/MAJOR=threshold] -
                 [/MINOR=threshold] -
                 [/WARNING=threshold] -
                 [/DIO -
                 [/QUEUE_LENGTH -
                 [/HOTFILES -
                 [/NODES=(...)]
```

The *disk_name* is either the physical device name or the logical volume name.

Table 2 describes qualifiers you can use with DISK. Note that you do not need to define all qualifiers.

Table 2 DISK Qualifiers

Qualifier	Description
/PERIOD	Optional qualifier. The default period is ALWAYS. Note that *only* the SYSTEM module uses this qualifier.
/CRITICAL, /MAJOR, /MINOR, and /WARNING	Define the amount of free space thresholds on the disk. The values are percentages, which can be floating values. Make sure that the critical threshold is smaller than the major threshold, that the major threshold is smaller than the minor threshold, and so on. These qualifiers are used by the SYSTEM module. To monitor free space on a disk, Dynamic Volume Expansion is taken into account; the SPI is capable of monitoring volume sets as well.
/DIO	Enables monitoring of the average number of direct I/Os made to that disk per second. This qualifier is used by the PERFORMANCE module.
/QUEUE_LENGTH	Enables monitoring of the average queue length of direct I/Os per second to that disk. This qualifier is used by the PERFORMANCE module.
/HOTFILES /NOHOTFILES	Enables or disables monitoring of hot files on the disk. This qualifier is used by the PERFORMANCE module. Note that the default configuration file is created with hot file monitoring disabled for all disks. If you want hot file monitoring on one or more disks, you must change the /NOHOTFILES qualifier to /HOTFILES and restart the PERFORMANCE SPI.
/NODES	If the disk is not mounted on all cluster members, use /NODES to specify the list of nodes that mount the disk. If you do not specify the /NODES qualifier, the disk is assumed to be mounted on all cluster members.

When you enable HOTFILE monitoring on one or more disks, you might also want to change two additional parameters in the configuration file:

Parameter	Description
HOTFILE_INTERVAL	Specifies the time interval over which the average DIO rate on each file will be calculated. The default period is 10 minutes. Specify the time interval in the format "*hh:mm:ss*". To specify a 5-minute interval, enter the following command: `PARAMETER HOTFILE_INTERVAL/VALUE="00:05:00"`
HOTFILE_TOPDIO	Specifies the number of hottest files on which the SPI will report. The default value is 3. To report on the 5 hottest files, enter the following command: `PARAMETER HOTFILE_TOPDIO/VALUE=5`

Examples:

- Example 1

```
DISK DISK$KITS /CRITICAL=5 /MAJOR=10 /NODES=(MYCULO,SWELL)!20 _$4$DUA55:
```

This example defines the monitoring of the disk with the logical volume name of DISK$KITS, which is usually mounted on the cluster members MYCULO and SWELL.

The configuration file that was initially generated using the VMSSPI$CONFIGURE_SYSTEM.EXE utility specifies critical, major, minor, and warning thresholds based on the actual amount of free space on the disk. The actual free space and the physical name of the disk are added as information in a comment at the end of the line.

- Example 2

```
DISK $1$DKA100: /DIO /QUEUE_LENGTH /HOTFILES
DISK $1$DUA53: /NODIO /QUEUE_LENGTH /NOHOTFILES
```

These examples show how to define the disk utilization monitoring of two disks. For disk 1DKA100:, disk utilization, queue length, and hot files are monitored. For disk 1DUA53:, only the queue length is monitored. (The DIO and HOTFILES qualifiers are negated.)

6.3.6 Specifying Batch Queues

Specify the names of batch queues to monitor as follows:

```
BATCHQUEUE queue-name - [/STARTED_PERIOD = period] -
                        [/STOPPED_PERIOD = period] -
                        [/[NO]PENDING_THRESHOLD=...] -
                        [/[NO]RETAINED_THRESHOLD=...] -
                        [/NODES=(node...)]
```

Explanations of BATCHQUEUE qualifiers are in Table 3.

Table 3 BATCH Qualifiers

Qualifier	Description
/STARTED_ PERIOD /STOPPED_ PERIOD	Defines when a batch queue is to be “started” during certain periods and “stopped” during other periods. You might want to check whether the actual queue state corresponds with a particular state. For information about how to specify periods, see Section 6.3.3.
/PENDING_ THRESHOLD	Makes it possible to warn the system manager about possible contentions in queues and problems with jobs currently executing and blocking the execution of other jobs. The SPI checks if the number of pending jobs in a queue exceeds a specified threshold. If it does, a message is sent.
/PENDING_ RETAINED	The SPI checks if the number of jobs retained in a queue exceeds a specified threshold. If it does, a message is sent.
/NODES	In most situations, you would not specify the /NODES qualifier because queues are usually monitored clusterwide.

If the two threshold qualifiers are negated, those items are not monitored.

Pending and retained jobs are monitored during the “Started” and “Stopped” periods that are defined.

Example:

```
$ BATCHQUEUE SYS$BATCH
```

In this example, the batch queue SYS$BATCH is always supposed to be started. If the state of the batch queue differs from Idle, Busy, or Available, notification is sent. Pending and retained jobs are not monitored.

6.3.7 Specifying Print Queues

Specify the names of print queues whose actual status needs to be monitored as follows:

```
PRINTQUEUE queue-name [/PERIOD=time_period] -
                      [/[NO]PENDING_THRESHOLD=...] -
                      [/[NO]RETAINED_THRESHOLD=...] -
                      [/NODES=(node...)]
```

Explanations of PRINTQUEUE qualifiers are in Table 4.

Table 4 PRINT Qualifiers

Qualifier	Description
/PERIOD	The default is ALWAYS.
/PENDING_ THRESHOLD	Warns the system manager about possible contentions in queues and problems with jobs currently executing and blocking the execution of other jobs.
	When the number of pending jobs in a queue exceeds a specified threshold, a message is sent.
/RETAINED_ THRESHOLD	When the number of jobs retained in a queue exceeds a specified threshold, a message is sent.
/NODES	In most situations, you would not specify the /NODES qualifier because queues are usually monitored clusterwide.

If the two threshold qualifiers are negated, those items are not monitored.

Pending and retained jobs are monitored during the “Started” and “Stopped” periods that are defined.

Example:

```
$ PRINTQUEUE SYS$LTA1 /PERIOD=WORKHOURS
```

This example specifies that the state of the print queue SYS$LTA1 is to be monitored only during the time intervals defined by the period WORKHOURS. Section 6.3.3 explains how to define this period.

6.3.8 Specifying Batch Jobs

Specify the names of batch jobs whose actual status needs to be monitored as follows:

```
JOB  job-name [/USERNAME=username] -
              [/QUEUE=queuename] -
              [/PERIOD=time_period]
              [/NODES=(...)]
```

The *job-name* is required. It defines the batch jobs that the SPI must check; it can contain the asterisk (*) and percent (%) wildcards.

Table 5 describes the qualifiers you can use with JOB.

Table 5 JOB Qualifiers

Qualifier	Description
/USERNAME	Optional qualifier. The default is SYSTEM.
/QUEUE	Optional qualifier. The default is SYS$BATCH. Specify the generic or execution queue on which the batch job is entered. If a generic queue is specified, and the job is currently running on one of the execution queues, the job will be considered to be present.
/PERIOD	Optional qualifier. The default is ALWAYS.
/NODES	In most situations, you would not specify this qualifier because batch jobs are usually monitored clusterwide.

Example:

```
$ JOB DAILY_CLEANUP /USERNAME=SYSTEM /QUEUE=SYS$BATCH
```

This example defines the monitoring of a batch job named DAILY_CLEANUP for user SYSTEM, which should be on the SYS$BATCH queue at all times.

6.3.9 Specifying Shadow Sets

Specify the names of shadow sets whose actual status needs to be monitored as follows:

```
SHADOWSET shadow-name /MEMBERS=(member1,[member2],[member3]) -
                     [/PERIOD=period] -
                     [/NODES=(...)]
```

For *shadow-name*, specify the physical name of the shadow set. You must also specify the members. No logical names are accepted.

Table 6 describes other qualifiers to SHADOWSET.

Table 6 SHADOWSET Qualifiers

Qualifier	Description
/MEMBERS	Used to specify all the shadow set members.
/PERIOD	Optional qualifier. The default is ALWAYS.
/NODES	Needs to be specified only if the shadow set is not mounted on all cluster members.

Example:

```
$ SHADOWSET DSA1 /MEMBERS=($1$DGA1000,$1$DGA2000)
```

This example tells the OpenVMS SPI to monitor whether the shadow set DSA1 contains the members 1DGA1000: and 1DGA2000: at all times.

6.3.10 Enabling Intrusion Detection

You can enable intrusion detection by adding the following statement to the configuration file:

```
INTRUDERS
```

After you make this addition to the configuration file, users who enter an incorrect password four times are considered to be intruders and are denied access to the system even if they then enter a correct password. A message is also sent to the Message Agent to signal a suspected intruder.

Optionally, you can also send a notification of SUSPECTS. You specify SUSPECTS by entering the number of login attempts a user is permitted, which defines the *threshold* you want to establish on your system. You define this threshold as part of INTRUDER statement in the configuration file, which also specifies that you want to include notification of SUSPECTS. The format is the following:

```
INTRUDERS/INCLUDE=SUSPECTS/THRESHOLD=n
```

The default threshold is 0.

Example:

```
INTRUDERS/INCLUDE=SUSPECTS/THRESHOLD=3
```

This example instructs the SPI to do the following:

1. Send a message to the Message Agent when either an intruder or a suspect is detected.
2. Update the message when the count of the intruder or suspect changes.
3. Clear the message when the intrusion record is deleted from the intrusion database.

6.3.11 LAN Devices to Monitor

Use the following format to enable monitoring of a LAN device:

```
LAN device-name/NODE=node-name
```

For *device-name*, enter the name of the ethernet controller you want to monitor. If you are running in a cluster, also specify the name of the node on which this device is located.

Example:

```
LAN EWAO: /NODE=SWELL
```

6.3.12 Security Filter Setting

By default, the SECURITY module processes all messages that the AUDIT_ SERVER writes to the listener mailbox.

If you need to forward only certain classes of events to the OpenView server, you can enable additional filtering. To do this, edit the configuration file, disabling those classes of security events that do not need to be sent to the OpenView server by removing the comment sign (the exclamation point (!)) from selected commands:

```
!DISABLE AUDIT
!DISABLE BREAKIN
!DISABLE INSTALL
!DISABLE LOGFAIR
!DISABLE LOGIN
!DISABLE MOUNT
!DISABLE NETPROXY
!DISABLE SYSUAF
!DISABLE RIGHTSDB
!DISABLE SYSTIME
!DISABLE SYSGEN
!DISABLE OBJ_CREATE
!DISABLE OBJ_DELETE
!DISABLE OBJ_ACCESS
!DISABLE CONNECTION
```

```
!DISABLE NCP
!DISABLE PROCESS
```

7 Log Files

The SPI creates a number of log files that are the primary source of information about what the SPI is monitoring, what it has detected, and what information has been sent to the Monitor agent and Message Interceptor.

If unexpected behavior is detected, then check the first log file in the table that follows. Such behaviors might be incorrect messages or messages that were expected but did not appear in the Message Browser.

Module	Log File
SYSTEM	SYS$MANAGER:VMSSPI$SYSTEM_<*nodename*>.LOG
PERFORMANCE	SYS$MANAGER:VMSSPI$PERFORMANCE_<*nodename*>.LOG
SECURITY	SYS$MANAGER:VMSSPI$SECURITY_<*nodename*>.LOG

8 OpenView Templates

Table 7 Message Templates

VMSSPI_AUDSRV_Audit

Type:	Message
Description:	One of the characteristics of the security auditing system has been changed, or a change in the list of auditable events has been made.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Minor

VMSSPI_AUDSRV_AuditServer

Type:	Message
Description:	The AUDIT_SERVER process is not running, or security auditing is currently disabled on this system.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Critical

VMSSPI_AUDSRV_Breakin

Type:	Message
Description:	A breakin attempt was detected.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Critical

VMSSPI_AUDSRV_Connection

Type:	Message
Description:	A logical link was established or terminated through DECnet, DECwindows, $IPC or SYSMAN.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_Install

Type:	Message
Description:	A change was made to the known file list through the INSTALL utility.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

(continued on next page)

Table 7 (Cont.) Message Templates

VMSSPI_AUDSRV_Logfailure

Type:	Message
Description:	A Login failure was detected.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_AUDSRV_Login

Type:	Message
Description:	A successful process login was detected.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Normal

VMSSPI_AUDSRV_Logout

Type:	Message
Description:	A process logout was detected.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Normal

VMSSPI_AUDSRV_Mount

Type:	Message
Description:	A device was mounted or dismounted.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_NCP

Type:	Message
Description:	Access to the network configuration database through the network control program (NCP) was made.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_Netproxy

Type:	Message
Description:	The network proxy authorization file has been modified.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis

(continued on next page)

Table 7 (Cont.) Message Templates

OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_ObjectAccess

Type:	Message
Description:	An object (e.g. a file, device, volume or queue) has been accessed.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_ObjectCreate

Type:	Message
Description:	An object (e.g. a file, device, volume or queue) has been created.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_ObjectDelete

Type:	Message
Description:	A device has been deleted.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Minor

VMSSPI_AUDSRV_Process

Type:	Message
Description:	A process control system service (e.g. $FORCEX, $CREPRC...) has been executed.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_AUDSRV_Rightslist

Type:	Message
Description:	The rightslist database has been modified.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

(continued on next page)

Table 7 (Cont.) Message Templates

VMSSPI_AUDSRV_Sysgen

Type:	Message
Description:	One or more SYSGEN parameters have been changed.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_AUDSRV_Systime

Type:	Message
Description:	The system time has been changed.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Minor

VMSSPI_AUDSRV_Sysuaf

Type:	Message
Description:	The system user authorization file has been changed.
Frequency:	As occurs
Used By:	Security SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_ActiveCPU

Type:	Message
Description:	Not all available CPUs are currently active.
Frequency:	Every 2 minutes
Used by:	Performance SPI
Scope:	On node basis
OVO config:	None
Severity:	Warning

VMSSPI_BatchQueue

Type:	Message
Description:	A BatchQueue problem has been detected. The configuration file defines a batch queue to monitor, but no information could be obtained on this queue (for example, the queue does not exist, or the queue manager is not running).
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Minor

VMSSPI_ClusterMemberAdded

Type:	Message
Description:	A new member has been added to the OpenVMS Cluster.
Frequency:	As defined by the INTERVAL parameter

(continued on next page)

Table 7 (Cont.) Message Templates

Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Normal

VMSSPI_ClusterMemberRemoved

Type:	Message
Description:	A member has been removed from the OpenVMS Cluster.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Critical

VMSSPI_DiskState

Type:	Message
Description:	A problem has been detected with one of the disks to be monitored. Possible messages are: - Device is not a disk. (warning) - Disk is not mounted. (critical) - Disk is mounted foreign. (warning) - Disk is allocated. (warning) - Disk is marked for dismount. (critical) - Disk is spare for a software RAID set. (warning) - Disk is a member of a shadow set. (warning) - Disk is a member of a software RAID set. (warning) - Mount verification is in progress. (critical) - Mount verification has timed out. (critical) - Mount verification is pending. (critical)
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis
OVO Config:	None
Severity:	Depends on actual message sent; see above

VMSSPI_FreeSpace

Type:	Message
Description:	The free space on a disk can be monitored by specifying the disk in the configuration file, together with 4 thresholds. Those thresholds correspond with the critical, major, minor and warning severity levels. Each time the actual free space on the disk drops below a new threshold, a message is sent.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Corresponding to the defined thresholds.

(continued on next page)

Table 7 (Cont.) Message Templates

VMSSPI_HardwareError

Type:	Message
Description:	The error count on a device, CPU or Memory has changed. Note that when the OpenVMS System SPI is started, no messages are sent regarding the current error count on devices.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Intruder

Type:	Message
Description:	An intruder has been detected on the system.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Critical

VMSSPI_LANCarrierCheckFailures

Type:	Message
Description:	Carrier failures have been detected on a LAN device.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_MemberState

Type:	Message
Description:	A problem has been detected with one of the members of a shadow set: - Disk is unexpected member. (Minor) - Disk is copy target. (Minor) - Disk is merge member. (Warning) - Disk is in mount-verification. (Critical) - Mount verification has timed out for the disk. (Critical)
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Depends on actual message sent; see above

VMSSPI_NPAGEDYN

Type:	Message
Description:	Non-paged pool has been succesfully expanded (Warning), or the system failed to expand non-paged pool.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis
OVO Config:	None

(continued on next page)

Table 7 (Cont.) Message Templates

Severity:	Depends on actual message sent; see above

VMSSPI_PendingJobs

Type:	Message
Description:	The number of jobs on a print or batch queue waiting for execution exceeds a specified threshold.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Minor

VMSSPI_PrintQueue

Type:	Message
Description:	A problem has been detected with the status of a print queue. Either no information could be obtained on the queue (queue does not exist or the queue manager is not running), or the queue has not been started (the status is not “Idle” or “Busy.”)
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Minor

VMSSPI_ProcessLooping

Type:	Message
Description:	A process has been detected doing no direct or buffered I/O, while using at least 25% of one CPU for a period of at least two minutes. A message is then sent to indicate that the process seeems to be looping.
Frequency:	Every 2 minutes
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_ProcessOccurrences

Type:	Message
Description:	The configuration file defines a process that is to be monitored; the process name contains wildcards; and a certain number of occurrences of this process are present. The OpenVMS SPI detects a number of those processes but not a sufficient number of the occurrences that were defined.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis or clusterwide
OVO Config:	None
Severity:	Major

VMSSPI_ProcessState

Type:	Message
Description:	A process has been detected in a state other than LEF, LEFO, CEF, HIB, HIBO, COM and CUR.

(continued on next page)

Table 7 (Cont.) Message Templates

Frequency:	Every 10 seconds. The process must be seen in that special state during a period of minimum one minute.
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_QueueManager

Type:	Message
Description:	The status of a queue manager is not “Running.”
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Critical

VMSSPI_Quota_ASTLM

Type:	Message
Description:	A process has used most of its ASTLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_BIOLM

Type:	Message
Description:	A process has used most of its BIOLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_BYTLM

Type:	Message
Description:	A process has used most of its BYTLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_DIOLM

Type:	Message
Description:	A process has used most of its DIOLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

(continued on next page)

Table 7 (Cont.) Message Templates

VMSSPI_Quota_ENQLM

Type:	Message
Description:	A process has used most of its ENQLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_FILLM

Type:	Message
Description:	A process has used most of its FILLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_PGFLQUOTA

Type:	Message
Description:	A process has used most of its PGFLQUOTA quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_PRCLM

Type:	Message
Description:	A process has used most of its PRCLM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_Quota_TQELM

Type:	Message
Description:	A process has used most of its TQELM quota.
Frequency:	Every 10 seconds
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	None
Severity:	Major

VMSSPI_RetainedJobs

Type:	Message
Description:	The number of retained jobs on a print or batch queue exceeds a given threshold.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide

(continued on next page)

Table 7 (Cont.) Message Templates

OVO Config:	None
Severity:	Major

VMSSPI_SecurityServer

Type:	Message
Description:	The Security Server is not active. Intrusion detection is currently disabled.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis
OVO Config:	None
Severity:	Critical

VMSSPI_ShadowSetState

Type:	Message
Description:	A problem has been detected with the state of a shadow set. The shadow set is either not mounted or is in mount verification.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis
OVO Config:	None
Severity:	Critical

VMSSPI_Started

Type:	Message
Description:	One of the OpenVMS SPI processes has been started.
Frequency:	Upon startup
Used By:	All SPIs
Scope:	On node basis
OVO Config:	None
Severity:	Normal

Table 8 Monitor Templates

VMSSPI_BatchJobMissing

Type:	Monitor
Description:	A batch job is missing.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	As defined in the OVO template. The default is critical

VMSSPI_BatchQueueNotStarted

Type:	Monitor
Description:	The status of a batch queue is other than “Available,” “Idle,” or “Busy.”
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	As defined in the OVO template. Default is major

(continued on next page)

Table 8 (Cont.) Monitor Templates

VMSSPI_BatchQueueNotStopped

Type:	Monitor
Description:	The status of a batch queue is other than "Stopped."
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	As defined in the OVO template. Default is major

VMSSPI_CPUutilization

Type:	Monitor
Description:	The system uses high amounts of CPU.
Frequency:	1 minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the actual CPU utilization over total CPU capacity times 100, calculated over a period of 10 minutes. The value is thus independent of the number of processors in your system. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: 95% - Major: 90% - Minor: 85% - Warning: 80% In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the templates.

VMSSPI_ComputableProcesses

Type:	Monitor
Description:	The average number of processes in COM and COMO states is high.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the average number of processes with COM or COMO state, over a period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: 8 processes - Major: 6 processes - Minor: 4 processes - Warning: 2 processes In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_DIOrate

Type:	Monitor
Description:	High DIO rate detected on one of the disks.

(continued on next page)

Table 8 (Cont.) Monitor Templates

Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the average number of Direct I/Os per second to the disk, over a period of 10 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 400 I/Os per second - Major: more than 300 I/Os per second - Minor: more than 200 I/Os per second - Warning: more than 100 I/Os per second In some cases, you might need to define the severity levels per system or per disk type, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_DiskNotAvailable

Type:	Monitor
Description:	A disk to monitor is defined in the configuration file, but this disk appears to be unavailable.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis
OVO Config:	None
Severity:	Warning

VMSSPI_DiskQueueLength

Type:	Monitor
Description:	High queue length of DIOs detected on one of the disks.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the average queue length per second to the disk, over a period of 10 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 15 outstanding I/Os per second - Major: more than 10 outstanding I/Os per second - Minor: more than 7 outstanding I/Os per second - Warning: more than 2 outstanding I/Os per second In some cases, you might need to define the severity levels per system or per disk type, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_DiskWriteLocked

Type:	Monitor
Description:	A disk is mounted read-only.
Frequency:	As defined by the INTERVAL parameter

(continued on next page)

Table 8 (Cont.) Monitor Templates

Used By:	System SPI
Scope:	On node basis
OVO Config:	None
Severity:	Minor

VMSSPI_Hotfile

Type:	Monitor
Description:	A hot file has been detected. The number of DIOs per second made to this file is above the threshold.
Frequency:	As defined by the HOTFILE_INTERVAL parameter. The default is 10 minutes.
Used By:	?????
Scope:	Clusterwide
OVO Config:	The value reported is the average number of DIOs per second made to to this file. Verify the threshold defined in the template, and modify it according to your preference. The default threshold is 500 DIOs per second. In some cases, a different threshold might be required for each system or disk.
Severity:	Minor????????

VMSSPI_LANutilization

Type:	Monitor
Description:	The throughput on a LAN device is high.
Frequency:	Every minute.
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the line utilization to the line speed times 100 for the last minute. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: throughput is above 55% of line capacity. - Major: throughput is above 50% of line capacity. - Minor: throughput is above 45% of line capacity. - Warning: throughput is above 40% of line capacity. In some cases, you might need to define the severity levels per system or per device, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_MemoryUtilization

Type:	Monitor
Description:	High utilization of physical memory.
Frequency:	Every minute.
Used By:	Performance SPI
Scope:	On node basis

(continued on next page)

Table 8 (Cont.) Monitor Templates

OVO Config:	The value reported is the average percentage of memory utilization over a time period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 95% of the physical memory is in use. - Major: more than 90% of the physical memory is in use. - Minor: more than 85% of the physical memory is in use. - Warning: more than 80% of the physical memory is in use. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_MissingMember

Type:	Monitor
Description:	A disk is missing as member of a shadow set.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Critical

VMSSPI_PageFileFreeSpace

Type:	Monitor
Description:	The total free space in all page files is below a specified threshold.
Frequency:	As defined by the INTERVAL parameter
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the percentage of free space in the page file or files. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: less than 55% free space in pagefiles. - Major: less than 60% free space in pagefiles. - Minor: less than 65% free space in pagefiles. - Warning: less than 70% free space in pagefiles. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_ProcessMissing

Type:	Monitor
Description:	A process is missing on the system or clusterwide.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	On node basis or clusterwide
OVO Config:	None
Severity:	Critcal

(continued on next page)

Table 8 (Cont.) Monitor Templates

VMSSPI_ProcessSlots

Type:	Monitor
Description:	High amount of process slots are in use.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the average number of processes over the value of the SYSGEN parameters MAXPROCESSCNT times 100, calculated over a time period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 90% of the available process slots are in use. - Major: more than 80% of the available process slots are in use. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_ReshashtblDense

Type:	Monitor
Description:	A high amount of resources is being used.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is average number of resources on the system, compared to the value of the SYSGEN parameter RESHASHTBL, times 100. The average is calculated over a time period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Minor: the percentage of resources found to the size of the resource hash table is more than 110. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	Minor

VMSSPI_ReshashtblSparse

Type:	Monitor
Description:	A low amount of resources is being used; however, the value of the SYSGEN parameter RESHASHTBL is very high.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis

(continued on next page)

Table 8 (Cont.) Monitor Templates

OVO Config:	The value reported is average number of resources on the system, compared to the value of the SYSGEN parameter RESHASHTBL, times 100. The average is calculated over a time period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Minor: the percentage of resources found to the size of the resource hash table is less than 30. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	Warning

VMSSPI_ShadowSetMissing

Type:	Monitor
Description:	A shadow set has been defined in the configuration file, but this shadow set is not available on the system.
Frequency:	As defined by the INTERVAL parameter
Used By:	System SPI
Scope:	Clusterwide
OVO Config:	None
Severity:	Critical

VMSSPI_SwapFileFreeSpace

Type:	Monitor
Description:	The total free space in all swap files is below a specified threshold.
Frequency:	As defined by the INTERVAL parameter
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the percentage of free space in the swap file or files. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: less than 55% free space in swapfiles. - Major: less than 60% free space in swapfiles. - Minor: less than 65% free space in swapfiles. - Warning: less than 70% free space in swapfiles. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_SystemBIOrate

Type:	Monitor
Description:	The system BIO rate is high
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis

(continued on next page)

Table 8 (Cont.) Monitor Templates

OVO Config:	The value reported is the average number of buffered I/Os per second, for the entire system, and calculated over a period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 1000 BIOs per second made by the system - Major: more than 600 BIOs per second made by the system - Minor: more than 400 BIOs per second made by the system - Warning: more than 200 BIOs per second made by the system In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_SystemDIOrate

Type:	Monitor
Description:	The system DIO rate is high.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the average number of direct I/Os per second, for the entire system, and calculated over a period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 1000 DIOs per second made by the system - Major: more than 600 DIOs per second made by the system - Minor: more than 400 DIOs per second made by the system - Warning: more than 200 DIOs per second made by the system In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template

VMSSPI_SystemPageFaultRate

Type:	Monitor
Description:	The number of system page faults is high.
Frequency:	Every minute
Used By:	Performance SPI
Scope:	On node basis
OVO Config:	The value reported is the average number of system page faults per second, calculated over a period of 5 minutes. Verify the additional conditions defined in this template, and adjust the severity levels according to your preferences. The default severity levels in this template are: - Critical: more than 10 system page faults per second. - Major: more than 5 system page faults per second. In some cases, you might need to define the severity levels per system, which requires you to create additional conditions for this template.
Severity:	As defined in the template