Monitoring

Table of Contents:

◊ Dashboard
◊ Status
◊ Edit
◊ Agent Monitoring
◊ External Monitoring
◊ SNMP Monitoring
◊ Log Monitoring
Proactive and preventive system maintenance is only possible with accurate and easily accessible information regarding the key aspects of the states of all the computers and peripherals within the network. For example, knowing that disk space utilization on a computer has reached a predefined threshold can trigger a few simple automated steps to prevent disastrous situations (e.g., loss of data or long period of system unavailability) by freeing up some space (e.g., by removing large, but old and unwanted log files), reducing the disk utilization rate (e.g., by changing the settings of some programs to create less number of log files), and ordering a larger storage disk drive (e.g., by sending an email to the technician to order and schedule to install a larger drive).

To facilitate the much desired preventive maintenance, the required information must be collected from all managed systems, categorized as to the severity of the issues and be presented to the user in an easy to understand manner. Commodity operating systems have facilities to collect the needed data on an ongoing basis and record them in various log files. The data stored in such log files, unfortunately, do not lend themselves to proactive system maintenance in that such files are not accessed and/or processed unless after a problem is manifested and one needs to find the root cause of the problem.

The Kaseya Monitoring module facilitates proactive maintenance by providing you with easily observable notification alerts to inform you that a managed computer has reached a predefined threshold. Utilizing the Monitoring module, based on indicators that you define and choose, you can monitor the health of all managed machines and SNMP devices in real time and for example, be immediately notified when:

- A critical server or desktop computer goes off-line
- A machine user disables remote control
- Any software application is added or removed
- A hardware configuration changes
- A computer is running low on disk space
- A specific event or any event log entry is generated
- A protection policy violation occurs
- An agent procedure fails execution
- An unapproved application attempts to access the network
- An unapproved application attempts to access a protected file
- A new device appears on the local area network
- An external log records a specific log entry

When an event occurs or the system reaches a critical state as defined by you, corresponding alarms are triggered, resulting in a variety of also user defined actions, such as email notifications, execution of procedures, job ticketing, and so on. Five possible methods can be used to monitor managed computers so that the necessary alarms are generated:

- Alerts - Monitors events on agent-installed machines.
- Monitor Sets - Monitors the performance state on agent-installed machines.
- SNMP Sets - Monitors the performance state on non-agent-installed network devices.
- System Check - Monitors events on non-agent-installed machines.
- Log Monitoring - Monitors events in log files.
Each of the five methods of monitoring can generate both event-based and state-based alarms.

**Event-based alarms** are conditions that occur once. For example, a backup might fail (or succeed), a software program might be denied access to a peripheral, a printer might run out of paper, etc. These events are one-time events in that an alarm is triggered the moment they occur. For example, once a printer runs out of paper, an alarm indicating that the printer is out of paper can be triggered (based on user preferences). **State-based alarms** are conditions that trigger alarms only if they persist for a period of time. For example, a momentary loss of network connection is not necessarily a cause for alarm but loss of network connection for a predefined period might be a cause for alarm.

### 6.1 Dashboard

#### 6.1.1 Dashboard List

The **Dashboard List** page (Fig. 6.1) is the VSA’s primary method of visually displaying monitoring data, including triggered alarm conditions. The **Dashboard List** page maintains configurable monitoring windows called **Dashboard Views**. Each dashboard contains one or more panes of monitoring data called **dashlets**. Each VSA user can create his/her own customized dashboards.

Before we begin to learn how to create new dashboard views and dashlets, let us first understand the functions that are supported in this page. Fig. 6.1 below shows the generic view of the Dashboard List page and all the functions supported on this page are explained below.

1. **Add Dashboard**: Click to create a new dashboard. The new dashboard displays in a popup window.

2. **Title**: Enter a title for your dashboard and click the filter icon to filter the list of dashboards listed in the paging area. Include an asterisk (*) wildcard with the text you enter to match multiple records. Enter a different title to rename the dashboard.

3. **My Dashboards**: If checked, only the dashboards you are the owner of display.

4. **View**: Displays the view icons available for each dashboard.
   - Click to view this dashboard.
   - Click to configure this dashboard.
5. **Owner**: The owner of the dashboard.

**Note**: The ownership of the dashboard has to be taken in order to modify the dashboard.

6. **Title**: The name of the dashboard.

7. **Description**: The description of the dashboard.

8. **Load on Startup**: If checked, this dashboard displays when the user logs in. Choices apply only to the currently logged in user.

### Adding Dashboard Views and Dashlets

To add a new dashboard:

1. Click to create a new Dashboard View as shown in Fig. 6.2. The new dashboard displays in a popup window.

2. Enter a **Title** and **Description** for your new dashboard in the popup window.

3. Click the **Add Dashlets** tab on the side panel. The side panel displays a list of dashlets. These choices include:

   - **Alarm List** - The Alarm List dashlet displays all alarms for all machine IDs matching the dashlet’s machine ID/group ID filter. The display lists the most recent alarms first. By default, alarms generated within the last 24 hours are highlighted in red. Alarms generated within the last week are highlighted in yellow. The color-coding lets you quickly distinguish alarms you may not have examined yet.

   - **Alarm Network Status** - Alarm Network Status dashlet displays each machine group as an icon. You can click any group icon to display the machines within that group. If a machine has even a single Open alarm, then the icon for that machine displays a red exclamation point. Click any machine icon to display an Alarm Summary Window of Open alarms for that machine.

   - **Alarm Rotator** - Alarm Rotator dashlet displays current alarms that have occurred within the last 10 minutes. Each alarm displays one at a time, in a rotating fashion, for 10 seconds.
• **Alarm Ticker** - Alarm Ticker dashlet displays current alarms that have occurred within a specified period. Each alarm displays one at a time, in a “ticker-tape” fashion, for 10 seconds.

• **Network Status** - Network Status dashlet is specific for machines assigned monitor sets or devices assigned SNMP sets. Network Status dashlet displays each machine group as an icon. You can click any group icon to display the machines and SNMP devices within that group. If even a single monitor set or SNMP set is in an alarm state, then the icon for that machine or device displays a red exclamation point. Click any machine icon or device icon to display a list of monitor set alarms or SNMP set alarms that are currently outside their alarm thresholds. Alarms in this list are automatically removed as soon as the monitor set or SNMP set returns to a "no alarm" state.

• **Group Alarm Status** - Group Alarm Status dashlet summarizes the alarm status of all group alarm categories, for all machine IDs matching the dashlet's unique machine ID/group ID filter. Alert, system check, and log monitoring alarms are automatically assigned to a group alarm category. If an alarm is triggered, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined.

• **Monitoring Set Status** - The Monitoring Set Status dashlet displays all alarms assigned to a machine ID, whether created by monitor set, alert, system check, SNMP set, or Log Monitoring. Applies to all machine IDs matching the dashlet’s unique machine ID/group ID filter.

• **Monitor Status** - Monitor Status dashlet displays a bar chart showing the number of alarms created for the selected time interval. Applies to all machine IDs matching the dashlet’s unique machine ID/group ID filter.

• **Machines Online** - Machines Online chart shows the percentage of servers and workstations online. Applies to all machine IDs matching the dashlet’s unique machine ID/group ID filter.

• **Top N - Monitor Alarm Chart** - Top N - Monitor Alarm Chart dashlet displays a bar chart showing which machines have the most alarms for the selected time interval. Applies to all machine IDs matching the dashlet’s unique machine ID/group ID filter. The chart shows up to 10 machines.

• **KES Status** - KES Status dashlet displays different views of the security status of machine IDs using Kaseya Endpoint Security protection.

  **Note:** This dashlet does not display unless the Kaseya Endpoint Security add-on module is installed for the VSA.

• **KES Threats** - KES Threats dashlet displays different views of the security threats reported for machine IDs using Kaseya Endpoint Security protection.

  **Note:** This dashlet does not display unless the Kaseya Endpoint Security add-on module is installed for the VSA.

4. Check as many checkboxes as you like, then click the *Add* button. The side panel closes and the dashlets display in the Dashboard View.

5. Click the *Delete* tab to delete dashlets already displayed in the dashboard view.

6. Click *to save the dashboard view. Click* to save the dashboard view using a different title and description.

7. Click *Share* to share this dashboard view with other users, user roles or to make it public for all users to use and edit.
6.1.2 Dashboard Settings

The Dashboard Settings page (Fig. 6.3) enables you to customize controls for dashlets.

1. Turn notification sounds on or off for all popup monitoring windows.
2. The Chart Total Monitor Alarms and Chart Top N Monitor Alarms title and background colors are customizable. Each chart parameter is customizable; this includes the chart time interval and the number of machines referenced by the Chart Top N Monitor Alarms.
3. The Customize machines online chart zone specifies two percentages to create three zones of machines online:
   • The percentage of machines online, below which represents an alarm condition.
   • The additional percentage of machines online, below which represents a warning condition.
4. Show refresh time - Select this option to show the refresh times on the dashboard window.
5. Custom Dashboard Skin - Select the border and title bar style you want dashlets to display.
6. Apply – Click this option to apply the selected settings.
7. Default – Click this option to select the default settings.

6.2 Status

6.2.1 Alarm Summary

The Alarm Summary page displays alarms for all machine IDs that match the current machine ID / group ID filter. Additional filtering can be included for listed alarms using fields in the Alarm Filters panel. You can also
close alarms or re-open them and add notes to alarms.

**Filtering Alarms**

Values can be selected or entered in one or more of the following Alarm Filter fields. The filtering takes effect as soon as you select or enter a value.

- **Alarm ID** - A specific alarm ID.
- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Alarm State** - Open or Closed. You can only select the Open status for an alarm listed in a dashlet.
- **Alarm Summary Window**.
- **Alarm Type** - Alarm or Trending.
- **Alarm Text** - Text contained in the alarm.
- **Filter Alarm Count** - The number of alarms displayed using the current filter criteria.

Fig. 6.4 below shows the generic view of the Alarm Summary page. The functions supported by this page are listed and explained below.

1. **Alarm ID**: Lists a system-generated and unique ID for each alarm. The expand icon can be clicked to display specific alarm information.

2. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view. Each dashlet displays all machine groups and machine IDs matching the dashlet’s unique machine ID/group ID filter.

3. **State**: Click the Open/Closed link in the State column to set it to Closed/Open state. You can also set the Alarm State drop-down list to Closed and select one or more alarms listed in the paging area and click the Update button.

4. **Alarm Date**: The date and time the alarm was created.


6. **Ticket**: If a ticket has been generated for an alarm a Ticket ID link displays. Clicking this link displays the ticket in the Ticketing > View Ticket page. If no ticket has been generated for an alarm a New Ticket link displays. Click this link to create a ticket for this alarm.
7. **Name:** The name of the monitoring object.

8. **Delete:** Select one or more alarms listed in the paging area and click the *Delete* button to delete the alarm.

9. **Notes:** Notes can be entered in the *Notes* field for an alarm. Select one or more alarms listed in the paging area, enter the notes and click the *Update* button.

### 6.2.2 Suspend Alarms

The **Suspend Alarms** page suppresses alarms for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms.*

Fig. 6.5 below shows the generic view of the Suspend Alarms page. The functions supported on this module are listed and explained below.

![Fig. 6.5: Suspend Alarms](image_url)

1. **Add / Replace:** Click *Add* to add a schedule time period when alarms will be suspended for selected machine IDs. Click *Replace* to remove suspend alarm time periods currently assigned to selected machine IDs and assign them a new single time period to suspend alarms.

2. **Clear All:** Clears all time periods scheduled for suspending alarms for all selected machine IDs.

3. **Schedule:** Click *Schedule* to schedule this task on selected machine IDs using the schedule options previously selected. Enter the year, month, day, hour, and minute to schedule this task.

4. **Cancel:** Clears a time period matching the date/time parameters for suspending alarms on selected machine IDs.

5. **Run recurring:** Check the box to make this task a recurring task. Enter the number of periods to wait before running this task again.

6. **Suspend alarms:** Select the duration of time during which alarms will be suspended.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **Next Suspend:** Lists the start times when machine ID alarms are scheduled to be suspended.

9. **Duration:** Lists the duration of the time periods alarms are scheduled to be suspended.

10. **Recur:** If recurring, displays the interval to wait before running the task again.
### 6.2.3 Live Counter

The **Live Counter** page displays live **performance counter** data for a selected machine ID. A performance counter is a data item that is associated with a performance object, and if necessary, the instance. Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance. Only machines IDs assigned one or more monitor sets using Assign Monitoring are listed on this page. The list of machine IDs you can select depends on the machine ID / group ID filter.

**Performance Counter:** A data item that is associated with a performance object, and if necessary, the instance.

Each specific Live Counter displays in a new window. Each window displays a bar chart with 75 data points containing the value of the counter object for the refresh rate specified. The chart refresh rate can be set between 3 and 60 seconds. The new data displays on the far right of the chart and the data moves from right to left as it ages.

Each bar within the chart displays in a specific color, which is determined by the alarm and warning thresholds of the monitor set counter object.

- Red - if alarming
- Yellow - if within warning threshold
- Green - if not alarming or not in warning threshold

Fig. 6.6 below shows the generic view of the Live Counter page. The functions supported by this page are listed and explained below.

![Live Counter Page](image-url)

**Fig. 6.6: Live Counter**

1. **Machine.Group ID:** Lists the Machine,Group IDs currently matching the Machine ID / Group ID filter and that has been assigned one or more monitor sets. Click a machine ID to select a monitor set, refresh rate and one or more counters.

2. **Select Monitor Set:** Select a monitor set.

3. **Refresh Rate:** Enter a value from 3 to 60. This is the interval Live Counter uses to gather data.

4. **Select Counter:** Lists the counters included in a selected monitor set. Click a counter link to display a Live Counter window for that counter.
6.3 Edit

6.3.1 Monitor Lists

The Monitor Lists page maintains the complete list of all objects, services and processes loaded on the KServer that are used to create Monitor Sets and SNMP Sets. The Monitor List page also maintains user-defined group alarms*.

Group Alarms: Alert, system check, and log monitoring alarms are automatically assigned to a group alarm category. If an alarm is triggered, the group alarm it belongs to is triggered as well.

Fig. 6.7 shows the generic view of the Monitor Lists page. All the tabs listed on this page are explained below.

1. **Counter Objects**: This tab lists counter objects you can include in a Monitor Set. Monitor Set uses the PerfMon* combination of object/counter/instance to collect counter information.

2. **PerfMon**: PerfMon sample is an introduction to performance counters. It demonstrates how to monitor local or remote system performance.

3. **Counters**: This tab lists counters you can include in a Monitor Set. Monitor Set uses the PerfMon combination of object/counter/instance to collect counter information.

4. **Counter Instances**: This tab lists counter instances you can include in a Monitor Set. Monitor Set uses the PerfMon combination of object/counter/instance to collect counter information.

   **Note**: Windows PerfMon requires that a counter object have at least one counter, but does not require an instance be available.

5. **Services**: This tab lists Windows services you can include in a Monitor Set to monitor the activity of Windows Services. This list can also be populated with the execution of the Update Lists by Scan page or the import of a Monitor Set.

6. **Processes**: This tab lists Windows processes you can include in a Monitor Set to monitor the transition of a process to or from a running state. A process is equivalent to an application. The processes list is not populated via the Update Lists by Scan feature. This list can be populated by the import
Chapter 6 - Monitoring

Sadjadi et al.

6.3.2 Update lists by scan

The Update Lists by Scan page scans one or more machine IDs and returns lists of counter objects, counters, instances and services to select from when creating or editing a monitor set. Typically only a handful of machines of each operating system type need to be scanned to provide a set of comprehensive lists. Update Lists by Scan also updates the list of event types available for monitoring using Monitoring > Alerts > Event Logs.

Fig. 6.8 below shows the generic view of the Update lists by scan page. The functions supported on this page are listed and explained below.

1. **Schedule**: Click *Schedule* to display the *Scheduler* window, which is used throughout the VSA to schedule a task.

2. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

3. **Last Scan**: This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.
4. **Next Scan:** This timestamp shows the next scheduled scan. Overdue date/time stamps display as red text with yellow highlight. A green checkmark indicates the scan is recurring.

5. **Cancel:** Click Cancel to cancel execution of this task on selected managed machines.

### 6.3.3 Monitor Sets

A **Monitor Set** is a set of count objects, counters, counterinstances, services and processes used to monitor the performance of machines. Typically, a threshold is assigned to each object-instance/counter, service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Update monitor set counter objects, instances and counters by source machine ID using **Monitor > Update Lists by Scan**.
2. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor > Monitor Lists**.
3. Create and maintain monitor sets using **Monitor > Monitor Sets**.
4. Assign monitor sets to machine IDs using **Monitor > Assign Monitoring**.
5. Optionally customize standard monitor sets as *individualized monitor sets*.
6. Optionally customize standard monitor sets using **Auto Learn**.

#### Sample Monitor Sets

The VSA provides a growing list of sample monitor sets. The names of sample monitor sets begin with ZC. You can modify sample monitor sets, but it is a better practice if you copy a sample monitor set and customize the copy. Sample monitor sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.

#### Folder Trees

Monitor sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

**Always Available**

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the folder.
- **Apply Filter** - Enter text in the filter edit box, then click the funnel icon to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

**When a Folder is Selected**

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.
- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
• **New Monitor Set** - Opens the Define Monitor Set window to create a new monitor set in the selected folder of the folder tree.

• **Import Monitor Set** - Imports a monitor set.

• **Take Ownership** - Takes ownership of a folder you do not own. This option only displays for master role users.

**When a Monitor Set is Selected**

• **Copy Monitor Set** - Copies the selected monitor set.

• **Export Monitor Set** - Exports the selected procedure.

• **Delete Monitor Set** - Deletes the selected procedure.

**Creating Monitor Sets**

1. Select a folder in the middle pane.
2. Click the **New Monitor Set** button.
3. Enter a name.
4. Enter a description.
5. Select a group alarm category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the Monitor Lists page. Group alarms display on the Dashboard List page.
6. Click **Save**. The Define Monitor Set window displays.

Fig. 6.9 below shows the generic view of the Monitor Sets page. The functions supported on this page are listed and explained below.

1. **Monitor Set Name**: Enter a descriptive name for the monitor set that helps you identify it in monitor set lists.

2. **Monitor Set Description**: Describe the monitor set in more detail. The rationale for the creation of
the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

3. **Group Alarm Column Name**: Assign this monitor set to a **Group Alarm Column Name**. If a monitor set alarm is triggered, the group alarm it belongs to is triggered as well. Group alarms display in the Group Alarm Status pane of the **Monitor > Dashboard List** page.

4. **Counter Thresholds**: This tab defines alarm conditions for all performance objects/instances/counters associated with a monitor set. These are the same performance objects, instances and counters displayed when you run **PerfMon.exe** on a Windows machine.

5. **Services Check**: This tab defines alarms conditions for a service if the service on a machine ID has stopped, and optionally attempts to restart the stopped service.

6. **Process Status**: This tab defines alarm conditions based on whether a process has started or stopped on a machine ID.

7. **Monitor Icons**: This tab selects the monitor icons that display in the Monitor Log page when various alarm states occur.

### 6.3.4 SNMP Sets

Certain network devices such as printers, routers, firewalls, servers and UPS devices can't support the installation of an agent. But a VSA agent installed on a managed machine on the same network as the device can read or write to that device using **simple network management protocol (SNMP)**. Read/write instructions are communicated using a set of object variables. Collectively, the set of object variables made available by a device is called its **Management Information Base** or **MIB**. The objects within a MIB are therefore referred to as **MIB objects**. Vendors typically provide a specific data file for each device called a **MIB file**. MIB files are used by monitoring systems such as the VSA to identify the MIB objects available on a device and the typical read or write values for each MIB object. The MIB file includes the "friendly name" associated with an object's ID number or **OID number**, enabling you to easily identify the object in SNMP sets.

**SNMP Sets** adds imports or modifies a SNMP set. A SNMP set is a set of MIB objects used to monitor the performance of SNMP enabled network devices. The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. SNMP quick sets are the easiest method of implementing SNMP monitoring on a device.

- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.

- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.

- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.

- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the SNMP type determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using **Monitor > LAN Watch**.
2. Assign SNMP sets to discovered devices using Monitor > Assign SNMP. This can include quick, standard, individualized or auto learn SNMP sets.

3. Display SNMP alarms using Monitor > SNMP Log or Dashboard List.

The following additional SNMP functions are available and can be used in any order.

1. Optionally review the list of all imported SNMP objects using Monitor > Monitor Lists.
2. Optionally maintain SNMP sets using Monitor > SNMP Sets.
3. Optionally add an SNMP object using Monitor > Add SNMP Object.
4. Optionally assign a SNMP type to an SNMP device manually using Monitor > Set SNMP Type.
5. Optionally write values to SNMP devices using Monitor > Set SNMP Values.

Folder Trees
SNMP sets are organized using two folder trees in the middle pane, underneath Private and Shared cabinets. Use the following options to manage objects in these folder trees:

Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the folder.
- **Apply Filter** - Enter text in the filter edit box, then click the funnel icon to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Folder is selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.
- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New SNMP Set** - Opens the Define SNMP Set window to create a new monitor set in the selected folder of the folder tree.
- **Import SNMP Set** - Imports a monitor set.
- **Take Ownership** - Takes ownership of a folder you do not own. This option only displays for master role users.

When a Monitor Set is selected

- **Delete Monitor Set** - Deletes the selected procedure.

Creating SNMP Sets

1. Select a folder in the middle pane.
2. Click the New SNMP Set button.
3. Enter a name.
4. Enter a description.
5. Select an SNMP type from the *Automatic deployment* to drop-down list. If a LAN Watch detects this type of SNMP device the system automatically begins monitoring the SNMP device using this SNMP set.

6. Select a group alarm category from the *Group Alarm Column Name* drop-down list. User defined group alarm column names are maintained using the Monitor Lists page. Group alarms display on the Dashboard List page.

7. Click *Save*. The *Define SNMP Set* window displays.

Fig. 6.10 below shows the generic view of the SNMP Sets page. The functions supported on this page are listed and explained below.

---

**Fig. 6.10: SNMP Sets**

---

1. **SNMP Monitor Set Name**: Enter a descriptive name for the SNMP set that helps you identify it in SNMP set lists.

2. **SNMP Monitor Set Description**: Describe the SNMP set in more detail. The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

3. **Automatic Deployment to**: Selecting a type automatically assigns a newly discovered SNMP device to a Set SNMP Type when performing a LAN Watch function.

4. **Group Alarm Column Name**: Assign this SNMP set to a *Group Alarm Column Name*. If a SNMP set alarm is triggered, the group alarm it belongs to is triggered as well. Group alarms display in the Group Alarm Status pane of the Dashboard List page.

5. **Save**: Saves changes to a record.

6. **Save As**: Saves a record using a new name.

7. **Export SNMP Set**: Click the *Export SNMP Set* link to display the procedure in XML format in the *Export Monitor Sets* popup window. You can copy it to the clipboard or download it to a text file.

8. **SNMP Sets**: This tab enables you to maintain all MIB objects associated with a SNMP set.

9. **SNMP Icons**: This tab selects the SNMP icons that display in the Dashboard List page when the following alarm states occur:
6.3.5 Add SNMP Objects

When objects are selected to include in an SNMP set you’re given the opportunity of adding a new SNMP object. This should not be necessary for the most part, because a LAN Watch retrieves the objects you typically require. But if you do need to add an SNMP object from a MIB file manually you can do so using Monitor > Add SNMP Object or by clicking the Add Object button while configuring an SNMP set.

The SNMP MIB Tree page loads a Management Information Base (MIB) file and displays it as an expandable tree of MIB objects. All MIB objects are classified by their location on the MIB tree. Once loaded you can select the MIB objects you want to install on your VSA. SNMP device manufacturers typically provide MIB files on their websites for the devices they manufacture.

If a vendor has supplied you with a MIB file, you can follow these steps:

1. Load the vendor’s MIB file by clicking Load MIB. There may be a message stating there are dependent files that need to be loaded first. The vendor may need to provide those also.
2. Click the expand icons in the MIB tree and find the desired items to monitor. Select each corresponding check box.
3. Click Add MIB Objects to move the selected items from Step 2 into the MIB object list.
4. Configure the settings for monitoring the new SNMP object within an SNMP set as you normally would.
5. The number of MIB objects in the tree can soon become unwieldy. Once the desired MIB objects have been added, the MIB file can be removed.

Fig. 6.11 below shows the generic view of the Add SNMP object page. The options supported on this page are listed and explained below.

1. Load MIB: Click Load MIB to browse for and upload a MIB file. When a MIB object is added, if the system does not already have the following standard MIB II files required by most MIBs, it loads them automatically. Once these files are loaded, the MIB tree located at the bottom of the Add SNMP Object page can be opened and navigated to find the new objects that the user can select. Most private vendor MIBs are installed under the Private folder.

   Note: The MIB file can be loaded and removed at any time and does not affect any MIB objects that are used in SNMP sets.

2. Add MIB Objects: Click Add MIB Objects to add selected objects to the VSA’s list of MIB objects.
3. **Remove MIB:** After selections have been made the MIB file can be removed. The size of the MIB tree can become so large that it is hard to navigate. Click *Remove MIB* to clean that process up.

### 6.4 Agent Monitoring

#### 6.4.1 Alerts

The *Alerts* page enables you to quickly define alerts for typical alarm conditions found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the *Low Disk* type of alarm displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alarm immediately to any machine ID displayed on the *Alerts* page and specify the response to the alarm.

**Group Alarms**

Alert, system check, and log monitoring alarms are automatically assigned to a group alarm category. If an alarm is triggered, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the *Group Alarm Status* dashlet of the *Monitor > Dashboard List* page. You can create new groups using the *Group Alarm Column Names* tab in *Monitor > Monitor Lists*. Group alarm column names are assigned to monitor sets using *Monitor > Define Monitor Set*.

**Machine summary alerts tab**

The *Alerts* tab in the *Machine Summary* page provides, in summary fashion, all the alerts defined for a machine ID. You can use this tab to quickly review, enable, or disable all the alerts applied to a single machine. Typically you display this page by *alt-clicking* the check-in status icon, for example, the icon next to any machine ID.

**Reviewing alarm conditions with or without creating alarms**

A user can assign monitor sets, SNMP sets, alerts, system checks or log monitoring to machine IDs without checking the *Create Alarm* checkbox and a *Monitor Action Log* entry will still be created. These logs enable a VSA user to review alarm conditions that have occurred with or without being specifically notified by the creation of an alarm, email or ticket. You can generate a report using *Info Center > Reports > Monitoring > Monitor Action Log*.

**To create an alert**

The same general procedure applies to all alert types.

1. Select an alert function from the *Select Alert Function* drop-down list as shown in Fig. 6.12.

2. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
   - Create Alarm
   - Create Ticket
   - Run Script
   - Email Recipients

3. Check the machine ID’s to apply the alert to.

4. Click the *Apply* button.
To cancel an alert

1. Select one or more paging rows.
2. Click the Clear button.

Select Alert function drop-down box has many options. Each of these options provide certain functionality which differentiates from each other. Each of these functions are listed and explained in detail.

I. Alerts - Summary

The Alerts - Summary page shows what alerts are enabled for each machine. Select Summary from the Select Alert Function drop-down list to view this page. You can apply or clear settings or copy enabled alerts settings. Specifically you can:

- Apply or clear settings for alarm, ticket and email notification for all enabled alert types at one time on selected machines.
- Copy all the enabled alert settings from a selected machine ID or machine ID template and apply them to multiple machine IDs.

Fig. 6.13 shows the generic view of the Alerts page when Summary is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.
1. **Create Alarm:** If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in **Monitor > Dashboard List**, **Monitor > Alarm Summary** and **Info Center > Reports > Logs > Alarm Log**.

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from **System > Preferences**.
   - If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If **Remove** is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using **System > Outbound Email**.

4. **Copy:** This option is only active when **Summary** is selected. Copy takes all the alert type settings for a single machine ID, selected by clicking **this machine ID to all selected machine IDs**, and applies these same settings to all other checked machine IDs.

5. **Apply:** Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click **Clear** to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **Alert Type:** Lists all alert types you can assign to a machine ID using the **Monitor > Alerts** page. Displays any agent procedure assignments for this machine ID.

9. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

10. **Email Address:** This column displays a comma separated list of email addresses where notifications are sent. The word **disabled** displays here if no alerts of this alert type are assigned to this machine ID.

### II. Alerts – Agent Status

The **Alerts - Agent Status** page triggers an alert when an agent is offline, first goes online, or someone has disabled remote control on the selected machine. Whenever the KServer service stops, the system suspends all agent online/offline alerts. If the KServer stops for more than 30 seconds, then agent online/offline alerts are suspended for one hour after the KServer starts up again. Rather than continuously try to connect to the KServer when the KServer is down, agents go to sleep for one hour after first trying to connect a couple times. The one hour alert suspension prevents false agent offline alerts when the KServer starts back up.
Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Alert when single agent goes off-line
- Alert when users disable remote control
- Alert when agent first goes online
- Alert when multiple agents in the same group go off-line

The following variables can be included in your formatted email alerts and in procedures.

Fig. 6.14 shows the generic view of the Alerts page when Agent Status is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;fn&gt;</td>
<td>#fn#</td>
<td>filename</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;sn&gt;</td>
<td>#sn#</td>
<td>procedure name the fetched the file</td>
</tr>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using System > Outbound Email.

5. **Apply**: Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click *Clear* to remove all parameter settings from selected machine IDs.

7. **Agent has not checked in for <N> <periods>**: If checked, an alert is triggered if the agent has not checked in for the specified number of periods.

8. **Alert when agent goes online**: If checked, an alert is triggered if the agent goes online.

9. **Alert when user disables remote control**: If checked, an alert is triggered if the user disables remote control.

10. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

11. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

12. **Email Address**: A comma separated list of email addresses where notifications are sent.

13. **Time Offline**: Displays the number of periods a machine ID must be off-line before an alarm condi-
tion occurs.

14. **Rearm Time:** The number of periods to ignore additional alarm conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

15. **Agent Goes Online:** Displays a checkmark if an alert is sent when an agent goes online.

16. **RC Disabled:** Displays a checkmark if an alert is sent when the user disables remote control.

### III. Alerts – Application Changes

The **Application Changes** page triggers an alert when a new application is installed or removed on selected machines. You can specify the directories to exclude from triggering an alert. This alert is based on the latest audit.

#### Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when application list change

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <code>&lt;db-vMachine.ComputerName&gt;</code></td>
</tr>
<tr>
<td>&lt;fn&gt;</td>
<td>#fn#</td>
<td>filename</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;sn&gt;</td>
<td>#sn#</td>
<td>procedure name the fetched the file</td>
</tr>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.15 shows the generic view of the Alerts page when Application Changes is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply**: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click Clear to remove all parameter settings from selected machine IDs.

7. **Alert when audit detects new application installed**: If checked, an alert condition is encounter when a new application is installed.
8. **Alert when audit detects existing application deleted**: If checked, an alert condition is encountered when a new application is removed.

9. **Exclude directories**: You can specify the directories to exclude from triggering an alert. The exclude path may contain the wildcard asterisk (*) character. Excluding a folder excludes all subfolders. For example, if you exclude *\Windows*, c:\Windows and all subfolders are excluded. You can add to the current list of applications, replace the current application list or remove the existing application list.

10. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

11. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

12. **Email Address**: A comma separated list of email addresses where notifications are sent.

13. **Installed Apps**: Displays a checkmark if an alert is sent when an application is installed.

14. **Removed Apps**: Displays a checkmark if an alert is sent when an application is removed.

**IV. Alerts – Get files**

The Alerts - Get File page triggers an alert when a procedure’s Get File or Get File in Directory Path command executes, uploads the file, and the file is now different from the copy previously stored on the KServer. If there was not a previous copy on the KServer, the alarm condition is encountered. Once defined for a machine ID, the same Get File alert is active for any agent procedure that uses a Get File command and is run on that machine ID.

**Passing Alert Information to Emails and Procedures**

The following type of monitoring alert emails can be sent and formatted:

- Alert when file fetched with Get File changes from the last fetch.
- Alert when file fetched with Get File is unchanged from last fetch.

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;fn&gt;</td>
<td>#fn#</td>
<td>filename</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;sn&gt;</td>
<td>#sn#</td>
<td>procedure name the fetched the file</td>
</tr>
</tbody>
</table>
Fig. 6.16 shows the generic view of the Alerts page when Get Files is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

   • The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.

   • If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.

   • If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

   • If Remove is clicked, all email addresses are removed without modifying any alert parameters.

   • Email is sent directly from the KServer to the email address specified in the alert. Set the From
Address using System > Outbound Email.

5. **Apply:** Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click *Clear* to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create *Alarm*
   - T = Create *Ticket*
   - S = Run Agent Procedure
   - E = Email Recipients

9. **Email Address:** A comma separated list of email addresses where notifications are sent.

**V. Alerts – Hardware changes**

The **Alerts - Hardware Changes** page triggers an alert when a hardware configuration changes on the selected machines. Detected hardware changes include the addition or removal of RAM, PCI devices, and disk drives. This alert is based on the latest audit.

**Passing Alert Information to Emails and Procedures**

The following type of monitoring alert emails can be sent and formatted:

- Alert when disk or PCI card is added or removed.
- Alert when the amount of installed RAM changes.

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;ha&gt;</td>
<td>#ha#</td>
<td>list of hardware additions</td>
</tr>
<tr>
<td>&lt;hr&gt;</td>
<td>#hr#</td>
<td>list of hardware removals</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;m&gt;</td>
<td>#m#</td>
<td>new RAM size</td>
</tr>
<tr>
<td>&lt;ro&gt;</td>
<td>#ro#</td>
<td>old RAM size</td>
</tr>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.17 shows the generic view of the Alerts page when Hardware changes is selected from the **Select Alert Function** drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm:** If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using System > Outbound Email.

5. **Apply:** Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.
6. **Clear**: Click *Clear* to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - **A** = Create *Alarm*
   - **T** = Create *Ticket*
   - **S** = Run Agent Procedure
   - **E** = Email Recipients

9. **Email Address**: A comma separated list of email addresses where notifications are sent.

### VI. Alerts – Low Disk

The **Low Disk** page triggers an alert when available disk space falls below a specified percentage of free disk space. A subsequent low disk alert is not created unless the target machine’s low disk space is corrected, or unless the alert is cleared, then re-applied. This alert is based on the latest audit.

**Passing Alert Information to Emails and Procedures**

The following types of monitoring alert emails can be sent and formatted:

- Alert when disk drive free space drops below a set percent.

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <code>&lt;db-vMachine.ComputerName&gt;</code></td>
</tr>
<tr>
<td>&lt;df&gt;</td>
<td>#df#</td>
<td>free disk space</td>
</tr>
<tr>
<td>&lt;dl&gt;</td>
<td>#dl#</td>
<td>drive letter</td>
</tr>
<tr>
<td>&lt;dt&gt;</td>
<td>#dt#</td>
<td>total disk space</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;pf&gt;</td>
<td>#pf#</td>
<td>percent free space</td>
</tr>
<tr>
<td>[#subject#]</td>
<td></td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td>[#body#]</td>
<td></td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.18 shows the generic view of the Alerts page when Low Disk is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm:** If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply:** Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click Clear to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.
8. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

9. **Email Address**: A comma separated list of email addresses where notifications are sent.

10. **Send alert when selected machines have less than <N> % free space on any fixed disk partition**: An alert is triggered if a machine’s free disk space is less than the specified percentage.

## VII. Alerts – Event Logs

The **Alerts - Event Logs** page triggers an alert when an event log entry for a selected machine matches specified criteria. After selecting the **event log type**, you can filter the alarm conditions specified by **event set** and by **event category**.

### Prerequisite
Event logging must be enabled for a particular machine using **Agent > Event Log Settings**.

### Windows Event Logs

An **event log service** runs on Windows operating systems (Not available with Win9x). The event log service enables event log messages to be issued by Window based programs and components. These events are stored in event logs located on each machine. The event logs of managed machines can be stored in the KServer database, serve as the basis of alerts and reports, and be archived.

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;cg&gt;</td>
<td>#cg#</td>
<td>Event category</td>
</tr>
<tr>
<td>&lt;cn&gt;</td>
<td>#cn#</td>
<td>computer name</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;ed&gt;</td>
<td>#ed#</td>
<td>event description</td>
</tr>
<tr>
<td>&lt;ei&gt;</td>
<td>#ei#</td>
<td>event id</td>
</tr>
<tr>
<td>&lt;es&gt;</td>
<td>#es#</td>
<td>event source</td>
</tr>
<tr>
<td>&lt;esn&gt;</td>
<td>#esn#</td>
<td>event source name</td>
</tr>
<tr>
<td>&lt;et&gt;</td>
<td>#et#</td>
<td>event time</td>
</tr>
<tr>
<td>&lt;eu&gt;</td>
<td>#eu#</td>
<td>event user</td>
</tr>
<tr>
<td>&lt;ev&gt;</td>
<td>#ev#</td>
<td>event set name</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;lt&gt;</td>
<td>#lt#</td>
<td>log type (Application, Security, System)</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>#tp#</td>
<td>event type - (Error, Warning, Informational, Success Audit, or Failure Audit)</td>
<td></td>
</tr>
<tr>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
<td></td>
</tr>
<tr>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
<td></td>
</tr>
</tbody>
</table>

Creating an Event Log Alert

1. On the **Monitor > Alerts** page select the **event log type** using the drop-down list.

2. Select the **Event Set filter** used to filter the events that trigger alerts. By default <All Events> is selected.

3. Check the box next to any of the following **event category**:
   - Error
   - Warning
   - Information
   - Success Audit
   - Failure Audit
   - Critical - Applies only to Vista.
   - Verbose - Applies only to Vista.

   **Note:** Red letters indicate logging disabled. Event logs may be disabled by the VSA for a particular machine, based on settings defined using **Agent > Event Log Settings**. A particular event category may be not be available for certain machines, such as the Critical and Verbose event categories for non-Vista machines

4. Specify the **frequency** of the alarm condition required to trigger an alert:
   - Alert when this event occurs once.
   - Alert when this event occurs <N> times within <N> <periods>.
   - Alert when this event doesn’t occur within <N> <periods>.
   - Ignore additional alarms for <N> <periods>.

5. Click the **Add or Replace** radio options, then click **Apply** to assign selected event type alerts to selected machine IDs.

6. Click **Remove** to remove all event based alerts from selected machine IDs.
Fig. 6.19 shows the generic view of the Alerts page when Event Logs is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run script**: If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply**: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click Clear to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.
8. **Log Type:** The type of event log being monitored.

9. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

   **EWISFCV:** The event category being monitored.

10. **Email Address:** A comma separated list of email addresses where notifications are sent.

   **Event Set:** The event set assigned to this machine ID. Multiple events sets can be assigned to the same machine ID.

11. **Interval:** The number of times an event occurs within a specified number of periods. Applies only if the Alert when this event occurs <N> times within <N> <periods> option is selected. Displays Missing if the Alert when this event doesn’t occur within <N> <periods> option is selected. Displays 1 if the Alert when this event occurs once is selected.

12. **Duration:** The number of periods and event must occur to trigger an alarm condition. Applies only if the Alert when this event occurs <N> times within <N> <periods> or Alert when this event doesn’t occur within <N> <periods> options are selected.

13. **Re-Arm:** Displays the number of periods to wait before triggering any new alarm conditions for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using Ignore additional alarms for <N> <periods>.

**VIII. Alerts – LAN Watch**

The **Alerts - LAN Watch** page works in conjunction with the LAN Watch page. LAN Watch scans a machine ID’s local LAN and detects new machines and devices connected to the machine’s LAN. Both LAN Watch and the **Alerts - LAN Watch** page can subsequently trigger an alert when a new machine or device is discovered on a LAN. Only the **Alerts - LAN Watch** page can create a ticket when a new machine or device is discovered on a LAN.

**Passing Alert Information to Emails and Procedures**

The following type of monitoring alert emails can be sent and formatted:

- Alert when new device discovered by LAN Watch

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
</tbody>
</table>
Fig. 6.20 shows the generic view of the Alerts page when *LAN Watch* is selected from the *Select Alert Function* drop-down list. The options supported on this page are listed and explained below.

<table>
<thead>
<tr>
<th>&lt;nd&gt;</th>
<th>#nd#</th>
<th>new device data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in *Monitor > Dashboard List, Monitor > Alarm Summary* and *Info Center > Reports > Logs > Alarm Log*.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

   - The email address of the currently logged on user displays in the *Email Recipients* field. It defaults from *System > Preferences*.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using *System > Outbound Email*. 

![Fig. 6.20: Alerts – LAN Watch](image)
5. **Apply**: Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click *Clear* to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create *Alarm*
   - T = Create *Ticket*
   - S = Run *Agent Procedure*
   - E = *Email Recipients*

9. **Email Address**: A comma separated list of email addresses where notifications are sent.

### IX. Alerts – Agent Procedure failure

The *Agent Procedure Failure* page triggers an alert when an agent procedure fails to execute on a managed machine. For example, if you specify a file name, directory path or registry key in an agent procedure, then run the agent procedure on a machine ID for which these values are invalid, you can be notified about the agent procedure failure using this alerts page.

#### Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:

- Format email message generated by Agent Procedure Failure alerts

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <code>&lt;db-vMachine.ComputerName&gt;</code></td>
</tr>
<tr>
<td>&lt;em&gt;</td>
<td>#em#</td>
<td>procedure error message</td>
</tr>
<tr>
<td>&lt;en&gt;</td>
<td>#en#</td>
<td>procedure name the fetched the file</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>#subject#</td>
<td></td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td>#body#</td>
<td></td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.21 shows the generic view of the Alerts page when Agent procedure failure is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in **Monitor > Dashboard List, Monitor > Alarm Summary** and **Info Center > Reports > Logs > Alarm Log**.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply**: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click Clear to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.
8. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

9. **Email Address**: A comma separated list of email addresses where notifications are sent.

### X. Alerts – Protection violation

The **Alerts - Protection Violation** page triggers an alert when a file is changed or access violation detected on a managed machine. Options include *Distributed file changed on agent and was updated*, *File access violation detected*, and *Network access violation detected*.

#### Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:

- Format email message generated by Protection Violations alerts.

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;pv&gt;</td>
<td>#pv#</td>
<td>violation description from Agent Log</td>
</tr>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.22 shows the generic view of the Alerts page when *Protection Violation* is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm:** If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using System > Outbound Email.

5. **Apply:** Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click *Clear* to remove all parameter settings from selected machine IDs.

7. **Distributed file changed on agent and was updated:** If checked, an alert is triggered when a file distributed using Procedure > Distributed File is changed on the managed machine. The agent verifies...
the distributed file at every full check-in.

8. **File access violation detected:** If checked, an alert is triggered when an attempt is made to access a file specified as blocked using **Audit > File Access**.

9. **Network access violation detected:** If checked, an alert is triggered when an attempt is made to access either an internal or external internet site using an application specified as blocked using **Audit > Network Access**.

10. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

11. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

12. **Email Address:** A comma separated list of email addresses where notifications are sent.

**XI. Alerts – New Agent Installed**

The **New Agent Installed** page triggers an alert when a new agent is installed on a managed machine by selected machine groups.

**Passing Alert Information to Emails and Procedures**
The following types of monitoring alert emails can be sent and formatted:

- **Agent checked in for the first time.**

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <code>&lt;db-vMachine.ComputerName&gt;</code></td>
</tr>
<tr>
<td>&lt;ct&gt;</td>
<td>#ct#</td>
<td>time the agent checked in for the first time</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.23 shows the generic view of the Alerts page when New Agent Installed is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Create Alarm:** If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply:** Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click Clear to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.
8. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

9. **Email Address**: A comma separated list of email addresses where notifications are sent.

### XII. Alerts – Patch Alert

The **Patch Alert** page triggers an alert for patch management events on managed machines.

- A new patch is available for the selected machine ID.
- A patch installation failed on the selected machine ID.
- The agent credential is invalid or missing for the selected machine ID.
- Windows Auto Update changed.

**To Create a Patch Alert**

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
   - Create Alarm
   - Create Ticket
   - Run Script
   - Email Recipients
2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

**To Cancel a Patch Alert**

1. Select the machine ID checkbox.
2. Click the **Clear** button.

The alert information listed next to the machine ID is removed.

**Passing Alert Information to Emails and Procedures**

The following types of patch alert emails can be sent and formatted:

- New Patch Available
- Patch Install Failed
- Patch Approval Policies Updated
• Agent Credential Invalid
• Windows Auto Update Configuration Changed

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;au&gt;</td>
<td>#au#</td>
<td>auto update change</td>
</tr>
<tr>
<td>&lt;bi&gt;</td>
<td>#bi#</td>
<td>bulletin ID</td>
</tr>
<tr>
<td>&lt;bl&gt;</td>
<td>#bl#</td>
<td>new bulletin list</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;fi&gt;</td>
<td>#fi#</td>
<td>failed bulletin ID</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;ic&gt;</td>
<td>#ic#</td>
<td>invalid credential type</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;pl&gt;</td>
<td>#pl#</td>
<td>new patch list</td>
</tr>
<tr>
<td></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>

Fig. 6.24 shows the generic view of the Alerts page when Patch Alert is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. Create Alarm: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.
2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply:** Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click Clear to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

9. **Email Address:** A comma separated list of email addresses where notifications are sent.

10. **New Patch:** If checked, an alarm is triggered when a new patch is available for this machine ID.

11. **Install Failed:** If checked, an alarm is triggered when a patch installation has failed for this machine ID.

12. **Invalid Credential:** If checked, an alarm is triggered when the credential is invalid for this machine ID.

13. **Win AU Changed:** If checked, an alarm is triggered if the group policy for Windows Automatic Update on the managed machine is changed from the setting specified by Patch Management > Windows Auto Update.
XIII. Alerts – Backup Alert

The Backup Alert page triggers an alert for backup events on managed machines.

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove page.

To Create a Backup Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
   - Create Alarm
   - Create Ticket
   - Run Script
   - Email Recipients
2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the Apply button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the Clear button.

The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of backup alert emails can be sent and formatted:

- Backup failed
- Verify backup failed
- Recurring backup skipped if machine offline
- Backup Completed Successfully
- Full Backup Completed Successfully
- Image Location free space below

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;be&gt;</td>
<td>#be#</td>
<td>backup failed error message</td>
</tr>
<tr>
<td>&lt;bt&gt;</td>
<td>#bt#</td>
<td>backup type</td>
</tr>
</tbody>
</table>
Include a view column from the database. For example, to include the computer name of the machine generating the alert in an email, use `<dbvMachine.ComputerName>`

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;db-view.column&gt;</code></td>
<td>not available</td>
</tr>
<tr>
<td><code>&lt;gr&gt;</code></td>
<td>#gr#</td>
</tr>
<tr>
<td><code>&lt;id&gt;</code></td>
<td>#id#</td>
</tr>
<tr>
<td><code>&lt;im&gt;</code></td>
<td>#im#</td>
</tr>
<tr>
<td><code>&lt;mf&gt;</code></td>
<td>#mf#</td>
</tr>
<tr>
<td><code>&lt;sk&gt;</code></td>
<td>#sk#</td>
</tr>
</tbody>
</table>

Fig. 6.25 shows the generic view of the Alerts page when *Backup Alert* is selected from the *Select Alert Function* drop-down list. The options supported on this page are listed and explained below:

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in *Monitor > Dashboard List*, *Monitor > Alarm Summary* and *Info Center > Reports > Logs > Alarm Log*.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the *Email Recipients* field. It defaults from *System > Preferences*.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
• If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

• If Remove is clicked, all email addresses are removed without modifying any alert parameters.

• Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. Apply: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. Clear: Click Clear to remove all parameter settings from selected machine IDs.

7. Backup Alert Parameters: The system triggers an alarm whenever the system discovers one of four different backup alert conditions for a selected machine ID:

   • Any Backup Completed - Alerts when any volume or folder backup completes successfully.
   • Full Backup Completed - Alerts when a full volume or folder backup completes successfully.
   • Backup Fails - Alerts when a volume or folder backup stops prior to completion for any reason. Typically, backup fails because the machine is turned off mid-backup or because the network connection to the file server referenced by Image Location is lost.
   • Recurring backup skipped if machine offline <N> times - Alerts when Skip if machine offline is set in Schedule Volumes and the backup is rescheduled the specified number of times because the machine is offline. Use this alert to notify you that backups are not even starting because the machine is turned off at the scheduled volume backup time.
   • Image location free space below <N> MB - Alerts when the hard disk being used to store the backups is less than a specified number of megabytes.

   Three additional parameters can be set:

   • Add - Adds alert parameters to selected machine IDs when Apply is selected without clearing existing parameters.
   • Replace - Replaces alert parameters on selected machine IDs when Apply is selected.
   • Remove - Clear alert parameters from selected machine IDs. Click the edit icon next to a machine ID group first to select the alert parameters you want to clear.

8. Machine.Group ID: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

9. ATSE: The ATSE response code assigned to machine IDs or SNMP devices:

   • A = Create Alarm
   • T = Create Ticket
   • S = Run Agent Procedure
   • E = Email Recipients

10. Email Address: A comma separated list of email addresses where notifications are sent.

11. Any Complete: If checked, an alarm is triggered when any backup is completed for this machine ID.

12. Full Complete: If checked, an alarm is triggered when a full backup is is completed for this machine ID.
13. **Backup Fails:** If checked, an alarm is triggered when any backup fails for this machine ID.

14. **Backup Skipped:** If checked, an alarm is triggered when any backup is skipped for this machine ID.

### XIV. Alerts – System

The **Alerts - System** page triggers an alert for selected events occurring on the KServer. Selecting the Alerts - System page does not display a managed machine list. The events listed only apply to the KServer. This option only displays for master role users.

**Passing Alert Information to Emails and Procedures**

The following types of monitoring alert emails can be sent and formatted:

- Admin account disabled manually by another user
- Admin account disabled because logon failed count exceeded threshold
- KServer has stopped
- Database backup failed
- Email reader failed (Ticketing module only)

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;an&gt;</td>
<td>#an#</td>
<td>disabled VSA user name</td>
</tr>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;bf&gt;</td>
<td>#bf#</td>
<td>database backup error data</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;el&gt;</td>
<td>#el#</td>
<td>email reader error message</td>
</tr>
<tr>
<td>&lt;fc&gt;</td>
<td>#fc#</td>
<td>value that tripped the failed logon attempt counter</td>
</tr>
<tr>
<td>&lt;fe&gt;</td>
<td>#fe#</td>
<td>time account re-enables</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;kn&gt;</td>
<td>#kn#</td>
<td>kserver IP/name</td>
</tr>
<tr>
<td>&lt;ms&gt;</td>
<td>#ms#</td>
<td>disabled VSA user type (master or standard)</td>
</tr>
<tr>
<td>#subject#</td>
<td></td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td>#body#</td>
<td></td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.26 shows the generic view of the Alerts page when System is selected from the Select Alert Function drop-down list. The options supported on this page are listed and explained below.

1. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

2. **Apply**: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

3. **Clear**: Click Clear to remove all parameter settings from selected machine IDs.

4. **Admin account disabled**: If checked, an alert is triggered when a VSA user account is disabled, whether manually or automatically.

5. **KServer stopped**: If checked, an alert is triggered when the KServer stops.

6. **System database backup failed**: If checked, an alert is triggered when the Kserver’s database backup fails

7. **Email reader in ticketing failed**: If checked, an alert is triggered if the Ticketing > Email Reader fails.

8. **System alerts sent to**: Displays the email recipients who are sent system alerts.
6.4.2 SNMP Traps Alert

The SNMP Traps Alert page triggers an alert when an SNMP Trap event log entry is created on a selected managed machine. SNMP event log entries are created in response to the managed machine receiving an SNMP trap message from an SNMP device on the same LAN as the managed machine.

When an SNMP Traps Alert is assigned to a managed machine, the agent on the machine begins generating SNMP trap events, one for each SNMP trap message it receives. The log type for these event sets is set to SNMP Trap. You can assign <All Events> to a managed machine to create an alert for any SNMP Trap event received by the managed machine, or you can create an event set filter criteria that limits the types of SNMP trap events triggering an alert.

Event Sets
Because the number of events in Windows events logs is enormous the VSA uses a record type called an event set to filter an alarm condition. Event sets contain one or more conditions. Each condition contains filters for different fields in an event log entry. The fields are source, category, event ID, user, and description. An event log entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any one of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

Creating an SNMP Traps Alert
1. Select the Monitor > SNMP Traps Alert page.
2. Select the Event Set filter used to filter the events that trigger alerts. Do not select an event set to include all SNMP Trap events.
3. Check the box next to the Warning event category. No other event categories are used by SNMP Trap Alert.
4. Specify the frequency of the alarm condition required to trigger an alert:
   - Alert when this event occurs once.
   - Alert when this event occurs <N> times within <N> <periods>.
   - Alert when this event doesn’t occur within <N> <periods>.
   - Ignore additional alarms for <N> <periods>.
5. Click the Add or Replace radio options, then click Apply to assign selected event type alerts to selected machine IDs.
6. Click Remove to remove all event based alerts from selected machine IDs.
7. Ignore the SNMP Community field. This option is not yet implemented.

Fig. 6.27 shows the generic view of the SNMP Trap Alerts page. The options supported on this page are listed and explained on the next page.
1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply**: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click Clear to remove all parameter settings from selected machine IDs.

7. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **Log Type**: The type of event log being monitored.

9. **ATSE**: The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
• T = Create Ticket
• S = Run Agent Procedure
• E = Email Recipients

EWISFCV: The event category being monitored.

10. Email Address: A comma separated list of email addresses where notifications are sent.

Event Set: Displays All events if no SNMP trap event set was selected, meaning all SNMP trap events are included.

11. Interval: The number of times an event occurs within a specified number of periods. Applies only if the Alert when this event occurs <N> times within <N> <periods> option is selected. Displays Missing if the Alert when this event doesn’t occur within <N> <periods> option is selected. Displays 1 if the Alert when this event occurs once is selected.

12. Duration: The number of periods and event must occur to trigger an alert. Applies only if the Alert when this event occurs <N> times within <N> <periods> or Alert when this event doesn’t occur within <N> <periods> options are selected.

13. Re-Arm: Displays the number of periods to wait before triggering any new alerts for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using Ignore additional alarms for <N> <periods>.

### 6.4.3 Assign Monitoring

The Assign Monitoring page creates monitor set alerts for managed machines. An alert is a response to an alarm condition. An alarm condition exists when a machine’s performance succeeds or fails to meet a pre-defined criteria.

**Monitor Sets**

A monitor set is a set of counter objects, counters, counter instances, services and processes used to monitor the performances of machines. Typically, a threshold is assigned to each object-instance/counter, service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Update monitor set counter objects, instances and counters by source machine ID using Monitor > Update Lists by Scan.
2. Optionally update monitor set counter objects, instances and counters manually and review them using Monitor Lists.
3. Create and maintain monitor sets using Monitor > Monitor Sets.
4. Assign monitor sets to machine IDs using Monitor > Assign Monitoring.
5. Optionally customize standard monitor sets as individualized monitor sets.
6. Optionally customize standard monitor sets using Auto Learn.

**Note:** Changes made to a monitor set affect all machine IDs the monitor set is already assigned to, within a couple minutes of the change.
Individualized Monitor Sets

1. You can individualize monitor set settings for a single machine.

2. Using Monitor > Assign Monitoring, select a standard monitor set using the <Select Monitor Set> drop-down list.

3. Assign this standard monitor set to a machine ID. The monitor set name displays in the Monitor Set column.

4. Click the individualized monitor set icon in the Monitor Set column to display the same options you see when defining a standard monitor set. An individualized monitor set adds an (IND) prefix to the name of the monitor set.

5. Optionally change the name or description of the individualized monitor set, then click the Save button. Providing a unique name and description helps identify an individualized monitor set in reports and log files.

6. Make changes to the monitoring settings of the individualized monitor set and click the Commit button. Changes apply only to the single machine the individualized monitor set is assigned to.

**Note:** Changes to a standard monitor set have no affect on individualized monitor sets copied from it.

Auto Learn Alarm Thresholds for Monitor Sets

You can enable Auto Learn alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by Auto Learn or run another session of Auto Learn again. Auto Learn cannot be used with individualized monitor sets.

To apply Auto Learn settings to selected machine IDs:

1. Using Monitor > Assign Monitoring, select a standard monitor set using the <Select Monitor Set> drop-down list.

2. Click Auto Learn to display the Auto Learn popup window. Use a wizard to define parameters used to calculate alarm threshold values.

3. Assign this standard monitor set, modified by your Auto Learn parameters, to selected machine IDs.

**Note:** You cannot apply Auto Learn settings to a monitor set that is already assigned to a machine ID. If necessary, clear the existing assignment of the monitor set to the machine ID, then perform steps 1 through 3 above.

Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

To Create a Monitor Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
   - Create Alarm
Create Ticket
Run Script
Email Recipients

2. Set additional email parameters.
3. Select the monitor set to add or replace.
4. Check the machine IDs to apply the alert to.
5. Click the Apply button.

To Cancel a Monitor Set Alert

1. Select the machine ID checkbox.
2. Click the Clear button.

The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures
The following types of monitoring alert emails can be sent and formatted:

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ad&gt;</td>
<td>#ad#</td>
<td>alarm duration</td>
</tr>
<tr>
<td>&lt;ao&gt;</td>
<td>#ao#</td>
<td>alarm operator</td>
</tr>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;av&gt;</td>
<td>#av#</td>
<td>alarm threshold</td>
</tr>
<tr>
<td>&lt;cg&gt;</td>
<td>#cg#</td>
<td>event category</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.Computer-Name&gt;</td>
</tr>
<tr>
<td>&lt;dv&gt;</td>
<td>#dv#</td>
<td>SNMP device name</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;ln&gt;</td>
<td>#ln#</td>
<td>monitoring log object name</td>
</tr>
<tr>
<td>&lt;lo&gt;</td>
<td>#lo#</td>
<td>monitoring log object type: counter, process, object</td>
</tr>
<tr>
<td>&lt;lv&gt;</td>
<td>#lv#</td>
<td>monitoring log value</td>
</tr>
<tr>
<td>&lt;mn&gt;</td>
<td>#mn#</td>
<td>monitor set name</td>
</tr>
</tbody>
</table>
Fig. 6.28 shows the generic view of the Assign Monitoring page. The options supported on this page are listed and explained below.

1. **Create Alarm:** If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

<table>
<thead>
<tr>
<th>#subject#</th>
<th>subject text of the email message, if an email was sent in response to an alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
5. **Add Monitor Set:** When a monitor set is assigned to machine IDs, the monitor set is added to the list of monitor sets currently assigned to those machine IDs.

6. **Replace Monitor Set:** When a monitor set is assigned to machine IDs, the monitor set replaces all monitor sets already assigned to those machine IDs.

7. **Apply:** Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

8. **Clear:** Click *Clear* to remove all parameter settings from selected machine IDs.

9. **Clear All:** Clears all monitor sets assigned to selected machine IDs.

10. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

11. **Monitor Sets:** Displays the list of all monitor sets assigned to machine IDs.

12. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

13. **Email Address:** A comma separated list of email addresses where notifications are sent.

### 6.4.4 Monitor Log

The *Monitor Log* page displays the agent monitoring object logs in chart and table formats.

1. **Machine ID.Group ID:** Click a machine ID link to display log data for all monitor sets assigned to that machine ID. The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

2. **Select monitoring object to display information:** The page displays a list of monitoring objects assigned to the selected machine ID.

3. **View:** Select a counter object by clicking the *View* link. The selected row is **bolded.** A selected row displays either as a chart or table.

   **Note:** If a monitoring object cannot be represented by a chart, only the table view is available.

4. **Expand Icon:** Click the expand icon to display details about a monitoring object.

5. **Refresh Data:** Click the refresh icon to refresh data when no values display. Applies to non-responsive monitoring. If your monitor doesn’t show any log values, verify the following:
   - Check the sample interval of the counter object. Once a monitor set is deployed counters return values to the monitor log using their specified sample interval. Wait for the sample interval plus the agent check-in interval for the first value to come back.
   - If there are no values returned, check Counter Thresholds for the Monitor Counter commands. If no values on the monitored machine or device meet the collection threshold they will not be inserted into the monitor log.
If a monitor isn’t responding, the log displays the message *Monitor Not Responding*. There can be several reasons for no response from the monitor:

- **Counters** - If the monitoring set includes a counter that does not exist on a managed machine, the log displays *Not Responding*. You can troubleshoot the monitoring of counters for a specific machine in two ways:
  
  - Use the **Monitor > Update Lists By Scan** page to scan for all monitor counters and services for that specific machine ID.
  
  - Connect to the machine managed by this agent, select the *Run* command in the *Start* menu, enter “`perfmon.exe`”, click *OK*, create a new counter log, and check for the existence of the counter objects/counter/instances that aren’t responding.

- **Services** - If the monitoring set includes a service that does not exist on a managed machine, the log displays *Service Does Not Exist*.

- **Processes** - If the monitoring set includes a process that does not exist on a managed machine, the log displays *Process Stopped*.

- **Permissions** - Make sure that the permissions for the agent’s working directory are set to full access for SYSTEM and NETWORK SERVICE. This can happen if the agent working directory is placed in the c:\program files\ or c:\windows directories. This is not recommended as these directories have special permissions set by the OS.

6. **Type**: The type of monitor object, counter, process or service.

7. **Monitor Set Name**: The name of the monitor set.

8. **Object Name**: The name of the monitor object.

9. **Last Value**: The last value reported.

10. **Bar Chart / Table**: Select the **Bar Chart** or **Table** radio option to display data in either format. Only monitor objects of type **Counters** can be displayed in bar chart format.

  - A bar chart displays the last 500 data points at the sample interval rate. The background of the chart displays in red for alarm threshold, yellow for warning threshold and green for no alarm.

  - Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds.

### 6.5 External Monitoring

#### 6.5.1 System Check

The VSA can monitor machines that don’t have an agent installed on them. This function is performed entirely within a single page called System Check. Machines without an agent are called external systems. A machine with an agent is assigned the task of performing the system check on the external system. A system check typically determines whether an external system is available or not. Types of system checks include: web server, DNS server, port connection, ping, and custom.

**To Create a System Check Alert**

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is
encountered:
  • Create Alarm
  • Create Ticket
  • Run Script
  • Email Recipients

2. Set additional email parameters.

3. Set additional system-check parameters. You may check multiple systems using the same machine ID.

4. Check the machine IDs to apply the alert to.

5. Click the Apply button.

**To Cancel a System Check Alert**

1. Select the machine ID checkbox.

2. Click the Clear button.

The alert information listed next to the machine ID is removed.

**Passing Alert Information to Emails and Procedures**
The following types of system check alert emails can be sent and formatted:

- System check alert

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine.ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;p1&gt;</td>
<td>#p1#</td>
<td>address checked</td>
</tr>
<tr>
<td>&lt;p2&gt;</td>
<td>#p2#</td>
<td>additional parameter</td>
</tr>
<tr>
<td>&lt;sc&gt;</td>
<td>#sc#</td>
<td>system check type</td>
</tr>
<tr>
<td>&lt;scn&gt;</td>
<td>#scn#</td>
<td>system check custom name</td>
</tr>
<tr>
<td>&lt;subject&gt;</td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td>&lt;body&gt;</td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.29 shows the generic view of the System Check page. The options supported on this page are listed and explained below.

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using System > Outbound Email.

5. **Apply**: Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click *Clear* to remove all parameter settings from selected machine IDs.

7. **System Check Parameters**
   Select a system check type:
- **Web Server** - Enter a URL to poll at a selected time interval.

- **DNS Server** - Enter a DNS address, either a name or IP, to poll at a selected time interval.

- **Port Connection** - Enter an address, either a name or IP, to connect to, and a port number to connect to, at a selected time interval.

- **Ping** - Enter an address, either a name or IP, to ping at a selected time interval.

- **Custom** - Enter a path to a custom program and output file to run at a selected time interval.
  - Program, parameters and output file - Enter program path. Optionally include a parameter that creates an output file, if applicable.
  - **Example:** `c:\temp\customcheck.bat > c:\temp\mytest.out`
    Output file path and name - Enter the name and path of the created output file.
  - **Example:** `c:\temp\mytest.out`
    Alarm if output file contains / does not contain - Alarm if output file contains / does not contain the specified text.
  - **Example:** Hello World.

The following optional parameters display for all types of system checks:

- **Every N Period** - Enter the number of times to run this task each time period.

- **Add** - Add this system check to selected machine IDs.

- **Replace** - Add this system check to selected machine IDs and remove all existing system checks.

- **Remove** - Remove this system check from selected machine IDs.

- **Custom Name** - Enter a custom name that displays in alarm messages and formatted emails.

- **Only alarm when service continues to not respond for N periods after first failure detected** - Suppresses the triggering of a system check alarm for a specified number of periods after the initial problem is detected, if N is greater than zero. This prevents triggering an alarm for a temporary problem.

- **Ignore additional alarms for N periods** - Suppresses the triggering of additional alarms for the same system check for a specified number of periods after the initial problem is reported, if N is greater than zero. This prevents reporting multiple alarms for the same problem.

8. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

9. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

10. **Email Address:** A comma separated list of email addresses where notifications are sent.

11. **Type:** The type of system check:
   - Web Server
- DNS Server
- Port Connection
- Ping
- Custom

12. **Interval:** The interval for the system check to recur.

13. **Duration:** The number of periods the system check alarm is suppressed, after the initial problem is detected. This prevents triggering an alarm for a temporary problem.

14. **ReArm:** The number of periods to ignore additional alarm conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

### 6.6 SNMP Monitoring

#### 6.6.1 LAN Watch

**LAN Watch** uses an existing agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without agents or SNMP devices. Optionally, VSA can send an alert when a LAN Watch discovers any new device. LAN Watch effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

**Using Multiple Machines on the Same LAN**

Typically, you do not have to run a LAN Watch on more than one machine in a scan range. Some reasons to do a LAN Watch on multiple machines within the same scan range include:

- There are multiple SNMP Communities within the same scan range and therefore there are multiple machines with different SNMP Community Read values.
- There are multiple vPro-enabled credentials required.
- There are different alert configurations required.
- The user wishes to have redundant SNMP monitoring.

**LAN Watch and Install Agents using Windows or Macintosh**

Both Windows and Macintosh agents can discover Windows and Macintosh machines on the same LAN using LAN Watch.

**Agent > Install Agents** can only install agents on:

- Windows machines if the LAN Watch discovery machine was a Windows machine.
- Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.
The generic view of the LAN Watch page is shown in Fig. 6.30 below. The options that are available for this module are:

1. **Schedule**: Click *Schedule* to display the Scheduler window, which is used throughout VSA to schedule a task.

2. **Cancel**: Click *Cancel* to stop the scheduled scan. *Cancel* also deletes all records of the devices identified on a LAN from VSA. If you re-schedule LAN Watch after clicking *Cancel*, each device on the LAN is re-identified as though for the first time.

3. **Scan IP Range**: Set the minimum and maximum IP addresses to scan here. Selecting a machine ID to scan, by checking the box next to that machine’s name, automatically fills in the minimum and maximum IP range based on that machine’s IP address and subnet mask.

   Note: LAN Watch does not scan more than 2048 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch limits it to 2048 addresses. LAN Watch only detects addresses on the local subnet to the machine you run LAN Watch from. For example, with a subnet mask of 255.255.255.0, there can be no more than 253 other devices on the local subnet.

4. **Enable SNMP**: If checked, scan for SNMP devices within the specified *Scan IP Range*.

5. **Read Community Name / Confirm**: LAN Watch can only identify SNMP devices that share the same SNMP community read value as the managed machine performing the LAN Watch. Enter the value in the *Read Community Name* and *Confirm* text boxes.

   Note: Community names are case sensitive. Typically the default read community name value is public, but may be reset by an administrator to Public, PUBLIC, etc.

6. **Enable vPro**: This option is available in Windows only. If checked, identifies vPro-enabled machines within the specified *Scan IP Range*. The machine does not need to be a vPro machine to discover vPro machines using LAN Watch. If a vPro machine is used as the LAN Watch discovery machine, it cannot discover itself.

7. **Enable Alerts**: If *Enable Alerts* is checked and a new device is discovered by LAN Watch, an alert
is sent to all email addresses listed in *Email Recipients*. LAN Watch alerts and email recipients can also be specified using the **Monitor > Alerts** page.

---

### Notes

*Machines that have not been connected to the LAN for more than 7 days and then connect are flagged as new devices and will generate an alert.*

---

8. **Email Recipients**: If alerts are enabled, enter the email addresses where alert notifications are sent. You can specify a different email address for each managed machine, even if it is for the same event. The *From* email address is specified using **System > Outbound Email**.

9. **Ignore devices seen in the last <N> days**: Enter the number of days to suppress alerts for new devices. This prevents creating alerts for devices that are connected to the network temporarily.

10. **Run Script**: If the option is checked and an alarm condition is encountered, an agent procedure is run. You must click the *Select agent procedure* link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

11. **Skip alert if MAC address matches existing agent**: Checking this box suppresses alerts if the scan identifies that the MAC address of a network device belongs to an existing managed machine with an agent on it. Otherwise a managed machine that was offline for several days and comes back online triggers an unnecessary alert during a LAN Watch.

12. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

13. **IP Range Scanned**: The IP addresses that are scanned by the selected machine ID when LAN Watch runs.

14. **Last Scan**: This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

15. **Primary DC**: This is available for Windows only. If a primary domain controller icon is displayed, this machine ID is a primary domain controller. If checked, performing a scan on a primary domain controller running Active Directory enables you to “harvest” the users and computers throughout a domain. You can subsequently install VSA agents automatically on computers listed in Active Directory and create VSA users and VSA users based on Active Directory administrator credentials.

16. **SNMP Active**: If the SNMP icon is displayed, SNMP devices are included in the scheduled scan.

17. **vPro Active**: This option is available for Windows only. If the vPro icon is displayed, vPro machines are included in the schedule scan.

18. **Alert Active**: If checked LAN Watch alerts are enabled for this scan.

### 6.6.2 Assign SNMP

The **Assign SNMP** page creates SNMP alerts for SNMP devices discovered using a LAN Watch. An alert is a response to an alarm condition.

#### Auto Learn Alarm Thresholds for SNMP Sets

You can enable **Auto Learn** alarm thresholds for any standard SNMP set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis. Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.
To apply Auto Learn settings to selected SNMP devices:

1. Select a standard SNMP set using the <Select SNMP Set> drop-down list.
2. Click Auto Learn to display the Auto Learn popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard SNMP set, modified by your Auto Learn parameters, to selected SNMP devices.

**Note:** You cannot apply Auto Learn settings to an SNMP set that is already assigned to a device. If necessary, clear the existing assignment of the SNMP set to the device, then perform steps 1 through 3 above.

Once Auto Learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

**Quick Sets**

The SNMP Info link page displays a list of SNMP objects provided by the specific SNMP device you selected. These objects are discovered by performing a limited SNMP “walk” on all discovered SNMP devices each time a LAN Watch is performed. You can subsequently define device-specific SNMP sets called quick sets and associate alerts with these quick sets. Quick sets can be individualized for a single device. The standard version of the quick set can be shared with other users and applied to similar devices throughout the VSA. The prefix (QS) is used to distinguish quick set names from other kinds of SNMP sets.

1. Discover SNMP devices using Monitor > LAN Watch.
2. Assign SNMP sets to discovered devices using Monitor > Assign SNMP.
3. Click the hyperlink underneath the name of the device, called the SNMP info link, in the Assign SNMP page to display a list of SNMP objects that apply to the specific SNMP device you selected. When the window opens, follow its instructions.
4. Display SNMP alarms using Monitor > SNMP Log or Dashboard List.

**To Create a SNMP Alert**

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
   - Create Alarm
   - Create Ticket
   - Run Script
   - Email Recipients
2. Set additional email parameters.
3. Select the SNMP set to add or replace.
4. Check the SNMP device to apply the alert to.
5. Click the Apply button.

**To Cancel a SNMP Alert**
1. Select the SNMP device checkbox.
2. Click the Clear button.

The alert information listed next to the SNMP device is removed.

**Passing Alert Information to Emails and Procedures**

The following types of monitoring alert emails can be sent and formatted:

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ad&gt;</code></td>
<td>#ad#</td>
<td>alarm duration</td>
</tr>
<tr>
<td><code>&lt;ao&gt;</code></td>
<td>#ao#</td>
<td>alarm operator</td>
</tr>
<tr>
<td><code>&lt;at&gt;</code></td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td><code>&lt;av&gt;</code></td>
<td>#av#</td>
<td>alarm threshold</td>
</tr>
<tr>
<td><code>&lt;cg&gt;</code></td>
<td>#cg#</td>
<td>event category</td>
</tr>
<tr>
<td><code>&lt;db-view.column&gt;</code></td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <code>&lt;db-vMachine.ComputerName&gt;</code></td>
</tr>
<tr>
<td><code>&lt;dv&gt;</code></td>
<td>#dv#</td>
<td>SNMP device name</td>
</tr>
<tr>
<td><code>&lt;gr&gt;</code></td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td><code>&lt;id&gt;</code></td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td><code>&lt;ln&gt;</code></td>
<td>#ln#</td>
<td>monitoring log object name</td>
</tr>
<tr>
<td><code>&lt;lo&gt;</code></td>
<td>#lo#</td>
<td>monitoring log object type: counter, process, object</td>
</tr>
<tr>
<td><code>&lt;lv&gt;</code></td>
<td>#lv#</td>
<td>monitoring log value</td>
</tr>
<tr>
<td><code>&lt;mn&gt;</code></td>
<td>#mn#</td>
<td>monitor set name</td>
</tr>
<tr>
<td><code>&lt;subject&gt;</code></td>
<td>#subject#</td>
<td>subject text of the email message, if an email was sent in response to an alert</td>
</tr>
<tr>
<td><code>&lt;body&gt;</code></td>
<td>#body#</td>
<td>body text of the email message, if an email was sent in response to an alert</td>
</tr>
</tbody>
</table>
Fig. 6.31 below shows the generic view of the Assign SNMP page. The options available on this page are listed and explained below.

1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. Select agent procedure link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
   - If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If Remove is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the From Address using System > Outbound Email.

5. **Apply**: Click Apply to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear**: Click Clear to remove all parameter settings from selected machine IDs.

7. **Clear All**: Clears all monitor sets assigned to selected machine IDs.
8. **Apply Filter:** Enter text in the filter edit box, then click the funnel icon to apply filtering to the drop-down list displayed in Select SNMP Set. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

9. **Select SNMP Set:** Select SNMP sets from the Select SNMP Set list, then click the Apply button to assign the SNMP set to selected machine IDs. You may assign more than one SNMP set to a machine ID. Add or edit SNMP sets using Monitor > SNMP Sets.

10. **Add Monitor Set:** Adds the selected SNMP set to selected SNMP devices.

11. **Replace Monitor Set(s):** Adds the selected SNMP set to selected SNMP devices and removes all other SNMP sets currently assigned to selected SNMP device.

12. **Edit SNMP List:** Manually add a new SNMP device or edit the information of existing SNMP devices. Enter the IP and MAC address, name and description for the SNMP device. You can also enter the sysDescr, sysLocation and sysContact values typically returned by polling.

13. **Name / Type:** The name returned by the ARP protocol when a LAN Watch is performed.

14. **Device IP:** The IP address of the SNMP device.

   **MAC Address:** The MAC address of the SNMP device.

15. **SNMP Info:** Displays the name returned by the SNMP protocol when a LAN Watch is performed. Click the SNMP Info link to display the SNMP objects for this SNMP device.

   **SNMP Sets:** Displays the list of SNMP sets assigned to a SNMP device.

16. **ATSE:** The ATSE response code assigned to machine IDs or SNMP devices:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Agent Procedure
   - E = Email Recipients

17. **Email Address:** A comma separated list of email addresses where notifications are sent.

### 6.6.3 SNMP Log

The SNMP Log page displays SNMP log data of MIB objects in a SNMP Set in chart or table formats.

1. Click a machine ID link to list all SNMP devices associated with a machine ID.

2. Click the IP address or name of an SNMP device to display all SNMP sets and MIB objects assigned to the SNMP device.

3. Click the expand icon to display the collection and threshold settings for a MIB object.

4. Click the down arrow icon to display MIB object log data in chart or table formats.

5. Click the Bar Chart or Table radio options to select the display format for log data.

SNMP monitor objects can contain multiple instances and be viewed together within one chart or table. For example, a network switch may have 12 ports. Each is an instance and can contain log data. All 12 instances can be combined in one chart or table. SNMP bar charts are in 3D format to allow for multiple instance viewing.
Fig. 6.32 shows the generic view of the SNMP Log page. All the options supported on this page are listed and explained below.

Fig. 6.32: SNMP Log

1. **Machine ID/Group ID / SNMP Devices**: All machines assigned to SNMP monitoring and currently matching the Machine ID / Group ID filter are displayed. Clicking the machine ID link displays all SNMP devices associated with the machine ID. Click the *SNMP device link* to display all MIB objects associated with the SNMP device.

2. **View**: Click the *View* link to display log data for a MIB object in a chart or table.

3. **Remove**: Click *Remove* to remove log data from a chart or table.

4. **View All**: If the SNMP monitor object has multiple instances, clicking the *View All* link displays all data for every instance.

5. **Remove All**: If the SNMP monitor object has multiple instances, clicking the *Remove All* link removes all data displayed for each instance.

6. **Monitor Set Name**: The name of the SNMP set the MIB object belongs to.

7. **Get Object Name**: The name of the MIB object used to monitor the SNMP device.

8. **Description**: The description of MIB object in the SNMP set.

9. **Bar Chart / Table**: Select the Bar Chart or Table radio button to display data in either format.
   - A bar chart displays the last 500 data points at the sample interval rate. The background of the chart displays in red for alarm threshold, yellow for warning threshold and green for no alarm.
   - Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds.

10. **Display Last**: Bar charts display log data for the last 500 intervals selected. For example, if you select *Display Last 500 minutes*, each bar in the chart represents 1 minute.

11. **Save View**: You can save custom views for each MIB object. The next time this MIB object is selected the saved information is loaded.

12. **Log rows per Page**: These fields only display in Table format. Select the number of rows to display
per page.

13. **Display Value Over / Under Value:** These fields only display in Table format. Filter the table rows displayed by filtering log data that is over or under the value specified.

**Refresh:** Click the refresh button to display the most current log data. If your monitor doesn’t show any log values, verify the following.

1. If there are no values returned, check the collection threshold for MIB objects in SNMP sets. If no values on the monitored device meet the collection threshold they are not included in the SNMP log.

2. The log value sample interval is determined by the total number of SNMPGet commands retrieving information from SNMP devices to the agent of the machine ID. The more SNMPGet commands the larger the sample interval. Check all SNMP devices associated with a machine ID. If some SNMP-Get commands are returning values but others are not, the SNMPGet commands for the failed requests are not compatible.

If a monitor is not responding, the log displays the message *Monitor Not Responding.* The SNMPGet command is incompatible with the device.

### 6.6.4 Set SNMP Values

The **Set SNMP Values** page enables you to write values to SNMP network devices. The SNMP objects must be *Read / Write* capable and requires entering the Write Community password assigned to the SNMP device. An SNMP community is a grouping of devices and management stations running SNMP. SNMP information is broadcast to all members of the same community on a network. SNMP default communities are:

- Write = private
- Read = public

**Note:** This page only displays machines that have been previously identified using a LAN Watch.

Fig. 6.33 below shows the generic view of the Set SNMP Values page. The options supported by this page are listed below.
1. **Machine ID, Group ID:** Lists Machine ID, Group IDs currently matching the Machine ID / Group ID filter and assigned a SNMP Community name. Click a *machine ID* to display SNMP devices associated with that machine ID.

2. **SNMP Device:** Select the specific SNMP device of interest. This displays a history of SNMP Set values written to an SNMP device by the agent of the machine ID.

3. **Create a SNMPSet command**
   Click *Create a SNMPSet command* to write a new value to this SNMP device. The following fields display:
   - **Description** - Enter an easy to remember description of this event. This displays in the history of SNMPSet values for this SNMP device.
   - **MIBObject** - Select the MIB object. Click Add Object to add a MIB object that currently does not exist on the Monitor Lists page.
   - **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
   - **writeCommunity** - The write Community password for the SNMP device. The default write community password is *private*.
   - **timeOutValue** - Enter the number of seconds to wait for the SNMP device to respond before the write command times out.
   - **setValue** - Enter the value to set the selected MIB object on the SNMP device.
   - **attempts** - Enter the number of times to try and write to the MIB object, if it fails to accept the write command.

4. **Execute SNMPSet:** Prepares a procedure that executes a SNMPSet command for the selected SNMP device.

5. **Cancel:** Ignores any data entered and re-displays the *Create a SNMP command* link and history.

### 6.6.5 Set SNMP Type

The *Set SNMP Type* page assigns types to SNMP devices manually. SNMP devices assigned to one of these types are monitored by SNMP sets of the same type. You can also give individual SNMP devices custom names and descriptions as well as remove the device from your database.

You can assign SNMP sets to devices by type automatically as follows:

1. Add or edit SNMP types using the *SNMP Device* tab in *Monitor > Monitor Lists*.

2. Add or edit the sysServicesNumber associated with SNMP types using the *SNMP Services* tab in *Monitor > Monitor Lists*. Broad categories of SNMP devices share the same sysServiceNumber.

3. Associate a SNMP type with a SNMP set using the *Automatic Deployment* to drop-down list in *Monitor > SNMP Sets > Define SNMP Set*.

4. Perform a LAN Watch. During a LAN Watch SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a sysServicesNumber associated with a SNMP type used by those SNMP sets.

5. Manually assign a SNMP type to an SNMP device using *Monitor > Set SNMP Type*. Doing so causes SNMP sets using that same type to start monitoring the SNMP device.
Fig. 6.34 below shows the generic view of the Set SNMP type. The options supported by this page are listed and explained below.

1. **Assign**: Applies the selected SNMP type to selected SNMP devices.

2. **Delete**: Removes selected SNMP devices from your database. If the device still exists the next time a LAN Watch is performed, the device will be re-added to the database. This is useful if a device’s IP or MAC address changes.

3. **Name**: List of SNMP devices generated for the specific machine ID by a LAN Watch.

4. **Type**: The SNMP type assigned to the SNMP device.

5. **Custom Name**: The custom name and custom description assigned to the SNMP device. If a device is given a custom name, the custom name displays instead of the SNMP name and IP address in alarms and in the SNMP log. To change the custom name and description click the edit icon next to the custom name.

6. **Device IP**: The IP address of the SNMP device.

7. **MAC Address**: The MAC address of the SNMP device.

8. **SNMP Name**: The name of the SNMP device.

### 6.7 Log Monitoring

#### 6.7.1 Parser Summary

The **Parser Summary** page displays and optionally defines alerts for all parser sets assigned to all machine IDs within the user’s scope. **Parser Summary** can also copy parser sets assignments to multiple machine IDs.

**Note**: Copying a parser set to a machine ID on this page activates the log parser on the machine IDs it is copied to. Parsing occurs whenever the log file being parsed is updated.
Log Monitoring Setup

Log Parser - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.

Assign Parser Sets - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. Activate parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.

Parser Summary - Quickly copy active parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

Notification
The agent collects log entries and creates an entry in the log monitoring log based on the criteria defined by the parser set, whether or not any of the notification methods are checked. You don’t have to be notified each time a new log monitoring entry is created. You can simply review the Log Monitoring log periodically at your convenience.

To Copy Parser Set Assignments
1. Select a source machine to copy parser set assignments from.
2. Select machine IDs to copy parser set assignments to.
3. Click Copy.

To Create a Parser Set Alert
1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
   • Create Alarm
   • Create Ticket
   • Run Script
   • Email Recipients
2. Set additional email parameters.
3. Check the machine IDs to apply the alert to.
4. Click the Apply button.

To Cancel a Parser Set Alert
1. Select the machine ID checkbox.
2. Click the Clear button.

The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures
The following types of monitoring alert emails can be sent and formatted:
• Log Monitoring parser alerts.
• Multiple log monitoring parser alerts.
• Missing log monitoring parser alert.

The following variables can be included in your formatted email alerts and in procedures.

<table>
<thead>
<tr>
<th>Within an Email</th>
<th>Within a Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;at&gt;</td>
<td>#at#</td>
<td>alert time</td>
</tr>
<tr>
<td>&lt;db-view.column&gt;</td>
<td>not available</td>
<td>Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use &lt;db-vMachine. ComputerName&gt;</td>
</tr>
<tr>
<td>&lt;ec&gt;</td>
<td>#ec#</td>
<td>event count</td>
</tr>
<tr>
<td>&lt;ed&gt;</td>
<td>#ed#</td>
<td>event description</td>
</tr>
<tr>
<td>&lt;gr&gt;</td>
<td>#gr#</td>
<td>group ID</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>#id#</td>
<td>machine ID</td>
</tr>
<tr>
<td>&lt;lpm&gt;</td>
<td>#lpm#</td>
<td>Log file set criteria</td>
</tr>
<tr>
<td>&lt;lpn&gt;</td>
<td>#lpn#</td>
<td>Log parser set name</td>
</tr>
<tr>
<td>&lt;lsn&gt;</td>
<td>#lsn#</td>
<td>Log file set name</td>
</tr>
</tbody>
</table>

Fig. 6.35 below shows the generic view of the Parser Summary page. The options supported by this page are listed and explained below.

1. Create Alarm: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. Create Ticket: If checked and an alarm condition is encountered, a ticket is created.

3. Email Recipients: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

   • The email address of the currently logged on user displays in the Email Recipients field. It
defaults from **System > Preferences**.

- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.

- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

- If **Remove** is clicked, all email addresses are removed without modifying any alert parameters.

- Email is sent directly from the KServer to the email address specified in the alert. Set the **From Address** using **System > Outbound Email**.

4. **Apply**: Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

5. **Clear All**: Clears all monitor sets assigned to selected machine IDs.

6. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

7. **Log Set Names**: Lists the names of parser sets assigned to this machine ID.

8. **ATSE**: The ATSE response code assigned to machine IDs:
   - A = Create Alarm
   - T = Create Ticket
   - S = Run Procedure
   - E = Email Recipients

9. **Email Address**: A comma separated list of email addresses where notifications are sent.

### 6.7.2 Log Parser

The **Log Parser** page defines log parsers and assigns them to selected machine IDs.

---

**Note**: The log parsers are only active if they are subsequently assigned a log parser set using **Assign Parser Sets**.

---

**Log Monitoring**

The VSA is capable of monitoring data collected from many standard log files. **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and syslog files created for Unix, Linux, and Macintosh operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the KServer database, **Log Monitoring** uses parser definitions and parser sets to parse each log file and select only the data you’re interested in.

**Log Monitoring Setup**

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.

2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific
values stored in the parameters. Activate parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.

3. **Parser Summary** - Quickly copy active parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

### The Log File Parsing Cycle

The parsing of a log file is triggered whenever the log file is changed. In most cases this involves appending new text to the end of the file. To avoid scanning the entire log file from the beginning each time the file is updated, the agent parses log files as follows:

- After each update the agent stores a “bookmark” of the last 512 bytes of a log file.
- When the log file is updated again, the agent compares the bookmark from the old update with the same byte position in the new update.
- Since log files may be archived before the log parser is run, parsing can include archives files if they exist.
- You can specify sets of log files and sets of archive files by specifying full pathnames with asterisk (*) and question mark (?) wildcards. If a set of files is specified the parser begins with the latest file in the set.
- If the bookmark text is the same in both the old update and the new update, the agent begins parsing text after the bookmark.
- If the bookmark text is not the same and no Log Archive Path is specified, the agent parses the entire log file from the beginning. If a Log Archive Path is specified, the agent searches for the bookmark in the archive files. If the bookmark cannot be found, the agent bookmarks the end of the log file and starts parsing from there in the next cycle.
- Once parsing is completed a new bookmark is defined based on the last 512 bytes of the newly updated log file and the process repeats itself.

**Note:** The parsing of a log file is not a procedure event itself. Only a new configuration, or reconfiguration, using Log Parser, Assign Parser Sets or Parser Summary generates a procedure you can see in the Procedure History or Pending Procedure tabs of the Machine Summary page.

Fig. 6.36 below shows the generic view of the Log Parser page. The functions supported on this page are listed and explained below.
4. **New**: Select `<Select Log Parser>` in the Log File Parser drop-down list and click New to create a new log parser.

5. **Edit**: Select an existing log parser in the Log File Parser drop-down list and click Edit to edit the log parser.

6. **Apply**: Click Apply to assign a selected log parser to selected machine IDs.

7. **Clear**: Click Clear to remove a selected log parser from selected machine IDs.

8. **Clear All**: Click Clear All to remove all log parsers from selected machine IDs.

9. **Add Log Parser / Replace Log Parsers**: Select Add Log Parser to add a log parser to existing machine IDs. Select Replace Log Parsers to add a log parser and remove all other log parsers from selected machine IDs.

### 6.7.3 Assign Parser Sets

The **Assign Parser Sets** page creates and edits parser sets and assigns parsers sets to machine IDs. Optionally triggers an alert based on a parser set assignment. A machine ID only displays in the paging area if:

- That machine ID has been previously assigned a log file parser definition using
- That same log file parser definition Monitor > Log Parser is selected in the Select Log File Parser drop-down list.

**Note**: Assigning a parser set to a machine ID on this page activates the log parser. Parsing occurs whenever the log file being parsed is updated.

**Notification**

The agent collects log entries and creates an entry in the log monitoring log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked*. You don’t have to be notified each time a new log monitoring entry is created. You can simply review the Log Monitoring log periodically at your convenience.

**Parser Definitions and Parser Sets**

When configuring Log Monitoring it’s helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A parser definition is used to:

- Locate the log file being parsed.
- Select log data based on the log data’s format, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in Log Monitoring.

A parser set subsequently filters the selected data. Based on the values of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts. Without the filtering performed by the parser set, the KServer database would quickly expand. For example a log file parameter called `$FileServerCapacity$` might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in Log Monitoring, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

**Fig. 6.37** below shows the generic view of the Assign Parser sets. The functions supported on this page are...
1. **Create Alarm**: If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

2. **Create Ticket**: If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script**: If checked and an alarm condition is encountered and an agent procedure is run. *Select agent procedure* link must be selected to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients**: If checked and an alarm condition is encountered, an email is sent to the specified email addresses.
   - The email address of the currently logged on user displays in the *Email Recipients* field. It defaults from *System > Preferences*.
   - If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
   - If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
   - If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.
   - Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using *System > Outbound Email*.

5. **Select Log File Parser**: Select a log parser from the *Select log file parser* drop-down list to display all machine IDs previously assigned this log parser using the Log Parser page.

6. **Define log sets to match**: After a log parser is selected, click *Edit* to define a new parser set or select an existing parser set from the Define log sets to match drop-down list.

7. **Alert when**: Specify the *frequency* of the parser set condition required to trigger an alert:
• Alert when this event occurs once
• Alert when this event occurs <N> times within <N> <periods>
• Alert when this event doesn’t occur within <N> <periods>
• Ignore additional alarms for <N> <periods>

8. **Add / Replace**: Click the *Add or Replace* radio options, then click *Apply* to assign a selected parser set to selected machine IDs.

9. **Remove**: Click *Remove* to remove all parser sets from selected machine IDs.

10. **Apply**: Applies the selected parser set to checked machine IDs.

11. **Clear**: Clears the assignment of a selected parser set from selected machine IDs.

12. **Clear All**: Clears all parser sets assigned to selected machine IDs.