Kaseya

Kaseya 2

Standard Solution Package

User Guide

Version R8

English

September 19, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

C h a p t e r   1

Introduction

In This Chapter

Overview

The **Standard Solution Package** is a set of data objects—collectively called **content**—preloaded into the VSA. Kaseya has defined this content to reflect best-practice solutions for managing machines within a customer environment. The content, along with documentation and methodologies, is designed to help Kaseya administrators rapidly and consistently apply a standard set of recommended configuration solutions immediately after agents have been deployed.

Features & Capabilities

The features and capabilities encompass product Usability Enhancements, Auditing & Inventory, Remote Support, Patch Management, Monitoring & Alerting, Policies, Automation, Reporting, and more.

Modules Supported

This package is designed with content and support for the Kaseya K2 (v6.3) core modules/features such as System, Agent, Audit, Remote Control (including LiveConnect), Patch Management, Monitoring, Agent Procedures, Info Center, Views, and Policy Management.

Supported OS Platforms and Software

Agent OS Platforms Supported

This package provides content and support for the following OS platforms on agent machines.

- Microsoft Windows XP, 2003, 2003 R2, Vista, 2008, 2008 R2, 7, 2012
- Apple Macintosh Mac OS X 10.5 (Leopard), 10.6 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion)
- SuSE Linux Enterprise 10 and 11, Red Hat Enterprise Linux 5 and 6, Ubuntu 8.04 and higher, and OpenSuSE 11, CentOS 5 & 6

3rd Party Systems Supported

The ITSM-SS is designed with content and support for the following 3rd Party systems and applications.

- Email/Messaging
  - Exchange 2003, 2007, 2010, SMTP, IMAP, POP3, Blackberry Enterprise Server
- AntiVirus/AntiMalware
  - Symantec AntiVirus v10, Corporate Edition v10, Endpoint Protection v11
  - McAfee VirusScan/Enterprise, Total Protection, Endpoint Protection
  - Sophos AntiVirus
  - Trend Micro OfficeScan v10, Worry-Free Business Security v11
  - AVG Technoligies AntiVirus v8
  - Kaspersky Endpoint Security v8
  - Microsoft Security Essentials, Forefront Endpoint Protection
  - Microsoft Security Center Integrated 3rd Party AV/AM Products
- Backup/Recovery
  - Symantec Backup Exec v10/11/12/12.5/2010/2012
  - Computer Associates BrightStor ARCServe Backup r11.1/11.5/12/12.5/15
- Database Servers
  - Microsoft SQL Server 2005/2008/2008 R2

- Remote Access
  - Terminal Server, Citrix MetaFrame/Presentation Server/XenApp
- Network Infrastructure
  - Microsoft Active Directory, File & Print, DHCP Server, DNS Server, FTP Server
- Web Servers
  - Microsoft IIS 6/7, SharePoint Server 2007/2010

Package Summary

The **Standard Solution Package** of content is preloaded automatically into the VSA. Some types of content are organized by **System cabinet** in a data object tree. These include:

- **Policies** - Policy Management > Policies
- **Agent Procedures** - Agent Procedures > Create / Schedule
- **Monitor Sets** - Monitor > Monitor Sets

Other types of content display in dedicated drop-down lists:

- **Views** - A list of predefined *views* with a `zz[SYS]` prefix is displayed by selecting the **View** drop-down list at the top of any machine page displaying the machine ID / group ID filter.
- **Patch Management Policies** - A list of predefined *patch management approval and denial policies* with a `zz[SYS]` prefix displays by selecting the **Patch Management > Approval by Policy > Policy** drop-down list.
- **Event Sets** - A list of predefined *event sets* with a `zz[SYS]` prefix displays by selecting the **Monitor > Event Log Alerts > Define events to match or ignore** drop-down list.

IT Services Focus

The **Standard Solution Package** is targeted towards the delivery of common IT services typically provided by an IT service provider or IT support organization. These common IT services include:

IT Service	Description
Default Configuration	Provides simplified administration of the configuration and provisioning of basic settings and remote support notification policies.
Audit / Inventory	Provides up to date hardware/software inventory data for machines.
Patch / Update Management	Provides patch / update management capabilities to improve stability, reduce vulnerabilities and risks associated with them, and visibility into the patch status of machines.
Routine Maintenance	Provides routine maintenance on machines to keep them operating more efficiently.
Monitoring	Provides continuous monitoring of servers and/or workstations for services, performance data, processes, events, health, and overall availability.
Reporting	Provides reporting capabilities that provide visibility into all aspects of the various IT support services being provided.

Automated and Specialized System Configuration

Content is provided that is commonly applicable to all the machines you manage. The rest of the predefined content represents a catalog of well-known alternative solutions that you might consider applying in specialized circumstances.

- **Automated System Configuration** - Commonly used content can be quickly and automatically configured for a specific organization using the **Systems Management Configuration** setup wizard. Simply follow the steps under the **Systems Management Configuration** *(page 2)* section of this

guide. Content used by the wizard is described in the **Setup Wizard Enabled Content** *(page 15)* section of this guide.

- **Specialized System Configuration** - After you run the **Systems Management Configuration** setup wizard, you can modify the policies applied. You can also select additional or different content or policies and reorganize the initial configuration to suit your business requirements. This customization capability is introduced in the topic **Customizing an Organization's Policies** *(page 10)*. The **Complete Content Catalog** *(page 57)* section of this guide describes the data objects that are available for you to use.

Chapter 2

Systems Management Configuration

In This Chapter

The Setup Wizard

Version 6.3 of the Kaseya **Virtual System Administrator™** introduces the **Systems Management Configuration** setup wizard. The setup wizard enables you to quickly *configure and apply machine management policies for a specific organization.* Once configured, these polices are assigned to each machine you manage on behalf of that organization. Policies govern many different aspects of machine management:

- Audit scheduling
- Monitoring
- Alerts
- Patch Management
- Routine machine maintenance using agent procedures

With policies you no longer have to manage each machine individually. You only have to assign or change the policy. A policy assignment or a change within an assigned policy is propagated within 30 minutes to all member machines without you having to schedule anything. Once applied, you can quickly determine whether managed machines are in compliance or out of compliance with their assigned policies. Compliance tracking by individual policy provides you with the information you need to deliver IT services consistently throughout the organizations you manage.

Note the following before running the **Systems Management Configuration** setup wizard on any organization.

- You can rerun the **Systems Management Configuration** setup wizard to select different options for an organization, provided you haven't customized policy assignments for the same organization in **Policy Management**.
- Running the **Systems Management Configuration** setup wizard means you intend on managing that organization *by policy*. If you modify agent setting *manually* after applying a policy, a "policy override" condition exists. For example, making changes to the agent menu of a machine using the **Agent Menu** page in the **Agent** module sets up an override condition for that agent machine. Overridden **Policy Management** policies will be ignored from then on. An overridden policy can always be cleared using the **Policy Management** module.

Running the Setup Wizard

1. Navigate to the **System > Orgs/Groups/Depts/Staff > Manage** page.
2. Select an organization in the middle pane.
3. Select the **Systems Management** tab.
4. Click the **Configure** button.

> **Note:** In a new VSA with no agents yet installed, you may be prompted by the notification bar to run this same setup wizard for the `myOrg` organization.
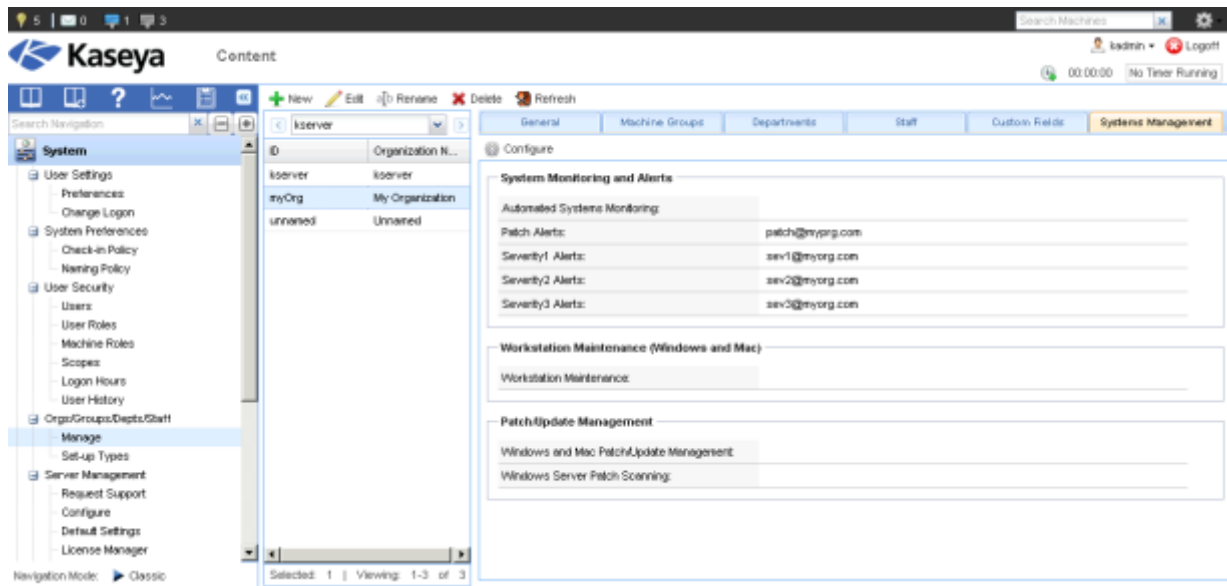
In This Section

Setup Wizard Page 1 - System Monitoring and Alerts

- **Enable Automated Systems Monitoring** – When the system finds an alertable item, it creates an alarm and notifies you by email.
- **Patch Alerts** – The email address for patch alert email notifications only.

  > **Note:** This email address is not used unless the **Patch Management wizard page** *(page 5)* checkboxes are checked.

- **Use Email Address for All Alerts** – Uncheck this checkbox to see three additional *severity alert* fields. Check this box to use the same email address entered in the **Patch Alerts** edit box for all four types of alerts.
  Severity alerts refers to all other alerts *except Patch Alerts.* Different types of alerts are considered more severe than others. An IT organization may have multiple teams, each responding to different levels of alerts.
  - ➢ **Severity 1 Alerts** - The email address for low level alerts.
  - ➢ **Severity 2 Alerts** - The email address for medium level alerts.
 - ➢ **Severity 3 Alerts** - The email address for high level alerts.

> **Note:** To enable multiple organizations to make use of the same built-in, standard policies in **Policy Management**, placeholder **tokens** are entered in policy fields requiring an email address. These token values are `#patchAlertEmail#`, `#sev1AlertEmail#`, `#sev2AlertEmail#`, and `#sev3AlertEmail#`. The VSA automatically replaces a token value in a policy with the appropriate email address for a specific organization when an alert notification is sent out. The organization email addresses referenced by tokens are specified using this wizard page. The **Policy Management** policy categories that include email addresses are **Alerts**, **Monitor Sets** and **Patch Settings**.

Setup Wizard Page 2 - Workstation Maintenance

- **Enable Weekly Workstation Maintenance** – If checked, weekly workstation maintenance routines are run once a week, from Monday through Friday between 6 PM to 6 AM. Applies to Windows and Macintosh workstations only. Does not apply to Linux. This includes:
  - ➢ Disk / file system integrity checks
  - ➢ Disk optimization and defragmentation

➢ Temporary file cleanup
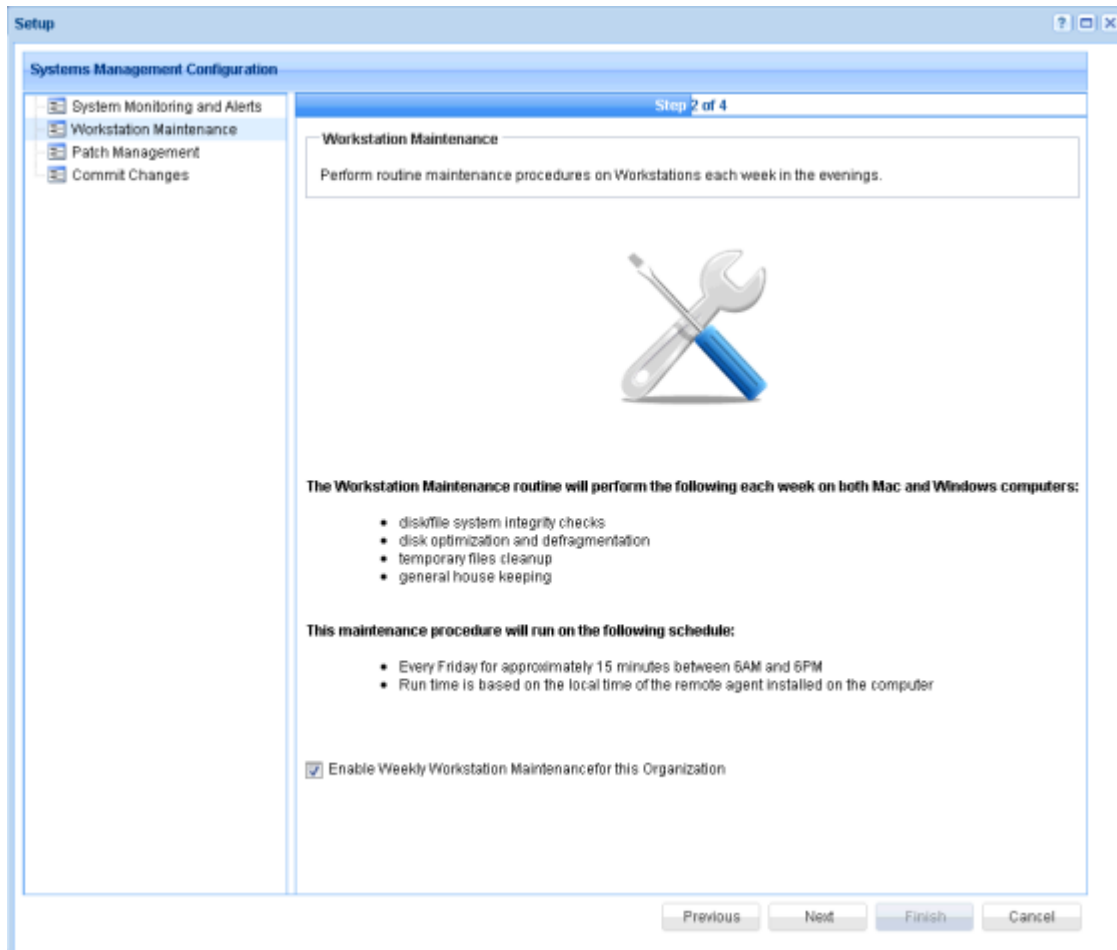
Setup Wizard Page 3 - Patch Management

- **Enable workstation patch and update management** – If checked, all windows workstations will be scanned and patched automatically. If a patch requires a reboot, the user is sent a request every 60 minutes to allow the reboot to proceed.
- **Enable Windows server patch scanning** – All windows servers will be automatically scanned for their current status. No patches will be installed during the process. All server scans occur in the evening. Patching for servers must be performed manually.
- **Patch Management Credentials** – The system will automatically create this administrator account on each computer. This will only affect computers with agents. You can change or delete these credentials at any time.

Note: A credential for this new account is added to the Audit > Manage Credentials page for this organization. The new credential is designated an agent credential, which means it is configured to serve as the agent credential when a **Systems Management Configuration**-enabled policy is run for this organization.

Setup Wizard Page 4 - Configuration Completed

After you click the Finish button a message box confirms your request is being processed and will take up to 5 minutes. Policies for this organization will be created and applied to systems with agents that belong to this organization.
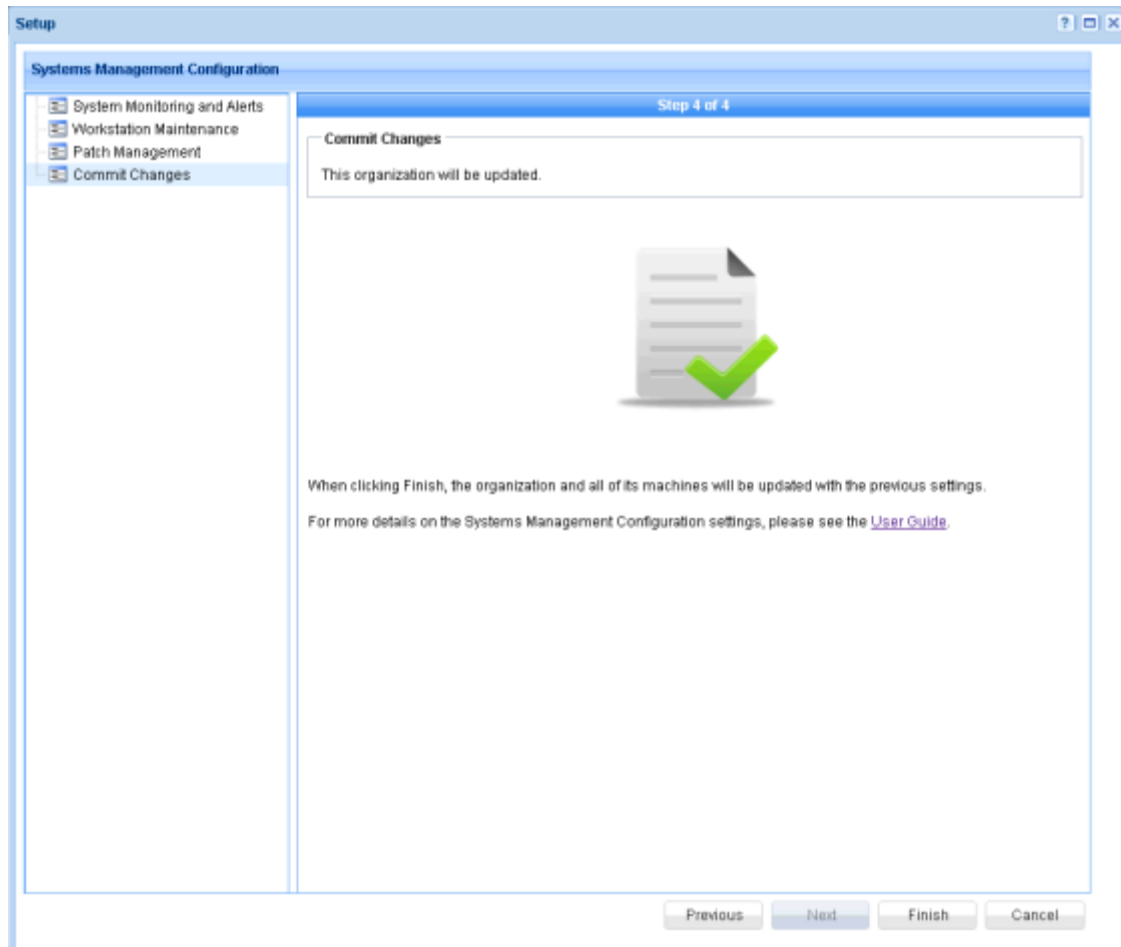
Confirmation on the System Management Tab

When the **Systems Management Configuration** setup wizard closes it may take up to 5 minutes for policies to be applied to managed machines in the organization you selected. Only then will you see green checkboxes on the **System Management** tab confirming options you elected to use have been applied. Applied policies may then take 30 minutes or more to propagate to managed machines in that organization.
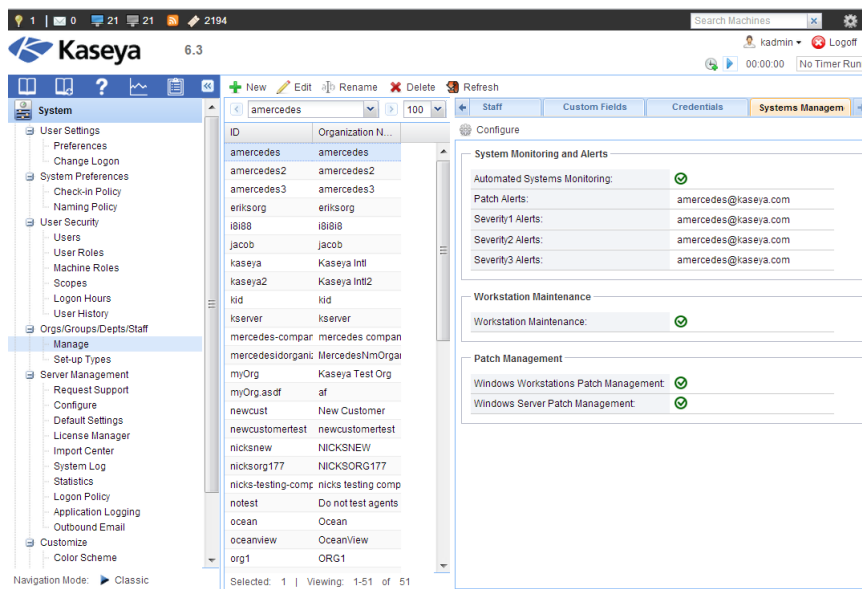
Deploying Agents

At this point the only task left to do is to add managed machines to an organization. There are multiple ways to deploy agents.

- **Discovery** - If you already have at least one agent installed on a network, the recommended method for discovering and installing agents is to use the **Discovery module** *(http://help.kaseya.com/webhelp/EN/KDIS/R8/index.asp#7293.htm)*. The notification bar may prompt you to run network discovery when a new network is discovered.
- **Agent Deploy** – If you're deploying your *first* agent to a new network, then use the Agent > **Deploy Agents** *(http://help.kaseya.com/webhelp/EN/VSA/R8/index.asp#491.htm)* page. See the **Agent Deployment** *(http://help.kaseya.com/webhelp/EN/VSA/R8/EN_agentdeployment_R8.pdf#zoom=70&navpanes=0)* quickstart guide for an introduction to installing agents.

Remember, the **Systems Management Configuration** setup wizard only applies policies to the organization you just selected. Ensure the agents you deploy are assigned to this same organization.

How Does It Work?

The Setup Wizard *(page 2)* section only covered how to the use the **Systems Management Configuration** setup wizard. If that's all you need to know, then you can skip this section. But if you're curious about how **Systems Management Configuration** leverages existing VSA functionality, then read on.

In This Section

Prerequisites

1. Ensure you're logged on to the VSA as a *master administrator* in an on premise VSA or as a *system administrator* in a cloud-based VSA. This ensures you have access to the features discussed in this section.

2. Ensure the **Show shared and private folder contents from all users - Master Admin Only** checkbox is checked in **System > User Settings > Preferences**. This additional checkbox provides visibility of the System cabinet folders described in this section.
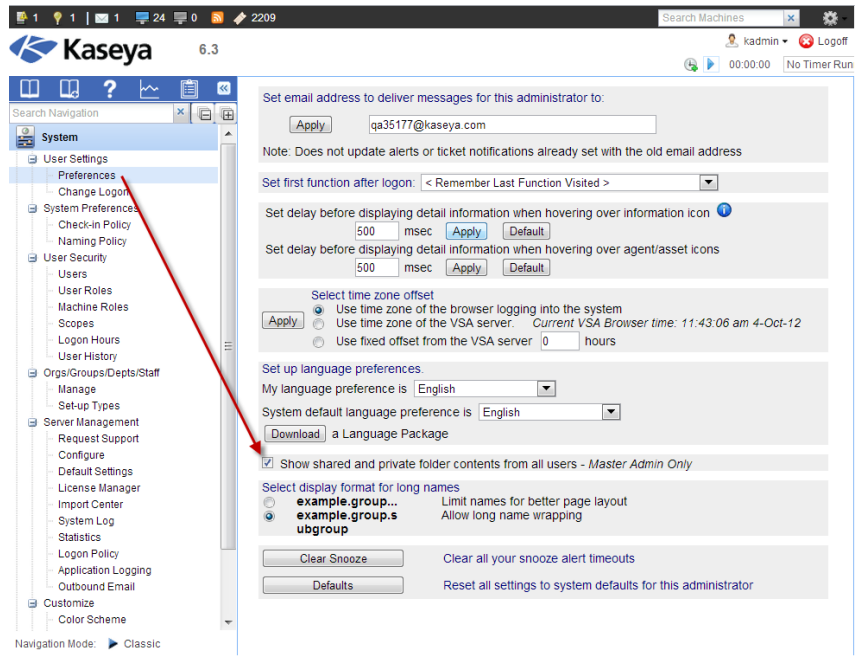
System Policies in Policy Management

The choices made in the **Systems Management Configuration** setup wizard create a list of policies that are applied to the organization you selected. Let's take a look at these policies.

1. Navigate to the **Policy Management** module.

2. Select the **Organizations / Machines Group** page.
3. For the same organization you selected when running the **Systems Management Configuration** setup wizard, expand the folder in the middle pane.
4. Expand the **Systems** cabinet in the right hand pane.
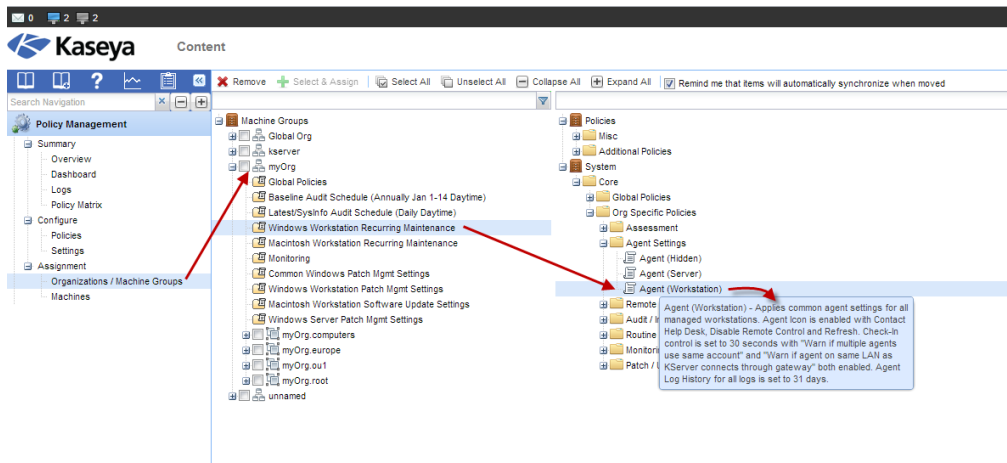
Notice that any folder assigned to your organization has a corresponding folder in the right hand pane. That folder typically contains subfolders and sets of policies in each subfolder. Hover the cursor over any specific policy to see the description for this pre-defined policy. Each managed machine in the selected organization is now managed by this policy, along with all the other policies assigned to this organization.

Customizing an Organization's Policies

Even without knowing how policies are configured in detail, you can begin to customize the policies that are assigned to a specific organization.

Using the **Policy Management > Organizations / Machines Group** page, you can customize the policies assigned to an organization by manually dragging and dropping folders or policies to and from the organization tree. This includes removing System cabinet policies from an organization if you like. Note that **policy assignment rules** *(http://help.kaseya.com/webhelp/EN/KPM/R8/index.asp#8140.htm)* apply to the sequencing of policies listed below an organization.

Additional policies and folders can be dragged and dropped from either the Systems cabinet or the Policies cabinet. System cabinet policies cannot be modified, but there are more System cabinet policies available than those that can be selected using the **Systems Management Configuration** setup wizard. Before you attempt to create your own user-defined policies be sure to review the System cabinet policies available. The complete set of System cabinet policies are described in the **Setup Wizard Enabled Content** *(page 15)* section of this document. If you would like to know more about how a policy is constructed see the **Policy Details** *(page 11)* topic.
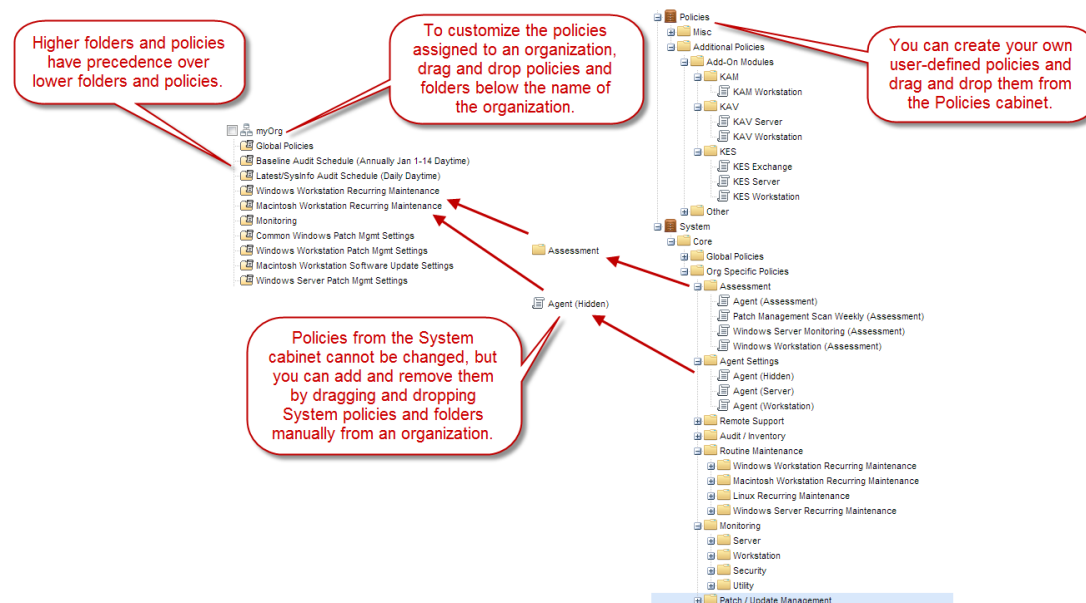
Policy Details

> **Note:** The next three topics describe in summary fashion how a policy is constructed. For more information about policies, consult the **Policy Management** online help and user guide *(http://help.kaseya.com/webhelp/EN/KPM/R8/index.asp#8410.htm)*.

The details of each policy—whether a System policy or a user-defined policy—can be inspected using the **Policies** page. A new policy can optionally include many different setting categories. For example, a single policy could set agent check-in properties, set an audit schedule and run agent procedures all at the same time.

The image below shows a partial list of the setting categories available to use when creating a new policy.
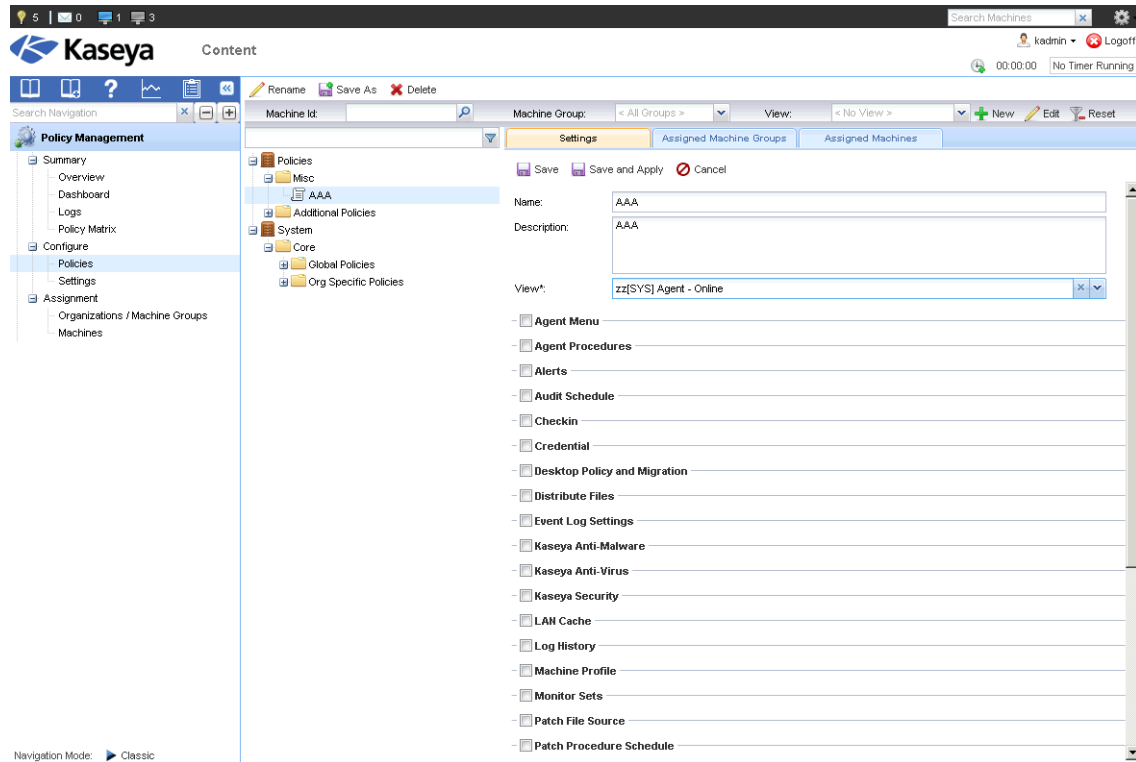
Built-in Settings vs Data-Specific Settings

When you review or configure policy settings in a specific policy, you'll notice two kinds of settings:

- **Built-in Settings** - These policy settings are usually checkboxes or radio options. They assign the setting to a managed machine and that's all you need to specify in the policy.
- **Data-Specific Settings** - These policy settings specify a *data object that exists elsewhere in the VSA*. Either that data object is part of the standard content that was preloaded into the VSA, or it's a data object that another VSA user created and is using with the policy.

For example, in the image below, a predefined System policy shows the "reboot" policy for a machine after patch updates have been applied. This is a *built-in setting* that does not require you to specify any other data object. The next topic discusses *data-specific settings*.
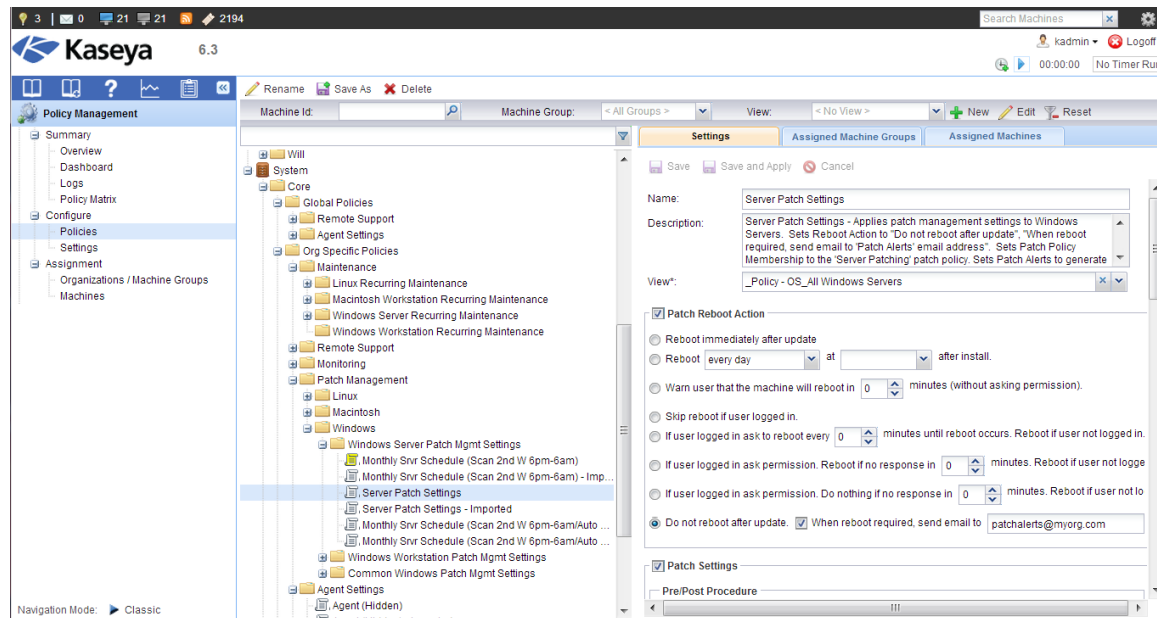
Linking Policies to Data Objects

Setting a data-specific setting in a policy requires specifying a data object in another part of the VSA.

Recall that the System cabinet policies in **Policy Management** are just one type of *standard content* that is preloaded into the VSA. Other types of content include:

- Views
- Patch Policies
- Event Sets
- Monitor Sets
- Agent Procedures

Much of the automated solutions provided by the **Systems Management Configuration** setup wizard is enabled by linking predefined System policies to these other types of predefined System data objects.

For example, in the image below we see details of a System cabinet policy called **Windows Workstation Maintenance (Weekly M-F 6pm-6am)**.

- This policy schedules the weekly running of an agent procedure called **Workstation Weekly Maintenance**.

- Also notice this same policy is restricted to machines belonging to the view **zz[SYS] Policy - OS_All Windows Workstations**.
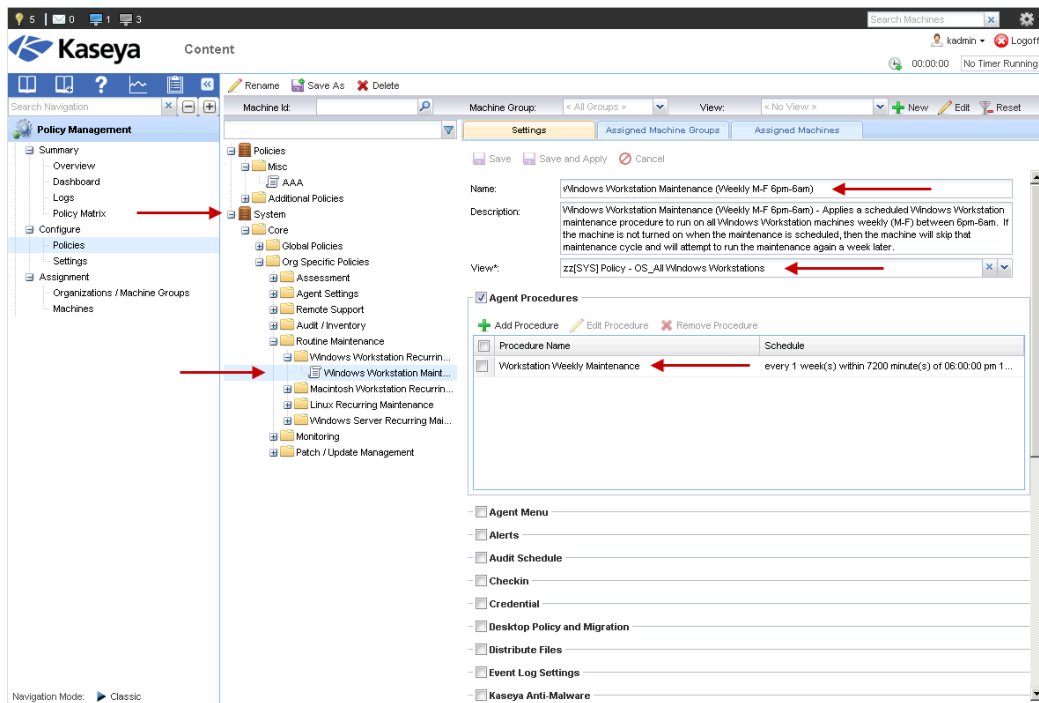
This is just one example of how System policies are linked to System content elsewhere in the VSA. Use this same method to examine the settings and links of any other policy. Except for the fact that you can't modify System policies and content, keep in mind there is nothing unique about how they are configured. When you're ready to try it yourself, create your own user-defined policies and content and link them together just as you see here. If you like, you can make a copy of a System policy using the **Save As** button and begin your customization from there.

Note: For more information about policies, consult the **Policy Management** online help and user guide *(http://help.kaseya.com/webhelp/EN/KPM/R8/index.asp#8410.htm)*.

Chapter 3

Setup Wizard Enabled Content

The following topics summarize the capabilities of content developed for use with   the **Systems Management Configuration** setup wizard. This same content can be used manually without the wizard.

In This Chapter

Default Configuration

Goal

Provide simplified administration of the configuration and provisioning of basic settings and remote support notification policies.

Overview

Kaseya agents have an array of configuration settings that should be managed consistently across all managed machines such as the Agent Menu, Check-in Control, Working Directory, Set Credential, Log History, Event Log Settings, and Remote Control Notification Policies. Default Agent Configuration addresses the need for consistent management across all systems for these basic system wide configuration settings.

Policies

A set of Policies is provided that apply default agent configuration settings across all machines within the supported IT infrastructure. These policies control such settings as the Agent Menu, Check-in Control, Working Directory, Set Credential, Log History, Event Log Settings, and Remote Control Notification Policies based on a general operations best practices system configuration use case. The policies are located under **[System].Core.Global Policies**, and are described below.

- **Agent Settings**
  - **Agent (Core)** - Applies common agent settings for all managed machines. Agent Icon is enabled but only Refresh option is enabled. Check-In control is set to 30 seconds with "Warn if multiple agents use same account" and "Warn if agent on same LAN as KServer connects through gateway" both enabled. Agent Log History for all logs is set to 31 days.
  - **Windows Agent** - Applies agent settings specific to Windows. Sets Agent Working Directory to c:\kworking.
  - **Linux Agent** - Applies agent settings specific to Linux. Sets Agent Working Directory to /tmp/kworking.
  - **Macintosh Agent** - Applies agent settings specific to Macintosh Workstations. Sets Agent Working Directory to /Library/kworking.
- **Remote Support**
  - **Server RC Notification Policy (Silent w Admin Note)** - Applies Remote Control notification settings for all servers. Sets user notification type to Silently take control, and enables the Require admin note to start remote control option.
  - **Workstation RC Notification Policy (Alert/Term w Admin Note)** - Applies Remote Control notification settings for all workstations. Sets user notification type to If user logged in display alert, Notify user when session terminates, and enables the Require admin note to start remote control option.

Audit / Inventory

Goal

Provide a routine audit/inventory strategy to support hardware and software asset visibility for long term planning, compliance, short and long term projects, decision support, and troubleshooting.

Overview

Kaseya supports multiple types of agent based audits to detect both hardware and software deployed within an IT infrastructure. These can be broken down into Latest, Baseline and System Info audits.

Latest audits incrementally update current hardware and software information about machines. Baseline audits provide a point in time picture of the hardware and software information about machines. System Info audits provide additional detail on hardware using SMBIOS. In order to keep available information about machines up to date so that strategic and tactical decisions can be made, it is important to schedule these audits to run in some regularly recurring pattern. With this audit information there must be easy ways to locate specific types of systems based on the detailed inventory data known about them and there must be ways of reporting and effectively acting on these groups of machines if needed.

Policies

A set of Policies is provided that apply recurring Audits to be scheduled across all machines within the supported IT infrastructure. These policies enable the collection of information critical to the Audit/Inventory service use case. The policies are located under **[System].Core.Org Specific Policies.Audit / Inventory**, and are described below.

- **Baseline.Baseline Audit Schedule (Annually Jan 1-14 Daytime)**

  - **Baseline Audit Schedule (Annually Jan 1-14 6am-6pm/Power Mgmt)** - Applies a scheduled Annual Baseline Audit for all machines that have been deployed and have checked in beginning on January 1st through the 14th between 6am-6pm. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where annual audits may be required for planning or compliancy purposes and so that for relevant Baseline/Latest Audit comparisons can be performed for operational tasks. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

- **Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)**

  - **Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt)** - Applies scheduled Latest and System Info Audits for all machines that have checked in to run daily (M-F) between 6am-6pm. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where customers need to run audits during business hours on weekdays because machines are generally turned off at night and on weekends. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

Views

A set of predefined Views is provided which can be used in all aspects of IT service management and in support of the Audit / Inventory service. These Views provide the ability to filter machines across the system based on their hardware, software, and role. The following Views can be used on both reporting and operational activities.

View Name	Description
zz[SYS] HW - Dell	Displays all machines with Dell as manufacturer
zz[SYS] HW - Dell PowerEdge	Displays all machines with Dell as manufacturer and PowerEdge in product name
zz[SYS] HW - HP	Displays all machines with HP or Hewlett Packard as manufacturer
zz[SYS] HW - HP ProLiant	Displays all machines with HP or Hewlett Packard as manufacturer and ProLiant in product name
zz[SYS] HW - IBM	Displays all machines with IBM as manufacturer
zz[SYS] HW - IBM Series X	Displays all machines with IBM as manufacturer and Series X in product name
zz[SYS] HW - Lenovo	Displays all machines with Lenovo as manufacturer
zz[SYS] HW - Not Portable	Displays all machines that are not mobile
zz[SYS] HW - Portable	Displays all machines that are mobile (i.e. chassis type = notebook or laptop or portable or tablet pc or hand-held or sub-notebook or

	netbook)
zz[SYS] HW - Under 1GB Memory	Displays all machines that have less than 1GB of memory
zz[SYS] HW - Under 512MB Memory	Displays all machines that have less than 512MB of memory
zz[SYS] HW - Virtual Guest	Displays all machines that are Virtualized computers (VMWare, XenServer, VirtualBox or HyperV guests)
zz[SYS] Network - 10.11.12.x	Displays agents of specific 10.11.12.x network
zz[SYS] OS - All Linux	Displays all Linux machines
zz[SYS] OS - All Mac OS X	Displays all Mac OS X machines
zz[SYS] OS - All Mac OS X Servers	Displays all Mac OS X Server machines
zz[SYS] OS - All Mac OS X Workstations	Displays all Mac OS X Workstation machines
zz[SYS] OS - All Servers	Displays all machines running a Server class Operating System
zz[SYS] OS - All Windows	Displays all Windows machines
zz[SYS] OS - All Windows SBS	Displays all Windows SBS Server machines
zz[SYS] OS - All Windows Servers	Displays all Windows Server machines
zz[SYS] OS - All Windows Workstations	Displays all Windows Workstation machines
zz[SYS] OS - All Workstations	Displays all machines running a Workstation class Operating System
zz[SYS] OS - Mac OS X 10.5 Leopard	Displays all Mac OS X v10.5 machines
zz[SYS] OS - Mac OS X 10.6 Snow Leopard	Displays all Mac OS X v10.6 machines
zz[SYS] OS - Mac OS X 10.7 Lion	Displays all Mac OS X v10.7 machines
zz[SYS] OS - Mac OS X 10.8 Mountain Lion	Displays all Mac OS X v10.8 machines
zz[SYS] OS - Win 2003 SBS	Displays all machines running a Windows 2003 Small Business Server Operating System
zz[SYS] OS - Win 2003 Server	Displays all machines running a Windows 2003 Server Operating System
zz[SYS] OS - Win 2008 R2 Server	Displays all machines running a Windows 2008 Server R2 Operating System
zz[SYS] OS - Win 2008 SBS	Displays all machines running a Windows 2008 Small Business Server Operating System
zz[SYS] OS - Win 2008 Server	Displays all machines running a Windows 2008 Server Operating System
zz[SYS] OS - Win 2012 Server	Displays all machines running a Windows 2012 Server Operating System
zz[SYS] OS - Win 7	Displays all machines running a Windows 7 Operating System
zz[SYS] OS - Win Vista	Displays all machines running a Windows Vista Operating System
zz[SYS] OS - Win XP	Displays all machines running a Windows XP Operating System
zz[SYS] Role - BackupExec Server	Displays all BackupExec Servers
zz[SYS] Role - Blackberry Server	Displays all Blackberry Enterprise Servers
zz[SYS] Role - BrightStor ARCserve Server	Displays all BrightStor ARCserve Servers
zz[SYS] Role - Citrix Server	Displays all Citrix Servers
zz[SYS] Role - DHCP Server	Displays all MS DHCP Servers
zz[SYS] Role - DNS Server	Displays all MS DNS Servers
zz[SYS] Role - Domain Controller	Displays all MS AD Domain Controller Servers
zz[SYS] Role - Exchange 2003 Server	Displays all MS Exchange 2003 Servers
zz[SYS] Role - Exchange 2007 Server	Displays all MS Exchange 2007 Servers
zz[SYS] Role - Exchange 2010 Server	Displays all MS Exchange 2010 Servers

zz[SYS] Role - Exchange Server	Displays all MS Exchange Servers
zz[SYS] Role - File Server	Displays all MS File Servers with non-admin file share(s)
zz[SYS] Role - FTP Server	Displays all MS FTP Servers
zz[SYS] Role - IIS Server	Displays all MS IIS Servers
zz[SYS] Role - IMAP4 Server	Displays all MS IMAP4 Servers
zz[SYS] Role - POP3 Server	Displays all MS POP3 Servers
zz[SYS] Role - Print Server	Displays all MS Print Servers with non-admin file share(s)
zz[SYS] Role - SharePoint Server	Displays all MS SharePoint Servers
zz[SYS] Role - SMTP Server	Displays all MS SMTP Servers that are not also MS Exchange Servers
zz[SYS] Role - SQL Server	Displays all MS SQL Servers
zz[SYS] Role - SQL Server (Default Instance)	Displays all MS SQL Servers setup with the default instance
zz[SYS] Role - SQL Server 2005	Displays all MS SQL 2005 Servers
zz[SYS] Role - SQL Server 2008	Displays all MS SQL 2008 Servers
zz[SYS] Role - Terminal Server	Displays all MS Terminal Servers in Application Mode
zz[SYS] Role - WINS Server	Displays all MS WINS Servers

Patch / Update Management

Goal

Provide a routine patch / update management strategy for managed machines to include scanning and patching, patch approval policies, control over patching behavior and visibility of patch status/compliance for decision support and troubleshooting.

Overview

Kaseya Patch Management supports Microsoft Windows patching only. A machines patch status is detected through a Patch Scan, and patch deployment is accomplished through either Automatic Update, Initial Update, Machine Update or Patch Update scheduling. A Patch Scan detects patches that are missing and installed on a machine and so that decisions about how to proceed with the patching strategy can be made. Patches that are detected by a Patch Scan are presented in an array of Patch Policies which can then be used to control which patches are approved to be deployed to machines. Automatic Updates deploys approved patches to machines on a schedule and based on their Patch Policy membership. Initial Updates, Machine Updates, and Patch Updates provide one-off or manual scheduling capabilities to the overall patch strategy. To keep available patch status information about machines up to date so that deployment and approval decisions can be made related to patch, it is important to schedule the Patch Scans audits in some regularly recurring pattern. The deployment of patches on a regular basis is also critical to the goals of Patch Management, so scheduling Automatic Updates to take place is also important. Using the Patch Management content these recurring tasks can be scheduled. The Patch Management content also includes a set of Patch Policies to which different machines can be assigned either automatically or manually. With this Patch Management strategy, there must be easy ways to locate specific systems based on the details of patches installed and/or missing, quantity of missing patches, machines in certain Patch Policies and there must be ways of reporting and effectively acting on these groups of machines if needed. Additional content provided with the package offer some basic support for Macintosh Software Updates, and Linux Package Updates/Upgrades.

Policies

A set of Policies that apply recurring Patch Scan and Automatic Update schedules across the Windows machines supported within the IT infrastructure is provided. These policies enable the recurring detection of patches that are installed and missing across all machines as well as the scheduling of deployment of approved patches. Policies are also included to assign Windows servers and workstations to the appropriate Patch Policies and to support not patching certain machines or setting up a test group for deploying patches prior to a general approval and deployment of new patches. An additional policy that applies recurring Macintosh Software Update schedules across the Macintosh machines supported within the IT infrastructure is provided.

The policies included are located under **[System].Core.Org Specific Policies.Patch / Update Management**, and are described below.

- **Windows.Common Windows Patch Mgmt Settings**
  - **Deny Patch Settings -** Applies patch management settings to machines selected in the 'zz[SYS] Policy - Patch_Deny Patching Group' View. Sets Reboot Action to "Do not reboot after update". Sets Patch Policy membership to the 'Deny Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".
  - **Test Patch Settings -** Applies patch management settings to machines selected in the 'zz[SYS] Policy - Patch_Test Patching Group' View. Sets Reboot Action to "If user logged in ask to reboot every 60 minutes until reboot occurs. Reboot if user not logged in". Sets Patch Policy membership to the 'Test Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".
  - **Disable Windows Automatic Update** - Disables Windows Automatic Updates on machines that have Windows Automatic Update Enabled. If Windows Automatic Update is enabled and Kaseya Patch management is being used, then Windows Automatic Update may conflict with the Kaseya patch management strategy and may result in the deployment of patches that have been denied or are still pending approval in Kaseya.
  - **File Source Internet** - Sets the File Source for patch management to the Internet for all Windows machines so that patches are downloaded directly from the Microsoft patch and download servers. This policy is the default and can be overridden with an alternate policy that is applied to specific orgs or machine groups and which has precedence over this policy.
- **Windows.Windows Workstation Patch Mgmt Settings**
  - **Workstation Patch Settings** - Applies patch management settings to Windows Workstations. Sets Reboot Action to "If user logged in ask to reboot every 60 minutes until reboot occurs. Reboot if user not logged in". Sets Patch Policy Membership to the 'Workstation Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".
  - **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt)** - Applies Daily Auto Update schedules to Workstation Patching Policy members that are missing 10 or more approved patches. Auto Updates are scheduled M-F each week from 6am-6pm. This policy is generally used when customers have machines that are missing quite a few patches and they want to get those systems up to date over the course of days rather than weeks or months. Once the machines are patched, then they will not need to be patched on a daily basis anymore. Auto Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.
  - **Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt)** - Applies Weekly Patch Scan and Auto Update schedules to Workstation Patching Policy members. Patch Scans are scheduled on Tue of each week from 6am-6pm and Auto Updates are scheduled on Wed of each week from 6am-6pm. This policy is generally used when customers want to take a more aggressive approach to patching to help minimize risk due to machines not

being patched and thus want new patches deployed relatively quickly to machines. Auto Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

- **Windows.Windows Server Patch Mgmt Settings**
  - ➢ **Server Patch Settings** - Applies patch management settings to Windows Servers. Sets Reboot Action to "Do not reboot after update", "When reboot required, send email to 'Patch Alerts' email address". Sets Patch Policy Membership to the 'Server Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".
  - ➢ **Weekly Srvr Schedule (Scan W 6pm-6am)** - Applies Patch Scan schedule to Server Patch Policy members. Patch Scans are scheduled on Wed of each week from 6pm-6am. No patch Auto Update deployments are scheduled on servers by this policy.
- **Macintosh.Macintosh Workstation Software Update Settings**
  - ➢ **Weekly Macintosh Workstation Software Update (Install Recommended W 6pm-6am)** - Applies a Mac Software Update to run on Wed of every week that will install recommended Macintosh Software updates on Macintosh Workstations. Software Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

Patch Approval/Denial Policies

> **Note:** Patch approval/denial "policies" are a specialized type of policy in the Patch Management module that should not be confused with policies defined using **Policy Management** module. **Policy Management** policies have been created that specify predefined patch approval/denial policies.

A set of predefined Patch Policies is provided to control approval and denial of various Windows patches applicable to the supported Microsoft software and Windows operating systems.

Patch Policy Name	Description
zz[SYS] Deny Patching	Used for denying all patches in cases where machines must not be patched for particular reasons. The Default Approval Status for new patches of all Microsoft Security Classifications is set to Denied. See Managing Patch Policy Memberships for more information on how machines can be assigned to this Patch Policy.
zz[SYS] Server Patching	Used for approving and denying patches for Windows Servers. The Default Approval Status for new patches of all Microsoft Security Classifications is set to Pending Approval. All Windows Servers are made a member of this Patch Policy when Server Patch Management is enabled through Automated Systems Management.
zz[SYS] Test Patching	Used for approving and denying patches for machines that are to be used for testing patches prior to general deployment to Windows Servers and Workstations. The Default Approval Status for new High Priority Security and Critical Updates based on their Microsoft Security Classifications is set to Approved. All Windows Servers are made a member of this Patch Policy when Server Patch Management is enabled through Automated Systems Management. See Managing Patch Policy Memberships for more information on how machines can be assigned to this Patch Policy.
zz[SYS] Workstation Patching	Used for approving and denying patches for Windows Workstations. The Default Approval Status for new High Priority Security and Critical Updates based on their Microsoft Security Classifications is set to Approved. All Windows Workstations are made a member of this Patch Policy when Workstation Patch Management is enabled through Automated Systems

	Management.

Views

An array of predefined Views is provided which can be used in all aspects of IT service management and in support of the Patch /Update Management service. These Views provide the ability to filter machines across the system based on their patch configuration, quantity of patches missing, patch reboot status, and patch policy membership, and more. The following Views can be used on both reporting and operational activities.

View Name	Description
zz[SYS] Patch - Deny Patching Policy	Displays all machines assigned as members to the "zz[SYS] - Deny Patching" patch policy.
zz[SYS] Patch - Missing 10+ Approved Patches	Displays all machines that are missing 10 or more approved patches based on the machines patch policy memberships and and the approved patches within those policies.
zz[SYS] Patch - Missing 20+ Approved Patches	Displays all machines that are missing 20 or more approved patches based on the machines patch policy memberships and and the approved patches within those policies.
zz[SYS] Patch - No Policy	Displays all machines that are not assigned to any patch policy
zz[SYS] Patch - Pending Reboot	Displays all machines with a pending patch deployment related reboot
zz[SYS] Patch - Scan Failed	Displays all machines where the last patch scan failed for some reason
zz[SYS] Patch - Scan Not Scheduled	Displays all machines that do not have a patch scan scheduled
zz[SYS] Patch - Server Patching Policy	Displays all machines that are a member of the "zz[SYS] - Server Patching" patch policy
zz[SYS] Patch - Servers w No Policy	Displays all Server machines that are not assigned to any patch policy
zz[SYS] Patch - Test Patching Policy	Displays all machines that are a member of the "zz[SYS] Test Patching" patch policy.
zz[SYS] Patch - Windows Auto Update Enabled	Displays all machines with Windows Automatic Update Enabled based on what was detected during the last Patch Scan
zz[SYS] Patch - Workstation Patching Policy	Displays all machines that are a member of the "zz[SYS] - Workstation Patching" patch policy
zz[SYS] Patch - Workstations w No Policy	Displays all Workstations machines that are not assigned to any patch policy

Agent Procedures

Agent procedures are provided that perform customized automation in support of the Patch /Update Management IT service. These agent procedures are located under the **System** cabinet of the Agent Procedures > **Schedule / Create** *(http://help.kaseya.com/webhelp/EN/VSA/R8/index.asp#2845.htm)* page.

- **Create Patch Management System Restore Point** - Runs as a pre-procedure for Automatic Updates. Restore points can be used during a recovery in the event that an installed patch/update causes problems.
  - ➢ **Location:** System.Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore.Create Patch Management System Restore Point
  - ➢ **Description:** Uses WMIC to create a System Restore Point called Patch Management. This agent procedure can be called prior to a patch deployment through a Automatic Update Pre-Agent Procedure.
  - ➢ **Run by Policy:** System.Core.Org Specific Policies.Patch/Update Management.Windows Workstation Patch Settings.Workstation Patch Settings

- **Mac Software Update - Install Recommended Updates and Retrieve/Log Results**
    - ➢ **Location:** System.Core.2 Macintosh Procedures.Software Update.Mac Software Update - Install Recommended Updates and Retrieve/Log Results
    - ➢ **Description:** Installs recommended Mac software updates.
    - ➢ **Run by Policy:** System.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings.Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am)

Routine Maintenance

Goal

Provide a routine maintenance strategy for managed machines to include system optimization, and preventative maintenance operations such as disk and temp files cleanup, hard drive analysis, repair and optimization and more. Routine maintenance is vital to help ensure systems run more smoothly and operate at their peak performance potential. Institute a basic automated routine maintenance schedule across supported systems initially focused on workstations but extensible and capable of supporting more advanced maintenance operations over time as well as servers as needed.

Overview

Kaseya automation called Agent Procedures can be used to perform most any automated task on one or many systems on a scheduled basis. Automatic tasks like check disks, disk fragmentation analysis and optimization, volume repairs, house cleaning, clearing caches, temporary files cleanup, log rotation, and more are combined into a powerful routine maintenance solution that is applied to Windows and Macintosh workstations to keep these systems running more smoothly.

Policies

A set of Policies apply recurring Routine Maintenance schedules across Windows and Macintosh workstations. These policies in turn cause Agent Procedures that perform the actual maintenance on each system at regularly scheduled times. The policies included are located under **[System].Core.Org Specific Policies.Routine Maintenance**, and are described below.

- **Windows Workstation Recurring Maintenance**
    - ➢ **Windows Workstation Maintenance (Weekly M-F 6pm-6am)** - Applies a scheduled Windows Workstation maintenance procedure to run on all Windows Workstation machines weekly (M-F) between 6pm-6am. If the machine is not turned on when the maintenance is scheduled, then the machine will skip that maintenance cycle and will attempt to run the maintenance again a week later.
- **Macintosh Workstation Recurring Maintenance**
    - ➢ **Macintosh Workstation Maintenance Schedule (Weekly M-F 6pm-6am)** - Applies a scheduled Macintosh maintenance procedure to run on all Macintosh Workstation machines weekly (M-F) between 6pm-6am. If the machine is not turned on when the maintenance is scheduled, then the machine will skip that maintenance cycle and will attempt to run the maintenance again a week later.

Agent Procedures

A set of Agent Procedures perform various aspects of the maintenance tasks on Windows and Macintosh workstations. These procedures are scheduled via Policy to run on a recurring schedule. The agent procedures included are located under **[System].Core**, and are described below.

- **1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance.Workstation Weekly Maintenance**
    - ➢ **Description:** Executes all the Weekly Desktop Maintenance tasks, schedule this script to run during your maintenance window.

- ➢ **Usage:** Scheduled by Policy Management to run on all Windows Workstations Weekly (M-F) between 6pm-6am via the "Windows Workstation Maintenance (Weekly M-F 6pm-6am)" Policy when when the Workstation Maintenance feature is enabled via Automated Systems Management.

- **Common Maintenance Tasks.System Restore.Create Weekly Desktop Maintenance System Restore Point**
  - ➢ **Description:** Uses WMIC to create a System Restore Point called Weekly Desktop Maintenance. This agent procedure can be called at the beginning of the Workstation Weekly Maintenance Procedure.
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **Common Maintenance Tasks.Flush DNS. Flush DNS Resolver Cache**
  - ➢ **Description:** Flushes and resets the contents of the DNS client resolver cache by performing IPCONFIG /FLUSHDNS
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **Common Maintenance Tasks.IE Files Management. Clear Internet Explorer Temp Files**
  - ➢ **Description:** Clears the Internet Explorer Temporary Files for the currently logged on user.
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **Common Maintenance Tasks.TEMP Files.Clear User TEMP Folder**
  - ➢ **Description:** Deletes all files and folders within and below the logged on users %TEMP% folder that are not currently locked/open by Windows.
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **Common Maintenance Tasks.Disk Cleanup.Windows Disk Cleanup**
  - ➢ **Description:** Sets the "sageset" registry entries for cleanmgr.exe and then executes cleanmgr.exe with the "sagerun" parameter to automatically clean files in the following locations: Active Setup Temp Folder Content Indexer Cleaner Downloaded Program Files Internet Cache Files Memory Dump Files Old ChkDsk Files Recycle Bin Remote Desktop Cache Files Setup Log Files Temporary Files Temporary Offline Files WebClient and WebPublisher Cache.
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **Common Maintenance Tasks.Check Disk.Check Disk System Drive (Schedule at Next Restart)**
  - ➢ **Description:** Executes a CHKDSK command on the system drive. The results of the maintenance are evaluated by the Check Disk Verify script.
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **Common Maintenance Tasks.Defragmentation.Defragment System Drive (Analysis & Prompt User If Reqd)**
  - ➢ **Description:** Performs a defragmentation analysis on the system drive in Windows (usually C:). Defragmentation results are written to the agent procedure log. If a user is logged onto the machine, then the procedure asks them if they want to run a full defragmentation on the drive and performs one if they answer yes.
  - ➢ **Usage:** Called by the Workstation Weekly Maintenance Procedure.

- **2 Macintosh Procedures.Maintenance.Macintosh Weekly Maintenance**
  - ➢ **Description:** Performs a number of routing maintenance tasks on a Macintosh OS X machine.
  - ➢ **Usage:** Scheduled by Policy Management to run on all Macintosh Workstations Weekly (M-F) between 6pm-6am via the "Macintosh Workstation Maintenance Schedule (Weekly M-F 6pm-6am)" Policy when when the Workstation Maintenance feature is enabled via Automated Systems Management.

- **General OS X House Cleaning**
  - ➢ **Description:** Performs system cleaning, removes old log files, "scratch" and "junk" files, clears user and system caches, rotates system and application logs, rebuilds DYLD cache, and rebuilds the Spotlight index.
  - ➢ **Usage:** Called by the Macintosh Weekly Maintenance Procedure.

- **Verify and Repair OS X Disk Volumes**
  - ➢ **Description:** Performs disk verification and repair operations using DISKUTIL.
  - ➢ **Usage:** Called by the Macintosh Weekly Maintenance Procedure.
- **Repair OS X Disk Permissions**
  - ➢ **Description:** Performs a disk repair permissions operation using DISKUTIL.
  - ➢ **Usage:** Called by the Macintosh Weekly Maintenance Procedure.

Monitoring

In This Section

Monitoring Features Overview

Goal

Provide a monitoring strategy to monitor and alert on hardware and software assets. Monitoring critical system events on Windows servers round-the-clock, seven days a week, ensures the health of your IT infrastucture. If an issue is to occur, failure to be notified immediately could materially impact the continuity of your business. As the machines within the IT supported infrastructure change over time, monitoring should attempt to pick up those changes and begin monitoring appropriately based on those changes.

Overview

Kaseya monitoring provides multiple ways of monitoring agent based and non-agent based systems within a customers IT supported infrastructure. Server availability monitoring in the form Agent Status Alerts provide notifications when systems go down or are otherwise "offline" due to root causes such as crashes, reboots, network connectivity, system overloading, etc.. Windows Service monitoring in the form of Monitor Sets with Service Checks provide continual monitoring of important Windows Services, and send notifications and perform auto-remediation (restart services) when these services are not running/stopped. Event Log monitoring in the form of Event Set Alerts provide continual monitoring of Windows Event Logs and send notifications when important events are logged in these Windows Event Logs. Performance monitoring in the form of Monitor Sets with Counter Thresholds provide continual monitoring of important Windows Performance Counters and send notifications when the values of the counters meet certain thresholds where there could be a negative impact to system performance, availability, and/or reliability. Monitoring statuses , events, and values for counters are recorded within the system for updating historical, trending, and reporting purposes. Alarms generated by monitoring systems are logged within the system for historical and reporting purposes. Multiple levels of severity are supported so that issues that do arise can be prioritized appropriately and the correct parties notified via email.

The following Monitoring Features Overview depicts the system and monitoring types included in the Standard Solution package.

Monitoring Types = (A=Availability, E=Event Log, S=Services, P=Performance)

System Type (Category)	Monitoring Types	Monitoring General Overview
All Windows Servers (OS)	AESP	Core Win Srvr Monitoring
Windows Server 2003 (OS)	--S-	Win 2003 Services
Windows Server 2008/2008 R2 (OS)	--S-	Win 2008/2008R2 Services
All Windows Workstations (OS)	AESP	Core Win Wkst Monitoring
Windows Vista (OS)	--S-	Win Vista Services
Windows 7 (OS)	--S-	Win 7 Services
Windows XP (OS)	--S-	Win XP Services
Dell PowerEdge (Hardware)	-E--	Dell PowerEdge HW Events

Setup Wizard Enabled Content

HP ProLiant (Hardware)	-E--	HP ProLiant HW Events
IBM Series x (Server Hardware)	-E--	IBM Series x HW Events
Backup Exec Server (Role)	-ES-	Backup Exec Monitoring
Blackberry Enterprise Server	-ESP	Blackberry Server Monitoring
BrightStor ARCServe Server	-ES-	BrightStor Server Monitoring
Citrix Server	-ES-	Citrix Server Monitoring
DHCP Server	-ESP	DHCP Server Monitoring
DNS Server	-ESP	DNS Server Monitoring
Domain Controller (Network Infra)	-ESP	DC/AD Monitoring
Exchange 2003 Server (Email)	-ES-	Exch 2003 Monitoring
Exchange 2007 Server (Email)	-ES-	Exch 2007 Monitoring
Exchange 2010 Server (Email)	-ESP	Exch 2010 Monitoring
Exchange Server (Email)	-ESP	Core Exchange Monitoring
File Server (File/Print)	--S-	File Server Monitoring
FTP Server (Web Systems)	--S-	FTP Server Monitoring
IIS Server (Web Systems)	-ESP	IIS Server Monitoring
IMAP4 Server (Email)	--S-	IMAP4 Server Monitoring
POP3 Server (Email)	--S-	POP3 Server Monitoring
Print Server (File/Print)	-ESP	Print Server Monitoring
Microsoft SE-FEP (Security)	-ES-	Microsoft SE-FEP Monitoring
SharePoint Server (Web Systems)	--S-	SharePoint Server Monitorin
SMTP Server (Email)	-ESP	SMTP Server Monitoring
SQL Server (Database)	--SP	Core SQL Server Monitoring
SQL Server 2005 (Database)	--S-	SQL Server 2005 Monitoring
SQL Server 2008 (Database)	--S-	SQL Server 2008 Monitoring
Terminal Server (Remote Access)	-ESP	Terminal Server Monitoring
WINS Server (Network Infra)	--S-	WINS Server Monitoring
AVG Tech (Security)	--S-	AVG Tech AV Monitoring
Kaspersky ES (Security)	--S-	Kaspersky ES Monitoring
McAfee (Security)	-ES-	McAfee Monitoring
Sophos (Security)	-ES-	Sophos Monitoring
Symantec AV (Security)	-ES-	Symantec AV Monitoring
Symantec EP (Security)	-ES-	McAfee AV Monitoring
Trend Micro (Security)	-ES-	McAfee AV Monitoring

Monitoring Severity Matrix

		Monitoring Actions		
Severity Level	**Description**	**Email**	**Alarm**	**Rearm**
Severity0	Informational/Logging	No	No	N/A
Severity1	Low Impact/Risk	Yes	Yes	7 Days
Severity2	Medium Impact/	Yes	Yes	1 Day
Severity3	High Impact/Risk	Yes	Yes	12 Hrs

| Fixed Alert | High Impact/Risk | Yes | Yes | 12 Hrs |

Note: Severity Levels apply only to Monitor Sets and Event Sets and are designated in the Name of the Set. Fixed Alerts are all configured to behave like Severity3.

Monitoring Policies

An array of policies apply specific *monitoring* configurations to machines based on their Windows Operating System and Version, Hardware, Functional Role, and Security/AntiVirus products. These policies enable the various Availability, Event Log, Service and Performance monitoring components and related monitoring automation. The policies included are located under **[System].Core.Org Specific Policies.Monitoring**, and are described below.

In This Section

Server

- **Common Windows Server Monitoring** - Applies a common set of monitoring to all Windows Servers. This includes hardware related Events Log, Windows Service, and common Windows Performance monitoring.
- **Windows Server (Core)** - Applies an array of core Windows Server monitoring to Windows Servers including monitoring for standard services, system performance, health reporting, event logs, and more.
- **Windows Server 2003** - Applies standard service monitoring for Windows 2003 Servers.
- **Windows Server 2008/2008 R2** - Applies standard service monitoring for Windows 2008/2008 R2 Servers.

Hardware

- **Dell PowerEdge** - Applies Dell PowerEdge server hardware specific monitoring and alerting. This monitoring may require specific Dell PowerEdge server management tools to be installed on the server machine.
- **HP ProLiant** - Applies HP ProLiant server hardware specific monitoring and alerting. This monitoring may require specific HP ProLiant server management tools to be installed on the server machine.
- **IBM Series x** - Applies IBM Series X server hardware specific monitoring and alerting. This monitoring may require specific IBM Series X server management tools to be installed on the server machine.

Roles

- **Backup Exec Server** - Applies monitoring to Backup Exec Servers.
- **Blackberry Enterprise Server** - Applies monitoring to Blackberry Enterprise Servers.
- **BrightStor ARCServe Server** - Applies monitoring to BrightStor Servers.
- **Citrix Server** - Applies monitoring to Citrix Servers.
- **DHCP Server** - Applies monitoring to DHCP Servers.
- **DNS Server** - Applies monitoring to DNS Servers.
- **Domain Controller** - Applies monitoring to Domain Controllers.
- **Exchange 2003 Server** - Applies monitoring to Exchange 2003 Servers.
- **Exchange 2007 Server** - Applies monitoring to Exchange 2007 Servers.

- **Exchange 2010 Server** - Applies monitoring to Exchange 2010 Servers.
- **Exchange Server** - Applies monitoring to Exchange Servers.
- **File Server** - Applies monitoring to File Servers.
- **FTP Server** - Applies monitoring to FTP Servers.
- **IIS Server** - Applies monitoring to IIS Servers
- **IMAP4 Server** - Applies monitoring to IMAP4 Servers.
- **POP3 Server** - Applies monitoring to POP3 Servers.
- **Print Server** - Applies monitoring to Print Servers
- **SharePoint Server** - Applies monitoring to SharePoint Servers.
- **SMTP Server** - Applies monitoring to SMTP Servers.
- **SQL Server** - Applies monitoring to SQL Servers.
- **SQL Server 2005** - Applies monitoring to SQL 2005 Servers.
- **SQL Server 2008** - Applies monitoring to SQL 2008 Servers.
- **Terminal Server** - Applies monitoring to Terminal Servers.
- **WINS Server** - Applies monitoring to WINS Servers.

Workstation

- **Common Windows Workstation Monitoring** - Applies a common set of monitoring to all Windows Workstations. This includes hardware related Events Log, Windows Service, and common Windows Performance monitoring.
- **Windows Workstation (Core**) - Applies an array of core Windows Workstation monitoring to Windows Workstations including monitoring for standard services, system performance, health reporting, and more.
- **Windows Vista** - Applies standard service monitoring for Windows Vista machines.
- **Windows 7** - Applies standard service monitoring for Windows 7 machines.
- **Windows XP** - Applies standard service monitoring for Windows XP machines.

Security.Antivirus

- **AVG Tech** - Applies monitoring for AVG Technologies AntiVirus.
- **McAfee** - Applies monitoring for McAfee AntiVirus.
- **Microsoft SE-FEP** - Applies monitoring for Microsoft Security Essentials and Forefront Endpoint Protection.
- **Sophos** - Applies monitoring for Sophos AntiVirus.
- **Symantec AV** - Applies monitoring for Symantec AntiVirus.
- **Symantec EP** - Applies monitoring for Symantec Endpoint Protection AntiVirus.
- **Trend Micro** - Applies monitoring for Trend Micro AntiVirus.

Utility

- **Update Lists By Scan** - Applies a scheduled Update Lists By Scan to run on all Windows machines to keep performance counter, event log, and running services information current for each machine for accurate monitoring purposes.
- **Monitoring Cleanup** - As the last policy that contains Alerts and Monitor Sets, this policy effectively ensures that previously applied monitoring (Event Logs Alerts and Monitor Sets assigned via other policies that are no longer needed due to role changes, etc.) gets removed.

Monitor Sets

An array of Monitor Sets are provided and get applied via the Monitoring related Policies. These Monitor Sets monitor Windows Services and Performance Counters using Service Checks and Counter Thresholds. The provided Monitor Sets include monitoring for important Windows OS services and services for common Microsoft systems such as Active Directory, Exchange, SQL, IIS, and more. Basic system performance monitoring for disk space, memory utilization, CPU utilization, as well as more advanced system specific performance monitoring is included. The Monitor Sets included are located under **[System].Core**, and are described below.

In This Section

Backup

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - ➤ Monitors Backup Exec Continuous Protection Services on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - ➤ Monitors Backup Exec DLO Agent Services on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Backup - Backup Exec Services - {Severity3}**
  - ➤ Monitors Backup Exec Services on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Backup - Backup Exec System Recovery Service - {Severity3}**
  - ➤ Monitors Backup Exec System Recovery Service on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - ➤ Monitors BrightStor ARCServe Backup Services on BrightStor ARCServe Backup Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Database

- **Database - SQL Server (All Instances) Services - {Severity3}**
  - ➤ Monitors SQL Server Services on SQL Server Servers using wildcard MSSQL* Service. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Database - SQL Server (Default Instance) - {Severity0}**

> ➢ Collects SQL Server (Default Instance) performance counters on SQL Servers. Used for Monitor Log display and Reporting purposes only.

- **Database - SQL Server (Default Instance) Performance - {Severity2}**

> ➢ Monitors SQL Server (Default Instance) Performance on SQL Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Database - SQL Server (Default Instance) Services - {Severity3}**

> ➢ Monitors SQL Server (Default Instance) Services on SQL Server Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Database - SQL Server 2005 Optional Services - {Severity3}**

> ➢ Monitors SQL Server 2005 Optional Services on SQL Server 2005 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Database - SQL Server 2005 Services - {Severity3}**

> ➢ Monitors SQL Server 2005 Services on SQL Server 2005 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Database - SQL Server 2008 Optional Services - {Severity3}**

> ➢ Monitors SQL Server 2008 Optional Services on SQL Server 2008 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Database - SQL Server 2008 Services - {Severity3}**

> ➢ Monitors SQL Server 2008 Services on SQL Server 2008 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Email

- **Email - Blackberry Server Performance - {Severity2}**

> ➢ Monitors Blackberry Server Performance on Blackberry Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Email - BlackBerry Server Services - {Severity3}**

> ➢ Monitors BlackBerry Server Services on BlackBerry Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2003 Services - {Severity3}**

> ➢ Monitors Exchange 2003 Services on Exchange 2003 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2007 Services - {Severity3}**

> ➢ Monitors Exchange 2007 Services on Exchange 2007 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**

> ➢ Collects Exchange 2010 Edge Transport Queues performance counters on Exchange 2010 Servers. Used for Monitor Log display and Reporting purposes only.

- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**

> ➢ Monitors Exchange 2010 Edge Transport Queues Performance on Exchange 2010 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**

> ➢ Monitors Exchange 2010 Edge Transport Queues Performance on Exchange 2010 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2010 Services - {Severity3}**

> ➢ Monitors Exchange 2010 Services on Exchange 2010 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange Client Active Logons - {Severity0}**
  - ➢ Collects Exchange Client Active Logons performance counter on Exchange Servers. Used for Monitor Log display and Reporting purposes only.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - ➢ Monitors Exchange IMAP4 Service on Exchange Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Email - Exchange POP3 Service - {Severity3}**
  - ➢ Monitors Exchange POP3 Service on Exchange Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - ➢ Monitors Exchange Server Performance on Exchange Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Email - Exchange Server (Core) Services - {Severity3}**
  - ➢ Monitors Exchange Server (Core) Services on Exchange Server (Core) machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - ➢ Collects Exchange Server Store and Database performance counters on Exchange Servers. Used for Monitor Log display and Reporting purposes only.
- **Email - SMTP Queue Performance - {Severity3}**
  - ➢ Monitors SMTP Queue Performance on SMTP Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Email - SMTP Server Service - {Severity3}**
  - ➢ Monitors SMTP Server Service on SMTP Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

File / Print

- **File / Print - DFS Service - {Severity3}**
  - ➢ Monitors DFS Service on DFS machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **File / Print - DFSR Service - {Severity3}**
  - ➢ Monitors DFSR Service on DFSR machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **File / Print - NTFRS Service - {Severity3}**
  - ➢ Monitors NTFRS Service on NTFRS machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
  - ➢ Monitors Print Queue Job Errors Performance on File & Print Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **File / Print - Spooler Service - {Severity3}**
  - ➢ Monitors Spooler Service on File & Print Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Network Infrastructure

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**
  - ➢ Monitors Active Directory Domain Controller Services on Active Directory Domain Controllers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Network Infrastructure - DHCP Server Performance - {Severity2}**
  - ➢ Monitors DHCP Server Performance on DHCP Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Network Infrastructure - DHCP Server Service - {Severity3}**
  - ➢ Monitors DHCP Server Service on DHCP Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Network Infrastructure - DNS Server Performance - {Severity2}**
  - ➢ Monitors DNS Server Performance on DNS Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Network Infrastructure - DNS Server Service - {Severity3}**
  - ➢ Monitors DNS Server Service on DNS Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Network Infrastructure - WINS Server Service - {Severity3}**
  - ➢ Monitors WINS Server Service on WINS Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

OS Platforms.Windows (Core).Disk Space

- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - ➢ Monitors Free Disk Space on Drive C on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - ➢ Monitors Free Disk Space on Drive D on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - ➢ Monitors Free Disk Space on Drive E on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - ➢ Monitors Free Disk Space on Drive F on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - ➢ Monitors Free Disk Space on Drive G on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - ➢ Monitors Free Space on C Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - ➢ Monitors Free Space on D Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - ➢ Monitors Free Space on E Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - ➢ Monitors Free Space on F Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - ➢ Monitors Free Space on G Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

OS Platforms.Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - ➢ Collects service status for All Automatic Services on Windows machines. Used for Monitor Log display and Reporting purposes only.
- **Windows (Core) - CPU and Memory - {Severity0}**
  - ➢ Collects CPU and Memory performance counters on Windows machines. Used for Monitor Log display and Reporting purposes only.
- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - ➢ Monitors Free Disk Space on Any Drive Below 1GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - ➢ Monitors Free Disk Space on Any Drive Below 2GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - ➢ Monitors Free Disk Space on Any Drive Below 750MB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - ➢ Monitors Free Disk Space on Drive C Below 1GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Windows (Core) - Free Disk Space on Drive C Below 2GB - {Severity1}**
  - ➢ Monitors Free Disk Space on Drive C Below 2GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - ➢ Monitors Free Disk Space on Drive C Below 750MB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Machine Health - {Severity0}**
  - ➢ Collects Machine Health performance counters on Windows machines. Used for Monitor Log display and Reporting purposes only.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - ➢ Monitors Processor and Memory Performance on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  - ➢ Monitors TCPv4 Connections Performance on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

OS Platforms Windows Servers

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - ➢ Monitors Cluster Services on Windows Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  - ➢ Monitors Disk Time and Queue Length Performance on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Windows Server (Core) - Drive C Performance - {Severity1}**
  - ➢ Monitors Drive C Performance on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows Server (Core) - General System Performance - {Severity1}**

> ➢ Monitors General System Performance on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Server (Core) - Server Reboots - {Severity1}**

  > ➢ Monitors Server Reboots on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Server (Core) - Standard Services - {Severity3}**

  > ➢ Monitors Standard Services on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Windows Server 2003 - Standard Services - {Severity3}**

  > ➢ Monitors Standard Services on Windows Server 2003 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Windows Server 2008/2008 R2 - Standard Services - {Severity3}**

  > ➢ Monitors Standard Services on Windows Server 2008/2008 R2 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

OS Platforms.Windows Workstations

- **Windows 7 - Standard Services - {Severity1}**

  > ➢ Monitors Standard Services on Windows 7 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Vista - Standard Services - {Severity1}**

  > ➢ Monitors Standard Services on Windows Vista machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows XP - Standard Services - {Severity1}**

  > ➢ Monitors Standard Services on Windows XP machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

Remote Access

- **Remote Access - Citrix Licensing Service - {Severity3}**

  > ➢ Monitors Citrix Licensing Service on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix Licensing WMI Service - {Severity3}**

  > ➢ Monitors Citrix Licensing WMI Service on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix MetaFrame Services - {Severity3}**

  > ➢ Monitors Citrix MetaFrame Services on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix Server Services - {Severity3}**

  > ➢ Monitors Citrix Server Services on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**

  > ➢ Monitors Citrix Virtual Memory Optimization Service on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Terminal Server Services - {Severity3}**

  > ➢ Monitors Terminal Server Services on Terminal Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Terminal Server Session Performance - {Severity2}**

➢ Monitors Terminal Server Session Performance on Terminal Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

Security

▪ **AV - AVG Tech AVG Services - {Severity3}**

➢ Monitors AVG Tech AVG Services on AVG Tech AVG machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Kaspersky Endpoint Security Services {Severity3}**

➢ Monitors Kaspersky Endpoint Security Services on Kaspersky Endpoint Security machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - McAfee Enterprise Services - {Severity3}**

➢ Monitors McAfee Enterprise Services on McAfee Enterprise machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Sophos Antivirus Services - {Severity3}**

➢ Monitors Sophos Antivirus Services on Sophos Antivirus machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Symantec Antivirus Services - {Severity3}**

➢ Monitors Symantec Antivirus Services on Symantec Antivirus machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Symantec Endpoint Protection Services - {Severity3}**

➢ Monitors Symantec Endpoint Protection Services on Symantec Endpoint Protection machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Trend Micro Client Server Security Services - {Severity3}**

➢ Monitors Trend Micro Client Server Security Services on Trend Micro Client Server Security machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Trend Micro OfficeScan Services - {Severity3}**

➢ Monitors Trend Micro OfficeScan Services on Trend Micro OfficeScan machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Web Systems

▪ **Web Systems - FTP Server Service - {Severity3}**

➢ Monitors FTP Server Service on FTP Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **Web Systems - IIS Performance - {Severity3}**

➢ Monitors IIS Performance on IIS Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **Web Systems - IIS Server - {Severity0}**

➢ Collects IIS Server performance counters on IIS Servers. Used for Monitor Log display and Reporting purposes only.

▪ **Web Systems - IIS Server Services - {Severity3}**

➢ Monitors IIS Server Services on IIS Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **Web Systems - SharePoint Server Services - {Severity3}**

➢ Monitors SharePoint Server Services on SharePoint Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Event Sets

An array of Event Sets are provided and get applied via the Monitoring related Policies. These Event Sets monitor Windows Event Logs for specific Events. The provided Event Sets include monitoring for important Windows OS events, for common Microsoft systems such as Active Directory, Exchange, SQL, IIS, for 3rd party applications/systems, and more. The Event Sets included are described below grouped by category.

In This Section

Security

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - ➢ Monitors for specific McAfee Anti-Virus Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Microsoft Security Essentials/Forefront Endpoint Protection Error and Warning events in the System Event Log. Alarms are considered Severity2.
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - ➢ Monitors for specific Misc AntiVirus Error and Warning events in the Application & System Event Logs. Alarms are considered Severity3.
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - ➢ Monitors for specific Misc AntiVirus Informational events in the Application & System Event Logs. Alarms are considered Severity1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Error and Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Informational events in the Application Event Log. Used for logging and reporting purposes only.

Backup

- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}**
  - ➢ Monitors for specific Backup Exec events in the Application Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Backup Exec Job Failure/Cancellation Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}**
  - ➢ Monitors for specific Backup Exec Job Success events in the Application Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}**
  - ➢ Monitors for specific BrightStor ARCserve Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific BrightStor ARCServe Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}**
  - ➢ Monitors for specific Microsoft Windows Backup Error events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}**
  - ➢ Monitors for specific Misc Backup Error events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}**
  - ➢ Monitors for specific Misc Backup Informational events in the Application Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}**
  - ➢ Monitors for specific Misc Backup Warning events in the Application Event Log. Alarms are considered Severity1.

Database

- **zz[SYS] Database - SQL Server (E) - APP - {Severity2}**
  - ➢ Monitors for specific SQL Server Error events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Database - SQL Server (E) - APP - {Severity3}**

➢ Monitors for specific SQL Server Error events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}**

➢ Monitors for specific SQL Server - ACID Error and Warning events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server - ACID Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}**

➢ Monitors for specific SQL Server - ACID Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server - ACID events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server - Backup Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}**

➢ Monitors for specific SQL Server - Backup Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server - Backup events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}**

➢ Monitors for specific SQL Server - DB Resources Error and Warning events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server - DB Resources Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}**

➢ Monitors for specific SQL Server - DB Resources Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server - DB Resources events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}**

➢ Monitors for specific SQL Server - MSDTC Error and Warning events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server - MSDTC Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}**

➢ Monitors for specific SQL Server - MSDTC Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server - MSDTC events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**

> ➢ Monitors for specific SQL Server - Network Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**

  > ➢ Monitors for specific SQL Server - Network Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**

  > ➢ Monitors for specific SQL Server - Query Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**

  > ➢ Monitors for specific SQL Server - Query Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**

  > ➢ Monitors for specific SQL Server - Replication Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**

  > ➢ Monitors for specific SQL Server - Replication Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**

  > ➢ Monitors for specific SQL Server - Replication Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**

  > ➢ Monitors for specific SQL Server - Replication events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**

  > ➢ Monitors for specific SQL Server - Reporting Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**

  > ➢ Monitors for specific SQL Server - Reporting Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**

  > ➢ Monitors for specific SQL Server - Reporting events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**

  > ➢ Monitors for specific SQL Server Agent - Multiple Instances Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**

  > ➢ Monitors for specific SQL Server Agent - Multiple Instances Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**

  > ➢ Monitors for specific SQL Server Agent - Multiple Instances Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**

  > ➢ Monitors for specific SQL Server Agent - Multiple Instances events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**

  > ➢ Monitors for specific SQL Server Agent - Single Instance Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**

> ➢ Monitors for specific SQL Server Agent - Single Instance Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**

  > ➢ Monitors for specific SQL Server Agent - Single Instance Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**

  > ➢ Monitors for specific SQL Server Agent - Single Instance events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**

  > ➢ Monitors for specific SQL Server Cluster Informational events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**

  > ➢ Monitors for specific SQL/Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.

Email

- **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**

  > ➢ Monitors for specific Blackberry Server Error events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**

  > ➢ Monitors for specific Blackberry Server Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**

  > ➢ Monitors for specific Blackberry Server Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}**

  > ➢ Monitors for specific Blackberry Server Events Error events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}**

  > ➢ Monitors for specific Blackberry Server Events Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}**

  > ➢ Monitors for specific Exchange 2000 and 2003 Error events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}**

  > ➢ Monitors for specific Exchange 2000 and 2003 Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}**

  > ➢ Monitors for specific Exchange 2000 and 2003 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}**

  > ➢ Monitors for specific Exchange 2000 and 2003 and 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}**

  > ➢ Monitors for specific Exchange 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**

- ➢ Monitors for specific Exchange 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
    - ➢ Monitors for specific Exchange 2007 events in the Application Event Log. Used for logging and reporting purposes only.
  - ▪ **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
    - ➢ Monitors for specific Exchange 2007 - Client Access Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - ▪ **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**
    - ➢ Monitors for specific Exchange 2007 - Client Access Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange 2007 - Client Access Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
    - ➢ Monitors for specific Exchange 2007 - Edge Transport Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - ▪ **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
    - ➢ Monitors for specific Exchange 2007 - Edge Transport Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange 2007 - Edge Transport Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**
    - ➢ Monitors for specific Exchange 2007 - Hub Transport Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - ▪ **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
    - ➢ Monitors for specific Exchange 2007 - Hub Transport Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange 2007 - Hub Transport Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
    - ➢ Monitors for specific Exchange 2007 - Mailbox Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - ▪ **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
    - ➢ Monitors for specific Exchange 2007 - Mailbox Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange 2007 - Mailbox Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**
    - ➢ Monitors for specific Exchange 2007 - Mailbox events in the Application Event Log. Used for logging and reporting purposes only.
  - ▪ **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**

- ➢ Monitors for specific Exchange 2007 - Transport Services Error and Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Exchange 2007 - Transport Services Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Exchange 2007 - Transport Services Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**
  - ➢ Monitors for specific Exchange 2007 - Unified Messaging Error and Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Exchange 2007 - Unified Messaging Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Exchange 2007 - Unified Messaging Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - ➢ Monitors for specific Exchange 2010 Server Error events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - ➢ Monitors for specific Exchange 2010 Server Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - ➢ Monitors for specific Exchange 2010 Server Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - ➢ Monitors for specific Exchange 2010 Server Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - ➢ Monitors for specific Exchange Server Error events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - ➢ Monitors for specific Exchange Server Error events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - ➢ Monitors for specific Exchange Server Informational events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
  - ➢ Monitors for specific Exchange Server 5.5 Error events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Exchange/Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific SMTP/Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Battery Error and Warning events in the System Event Log. Alarms are considered Severity1.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Battery Error and Warning events in the System Event Log. Alarms are considered Severity2.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell Battery Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitors for specific Dell Battery events in the System Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Controller Error and Warning events in the System Event Log. Alarms are considered Severity1.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Controller Error and Warning events in the System Event Log. Alarms are considered Severity2.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell Controller Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitors for specific Dell Controller events in the System Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Electrical Error and Warning events in the System Event Log. Alarms are considered Severity1.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Electrical Error and Warning events in the System Event Log. Alarms are considered Severity2.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell Electrical Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitors for specific Dell Electrical events in the System Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Enclosure Error and Warning events in the System Event Log. Alarms are considered Severity1.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Enclosure Error and Warning events in the System Event Log. Alarms are considered Severity2.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell Enclosure Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Enclosure events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Environmental Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Environmental Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Environmental Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Environmental events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Fan Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Fan Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Fan Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Fan events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Hardware Changes Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Hardware Changes Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Hardware Changes Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Hardware Changes events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Hardware Log Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Hardware Log Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Hardware Log events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Media Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Media Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Media Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Media events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Memory Prefailure Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Memory Prefailure Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell OMSA System Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell OMSA System Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell OMSA System Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell OMSA System events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell OMSM System Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell OMSM System Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Physical Disk Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Physical Disk Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Physical Disk Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Physical Disk events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Power Management Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Power Management Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Power Management Error and Warning events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Power Management events in the System Event Log. Alarms are considered Severity0.

▪ **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Processor Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Processor Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Processor events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Redundancy Mirror Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Redundancy Mirror Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Redundancy Mirror events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Temperature Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**

➢ Monitors for specific Dell Temperature Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Temperature Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Temperature events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**

➢ Monitors for specific Dell Virtual Disk Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}**

➢ Monitors for specific Dell Virtual Disk Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Virtual Disk events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}**

➢ Monitors for specific HP Top Tools Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}**

➢ Monitors for specific HP/Compaq Insight Manager Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}**

➢ Monitors for specific HP/Compaq StorageWorks Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}**

➢ Monitors for specific IBM SeriesX Events Error events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}**

➢ Monitors for specific Misc HW Error events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}**

➢ Monitors for specific Misc HW Error events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}**

➢ Monitors for specific Misc HW Warning events in the System Event Log. Alarms are considered Severity1.

Network Infrastructure

▪ **zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}**

➢ Monitors for specific Active Directory Error events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**

➢ Monitors for specific Active Directory Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**

➢ Monitors for specific Active Directory Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**

➢ Monitors for specific Active Directory Events Error events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**

➢ Monitors for specific Active Directory Events Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**

➢ Monitors for specific Active Directory Logon/Logoff/Lockout Activity Failure Audit events in the Security Event Log. Alarms are considered Severity3

▪ **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**

➢ Monitors for specific Active Directory NTDS Error events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**

- ➢ Monitors for specific Active Directory NTDS Error events in the System Event Log. Alarms are considered Severity3.
- ▪ **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  - ➢ Monitors for specific Active Directory NTDS Informational events in the System Event Log. Used for logging and reporting purposes only.
- ▪ **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  - ➢ Monitors for specific DHCP Server Error events in the System Event Log. Alarms are considered Severity1
- ▪ **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  - ➢ Monitors for specific DHCP Server Warning events in the System Event Log. Alarms are considered Severity1.
- ▪ **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  - ➢ Monitors for specific DNS Server Error events in the System Event Log. Alarms are considered Severity1.
- ▪ **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  - ➢ Monitors for specific DNS Server Warning events in the System Event Log. Alarms are considered Severity1.
- ▪ **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  - ➢ Monitors for specific WINS Server Error events in the System Event Log. Alarms are considered Severity1.

Remote Access

- ▪ **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Citrix MetaFrame Error and Warning events in the Application Event Log. Alarms are considered Severity3
- ▪ **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**
  - ➢ Monitors for specific Citrix Server Events Error events in the Application Event Log. Alarms are considered Severity2.
- ▪ **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**
  - ➢ Monitors for specific Terminal Server Events Error events in the Application Event Log. Alarms are considered Severity2.
- ▪ **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**
  - ➢ Monitors for specific Terminal Server Events Error events in the Application Event Log. Alarms are considered Severity3.

Web Systems

- ▪ **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**
  - ➢ Monitors for specific IIS 6 Events Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- ▪ **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**
  - ➢ Monitors for specific IIS 7 Events Error events in the Application Event Log. Alarms are considered Severity2.
- ▪ **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**
  - ➢ Monitors for specific IIS 7 Events Error events in the Application Event Log. Alarms are considered Severity3.
- ▪ **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**

➢ Monitors for specific IIS Server Error events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**

➢ Monitors for specific IIS Server Warning events in the Application Event Log. Alarms are considered Severity1.

OS Platforms

▪ **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}**

➢ Monitors for specific Common Windows Server Error events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}**

➢ Monitors for specific Common Windows Server Error events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Common Windows Server events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}**

➢ Monitors for specific Common Windows Server Failure Audit events in the Security Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}**

➢ Monitors for specific Common Windows Server Failure Audit events in the Security Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}**

➢ Monitors for specific Common Windows Server Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}**

➢ Monitors for specific Common Windows Server Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}**

➢ Ignores monitoring for specific Common Windows Server Error and Warning events in the Application & System Event Logs.

▪ **zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}**

➢ Monitors for specific Windows Server Print Spooler Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}**

➢ Monitors for specific Windows Server Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}**

➢ Monitors for specific Windows Server Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}**

➢ Monitors for specific Windows Server Service Control Manager Informational events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}**

➢ Monitors for specific Windows Server System Shutdown Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}**

> ➢ Monitors for specific Common Windows Server 2008 Error events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}**

  > ➢ Monitors for specific Common Windows Server 2008 Error events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**

  > ➢ Monitors for specific Common Windows Server 2008 Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**

  > ➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**

  > ➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**

  > ➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity1

- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**

  > ➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**

  > ➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**

  > ➢ Monitors for specific Advanced Windows Server 2008 events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**

  > ➢ Monitors for specific Basic Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**

  > ➢ Monitors for specific Basic Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**

  > ➢ Monitors for specific Basic Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**

  > ➢ Monitors for specific Basic Windows Server 2008 events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**

  > ➢ Monitors for specific Basic Windows Server 2008 Failure Audit events in the Security Event Log. Alarms are considered Severity1.

- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**

  > ➢ Monitors for specific Basic Windows Server 2008 Failure Audit events in the Security Event Log. Alarms are considered Severity2.

- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**

  > ➢ Monitors for specific Basic Windows Server 2008 Failure Audit events in the Security Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**

➢ Monitors for specific Common Windows Workstation Error events in the System Event Log. Alarms are considered Severity1.

Chapter 4

Complete Content Catalog

The following topics summarize the complete list of all standard content provided with the VSA.

In This Chapter

Views

Agent Status

- **zz[SYS] Agent - Has Checked In**
  - ➢ Displays all machines that have checked in at least once (excludes Templates)
- **zz[SYS] Agent - Has Not Checked In**
  - ➢ Displays all agents that have not checked in (i.e.KDS deployment computers and templates)
- **zz[SYS] Agent - Offline**
  - ➢ Displays all agents offline for 1+ mins
- **zz[SYS] Agent - Offline 30+ Days**
  - ➢ Displays all agents offline for 30+ days
- **zz[SYS] Agent - Offline 60+ Days**
  - ➢ Displays all agents offline for 60+ days
- **zz[SYS] Agent - Online**
  - ➢ Displays all agents online in last 1 minute
- **zz[SYS] Agent - Online in Last 30 Days**
  - ➢ Displays all agents online in last 7 days
- **zz[SYS] Agent - Rebooted 14+ Days Ago**
  - ➢ Displays all agents that have NOT been rebooted in the last 14 days
- **zz[SYS] Agent - Suspended**
  - ➢ Displays all suspended agents
- **zz[SYS] Agent - User Logged On**
  - ➢ Displays all machines with a user logged onto them

Security

- **zz[SYS] AV - AVG Technologies**
  - ➢ Displays all machines with Grisoft AVG Anti-Virus installed
- **zz[SYS] AV - Kaspersky ES**
  - ➢ Displays all machines with Kaspersky Endpoint Security installed
- **zz[SYS] AV - McAfee**
  - ➢ Displays all machines with McAfee Anti-Virus installed
- **zz[SYS] AV - Microsoft SE-FEP**
  - ➢ Displays all machines with Microsoft Security Essentials or Forefront Endpoint Protection installed
- **zz[SYS] AV - Sophos**
  - ➢ Displays all machines with Sophos Anti-Virus installed
- **zz[SYS] AV - Symantec AV**
  - ➢ Displays all machines with Symantec Anti-Virus installed
- **zz[SYS] AV - Symantec EP**
  - ➢ Displays all machines with Symantec Endpoint Protection installed
- **zz[SYS] AV - Trend Micro**
  - ➢ Displays all machines with Trend Micro Anti-Virus installed

Backup

- **zz[SYS] Backup - CA BrightStor ARCServe**
  - ➢ Displays all machines with CA BrightStor ARCserve installed
- **zz[SYS] Backup - Symantec Backup Exec**
  - ➢ Displays all machines with Symantec Backup Exec installed

Hardware

- **zz[SYS] HW - Apple**
  - ➢ Displays all machines with Apple as manufacturer
- **zz[SYS] HW - Dell**
  - ➢ Displays all machines with Dell as manufacturer
- **zz[SYS] HW - Dell PowerEdge**
  - ➢ Displays all machines with Dell as manufacturer and PowerEdge in product name
- **zz[SYS] HW - HP**
  - ➢ Displays all machines with HP or Hewlett Packard as manufacturer
- **zz[SYS] HW - HP ProLiant**
  - ➢ Displays all machines with HP or Hewlett Packard as manufacturer and ProLiant in product name
- **zz[SYS] HW - IBM**
  - ➢ Displays all machines with IBM as manufacturer
- **zz[SYS] HW - IBM Series X**
  - ➢ Displays all machines with IBM as manufacturer and Series X in product name
- **zz[SYS] HW - Lenovo**
  - ➢ Displays all machines with Lenovo as manufacturer
- **zz[SYS] HW - Not Portable**
  - ➢ Displays all machines that are not mobile
- **zz[SYS] HW - Portable**
  - ➢ Displays all machines that are mobile (i.e. chassis type = notebook or laptop or portable or tablet pc or hand-held or sub-notebook or netbook). Note: Mac OS X and Linux machines excluded.
- **zz[SYS] HW - Under 1GB Memory**
  - ➢ Displays all machines that have less than 1GB of memory
- **zz[SYS] HW - Under 512MB Memory**
  - ➢ Displays all machines that have less than 512MB of memory
- **zz[SYS] HW - Virtual Guest**
  - ➢ Displays all machines that are Virtualized computers (VMWare, XenServer, VirtualBox or HyperV guests)

Network

- **zz[SYS] Network - 10.11.12.x**
  - ➢ Displays all agents of specific network subnet 10.11.12.x

Operating System

- **zz[SYS] OS - All Linux**
  - ➢ Displays all Linux machines
- **zz[SYS] OS - All Mac OS X**
  - ➢ Displays all Mac OS X machines

- **zz[SYS] OS - All Mac OS X Servers**
  - Displays all Mac OS X Server machines
- **zz[SYS] OS - All Mac OS X Workstations**
  - Displays all Mac OS X Workstation machines
- **zz[SYS] OS - All Servers**
  - Displays all machines running a Server class Operating System
- **zz[SYS] OS - All Windows**
  - Displays all Windows machines
- **zz[SYS] OS - All Windows SBS**
  - Displays all Windows SBS Server machines
- **zz[SYS] OS - All Windows Servers**
  - Displays all Windows Server machines
- **zz[SYS] OS - All Windows Workstations**
  - Displays all Windows Workstation machines
- **zz[SYS] OS - All Workstations**
  - Displays all machines running a Workstation class Operating System
- **zz[SYS] OS - Mac OS X 10.5 Leopard**
  - Displays all Mac OS X v10.5 machines
- **zz[SYS] OS - Mac OS X 10.6 Snow Leopard**
  - Displays all Mac OS X v10.6 machines
- **zz[SYS] OS - Mac OS X 10.7 Lion**
  - Displays all Mac OS X v10.7 machines
- **zz[SYS] OS - Mac OS X 10.8 Mountain Lion**
  - Displays all Mac OS X v10.8 machines
- **zz[SYS] OS - Win 2003 SBS**
  - Displays all machines running a Windows 2003 Small Business Server Operating System
- **zz[SYS] OS - Win 2003 Server**
  - Displays all machines running a Windows 2003 Server Operating System
- **zz[SYS] OS - Win 2008 R2 Server**
  - Displays all machines running a Windows 2008 Small Business Server Operating System
- **zz[SYS] OS - Win 2008 SBS**
  - Displays all machines running a Windows 2008 Server Operating System
- **zz[SYS] OS - Win 2008 Server**
  - Displays all machines running a Windows 2008 Server R2 Operating System
- **zz[SYS] OS - Win 2012 Server**
  - Displays all machines running a Windows 2012 Server Operating System
- **zz[SYS] OS - Win 7**
  - Displays all machines running a Windows 7 Operating System
- **zz[SYS] OS - Win Vista**
  - Displays all machines running a Windows Vista Operating System
- **zz[SYS] OS - Win XP**
  - Displays all machines running a Windows XP Operating System
- **zz[SYS] OS - Win 8**
  - Displays all machines running a Windows 8 Operating System

Patch Management

- **zz[SYS] Patch - Deny Patching Policy**
  - ➢ Displays all machines that are in the "Deny Patching" Patch Policy
- **zz[SYS] Patch - Missing 10+ Approved Patches**
  - ➢ Displays all machines that are missing 10 or more approved patches based on their patch policy membership(s)
- **zz[SYS] Patch - Missing 20+ Approved Patches**
  - ➢ Displays all machines that are missing 20 or more approved patches based on their patch policy membership(s)
- **zz[SYS] Patch - No Policy**
  - ➢ Displays all machines that are not a member of a Patch Policy
- **zz[SYS] Patch - Pending Reboot**
  - ➢ Displays all machines that are pending a reboot due to recent patch updates.
- **zz[SYS] Patch - Scan Failed**
  - ➢ Displays all machines that failed the patch scan.
- **zz[SYS] Patch - Scan Not Scheduled**
  - ➢ Displays all machines that do not have a patch scan scheduled.
- **zz[SYS] Patch - Server Patching Policy**
  - ➢ Displays all machines that are in the "Server Patching" Patch Policy
- **zz[SYS] Patch - Servers w No Policy**
  - ➢ Displays all machines that are not a member of a Patch Policy
- **zz[SYS] Patch - Test Patching Group**
  - ➢ Displays all machines that are designated as test systems for patch management
- **zz[SYS] Patch - Windows Auto Update Enabled**
  - ➢ Displays all machines that have Windows Automatic Update Enabled
- **zz[SYS] Patch - Workstation Patching Policy**
  - ➢ Displays all machines that are in the "Workstation Patching" Patch Policy
- **zz[SYS] Patch - Workstations w No Policy**
  - ➢ Displays all machines that are not a member of a Patch Policy

Server Role

- **zz[SYS] Role - Backup Exec Server**
  - ➢ Displays all Backup Exec Servers
- **zz[SYS] Role - Blackberry Server**
  - ➢ Displays all Blackberry Enterprise Servers
- **zz[SYS] Role - Brightstor ARCserve Server**
  - ➢ Displays all BrightStor ARCserve Servers
- **zz[SYS] Role - Citrix Server**
  - ➢ Displays all Citrix Servers
- **zz[SYS] Role - DHCP Server**
  - ➢ Displays all MS DHCP Servers
- **zz[SYS] Role - DNS Server**
  - ➢ Displays all MS DNS Servers
- **zz[SYS] Role - Domain Controller**
  - ➢ Displays all MS AD Domain Controller Servers

- **zz[SYS] Role - Exchange 2003 Server**
  - ➢ Displays all MS Exchange 2003 Servers
- **zz[SYS] Role - Exchange 2007 Server**
  - ➢ Displays all MS Exchange 2007 Servers
- **zz[SYS] Role - Exchange 2010 Server**
  - ➢ Displays all MS Exchange 2010 Servers
- **zz[SYS] Role - Exchange Server**
  - ➢ Displays all MS Exchange Servers
- **zz[SYS] Role - File Server**
  - ➢ Displays all MS File Servers
- **zz[SYS] Role - FTP Server**
  - ➢ Displays all MS FTP Servers
- **zz[SYS] Role - IIS Server**
  - ➢ Displays all MS IIS Servers
- **zz[SYS] Role - IMAP4 Server**
  - ➢ Displays all MS Exchange IMAP4 Servers
- **zz[SYS] Role - POP3 Server**
  - ➢ Displays all MS Exchange POP3 Servers
- **zz[SYS] Role - Print Server**
  - ➢ Displays all MS Print Servers
- **zz[SYS] Role - SharePoint Server**
  - ➢ Displays all MS SharePoint Servers
- **zz[SYS] Role - SMTP Server**
  - ➢ Displays all MS SMTP Servers
- **zz[SYS] Role - SQL Server**
  - ➢ Displays all MS SQL Servers
- **zz[SYS] Role - SQL Server 2005**
  - ➢ Displays all MS SQL 2005 Servers
- **zz[SYS] Role - SQL Server 2008**
  - ➢ Displays all MS SQL 2008 Servers
- **zz[SYS] Role - Terminal Server**
  - ➢ Displays all MS Terminal Servers in Application Mode
- **zz[SYS] Role - WINS Server**
  - ➢ Displays all MS WINS Servers

Policies

[System].Core.Global Policies.Agent Settings

- **Agent (Core)**
  - ➢ *Policy View:*   zz[SYS] Policy - Agent_Has Checked In
  - ➢ *Description:*   Agent (Core) - Applies common agent settings for all managed machines. Agent Icon is enabled but only Refresh option is enabled. Check-In control is set to 30 seconds with "Warn if multiple agents use same account" and "Warn if agent on same LAN as KServer connects through gateway" both enabled. Agent Log History for all logs is set to 31 days.

- **Windows Agent**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Windows
  - ➤ *Description:* Windows Agent - Applies agent settings specific to Windows. Sets Agent Working Directory to c:\kworking.
- **Linux Agent**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Linux
  - ➤ *Description:* Linux Agent - Applies agent settings specific to Linux. Sets Agent Working Directory to /tmp/kworking.
- **Macintosh Agent**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Mac OS X
  - ➤ *Description:* Macintosh Agent - Applies agent settings specific to Macintosh Workstations. Sets Agent Working Directory to /Library/Kaseya/kworking.

[System].Core.Global Policies.Remote Support

- **Server RC Notification Policy (Silent w Admin Note)**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Servers
  - ➤ *Description:* Server RC Notification Policy (Silent w Admin Note) - Applies Remote Control notification settings for all servers. Sets user notification type to Silently take control, and enables the Require admin note to start remote control option.
- **Workstation RC Notification Policy (Alert/Term w Admin Note)**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Workstations
  - ➤ *Description:* Workstation RC Notification Policy (Alert/Term w Admin Note) - Applies Remote Control notification settings for all workstations. Sets user notification type to If user logged in display alert, Notify user when session terminates, and enables the Require admin note to start remote control option.

[System].Core.Org Specific Policies.Agent Settings

- **Agent (Hidden)**
  - ➤ *Policy View:* zz[SYS] Policy - Agent_Has Checked In
  - ➤ *Description:* Agent (Hidden) - Applies common agent settings for all managed machines. Agent Icon is disabled/hidden. Check-In control is set to 30 seconds with "Warn if multiple agents use same account" and "Warn if agent on same LAN as KServer connects through gateway" both enabled. Agent Log History for all logs is set to 31 days.
- **Agent (Server)**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Servers
  - ➤ *Description:* Agent (Server) - Applies common agent settings for all managed servers. Agent Icon is enabled with Disable Remote Control, Refresh and Exit. Check-In control is set to 30 seconds with "Warn if multiple agents use same account" and "Warn if agent on same LAN as KServer connects through gateway" both enabled. Agent Log History for all logs is set to 93 days.
- **Agent (Workstation)**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Workstations
  - ➤ *Description:* Agent (Workstation) - Applies common agent settings for all managed workstations. Agent Icon is enabled with Contact Help Desk, Disable Remote Control and Refresh. Check-In control is set to 30 seconds with "Warn if multiple agents use same account" and "Warn if agent on same LAN as KServer connects through gateway" both enabled. Agent Log History for all logs is set to 31 days.

[System].Core.Org Specific Policies.Remote Support

- **Server RC Notification Policy (Silent w/o Admin Note)**

- ➢ *Policy View:*   zz[SYS] Policy - OS_All Servers
- ➢ *Description:*   Server RC Notification Policy (Silent w/o Admin Note) - Applies Remote Control notification settings for all servers. Sets user notification type to Silently take control and does not require an Admin Note to start remote control.

- **Workstation RC Notification Policy (Alert/Term w/o Admin Note)**
  - ➢ *Policy View:*   zz[SYS] Policy - OS_All Workstations
  - ➢ *Description:*   Workstation RC Notification Policy (Alert/Term w/o Admin Note) - Applies Remote Control notification settings for all workstations. Sets user notification type to If user logged in display alert, Notify user when session terminates, and does not require an Admin Note to start remote control.

- **Workstation RC Notification Policy (Silent w Admin Note)**
  - ➢ *Policy View:*   zz[SYS] Policy - OS_All Workstations
  - ➢ *Description:*   Workstation RC Notification Policy (Silent w Admin Note) - Applies Remote Control notification settings for all workstations. Sets user notification type to Silently take control but requires an Admin Note to start remote control.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Baseline.Baseline Audit Schedule (Annually Daytime)

- **Baseline Audit Schedule (Annually Jan 1-7 6am-6pm/Power Mgmt)**
  - ➢ *Policy View:*   zz[SYS] Policy - Agent_Has Checked In
  - ➢ *Description:*   Baseline Audit Schedule (Annually Jan 1-7 6am-6pm/Power Mgmt) - Applies a scheduled Annual Baseline Audit for all machines that have been deployed and have checked in beginning on January 1st through the 7th between 6am-6pm. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where annual audits may be required for planning or compliancy purposes and so that for relevant Baseline/Latest Audit comparisons can be performed for operational tasks. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)

- **Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt)**
  - ➢ *Policy View:*   zz[SYS] Policy - Agent_Has Checked In
  - ➢ *Description:*   Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt) - Applies scheduled Latest and System Info Audits for all machines that have checked in to run daily (M-F) between 6am-6pm. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where customers need to run audits during business hours on weekdays because machines are generally turned off at night and on weekends. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Nighttime)

- **Latest/SysInfo Audit Schedule (Daily M-F 6pm-6am/Power Mgmt)**
  - ➢ *Policy View:*   zz[SYS] Policy - Agent_Has Checked In
  - ➢ *Description:*   Latest/SysInfo Audit Schedule (Daily M-F 6pm-6am/Power Mgmt) - Applies scheduled Latest and System Info Audits for all machines that have checked in to run daily (M-F) between 6pm-6am. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where customers prefer to run audits in the evening when

systems are less utilized than during business hours and when machines are either left on at night or have been configured for Wake-On-LAN or vPro Power Management so that can be woken if powered off at night. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Daytime)

- **Latest/SysInfo Audit Schedule (Weekly M-F 6am-6pm/Power Mgmt)**
  - ➢ *Policy View:*   zz[SYS] Policy - Agent_Has Checked In
  - ➢ *Description:*   Latest/SysInfo Audit Schedule (Weekly M-F 6am-6pm/Power Mgmt) - Applies scheduled Latest and System Info Audits for all machines that have checked in to run weekly (M-F) between 6am-6pm. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where customers need to run audits during business hours on weekdays because machines are generally turned off at night and on weekends. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Nighttime)

- **Latest/SysInfo Audit Schedule (Weekly M-F 6pm-6am/Power Mgmt)**
  - ➢ *Policy View:*   zz[SYS] Policy - Agent_Has Checked In
  - ➢ *Description:*   Latest/SysInfo Audit Schedule (Weekly M-F 6pm-6am/Power Mgmt) - Applies scheduled Latest and System Info Audits for all machines that have checked in to run weekly (M-F) between 6pm-6am. The policy uses the power management feature at the scheduled audit time attempting to wake a powered off machine prior to the audit. The policy is generally used in situations where customers prefer to run audits in the evening when systems are less utilized than during business hours and when machines are either left on at night or have been configured for Wake-On-LAN or vPro Power Management so that can be woken if powered off at night. The policy can be selectively applied to various machines, machine groups, and/or entire organizations of machines.

[System].Core.Org Specific Policies.Maintenance.Windows Workstation Recurring Maintenance

- **Windows Workstation Maintenance (Weekly M-F 6pm-6am)**
  - ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows Workstations
  - ➢ *Description:*   Windows Workstation Maintenance (Weekly M-F 6pm-6am) - Applies a scheduled Windows Workstation maintenance procedure to run on all Windows Workstation machines weekly (M-F) between 6pm-6am. If the machine is not turned on when the maintenance is scheduled, then the machine will skip that maintenance cycle and will attempt to run the maintenance again a week later.

[System].Core.Org Specific Policies.Maintenance.Macintosh Workstation Recurring Maintenance

- **Macintosh Maintenance Schedule (Weekly M-F 6pm-6am)**
  - ➢ *Policy View:*   zz[SYS] Policy - OS_All Mac OS X Workstations
  - ➢ *Description:*   Macintosh Maintenance Schedule (Weekly M-F 6pm-6am) - Applies a scheduled Macintosh maintenance procedure to run on all Macintosh machines weekly (M-F) between 6pm-6am. If the machine is not turned on when the maintenance is scheduled, then the machine will skip that maintenance cycle and will attempt to run the maintenance again a week later.

[System].Core.Org Specific Policies.Maintenance.Linux Recurring Maintenance

- **Linux Maintenance Schedule (Weekly M-F 6pm-6am)**

➢ *Policy View:*   zz[SYS] Policy - OS_All Linux

➢ *Description:*   Linux Maintenance Schedule (Weekly M-F 6pm-6am) - Applies a scheduled Linux maintenance procedure to run on all Linux machines weekly (M-F) between 6pm-6am. If the machine is not turned on when the maintenance is scheduled, then the machine will skip that maintenance cycle and will attempt to run the maintenance again a week later.

[System].Core.Org Specific Policies.Maintenance.Windows Server Recurring Maintenance

- **Windows Server Maintenance (Weekly Sun 12am-4am)**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows Servers

  ➢ *Description:*   Windows Server Maintenance (Weekly Sun 12am-4am) - Applies a scheduled Windows Server maintenance procedure to run on all Windows Server machines weekly on Sunday between 12am-4am. If the machine is not turned on when the maintenance is scheduled, then the machine will skip that maintenance cycle and will attempt to run the maintenance again a week later.

[System].Core.Org Specific Policies.Monitoring.Server

- **Server Roles Enhanced Audit**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows Servers

  ➢ *Description:*   Server Roles Enhanced Audit - Applies a scheduled Enhanced Audit to run weekly on Sun between 12am-4am in order to identify server functional roles so that monitoring policies can be applied properly based on those roles.

- **Common Windows Server Monitoring**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows Servers

  ➢ *Description:*   Common Windows Server Monitoring - Applies a common set of monitoring to all Windows Servers. This includes hardware related Events Log, Windows Service, and common Windows Performance monitoring.

- **Windows Server (Core)**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows Servers

  ➢ *Description:*   Windows Server (Core) - Applies an array of core Windows Server monitoring to Windows Servers including monitoring for standard services, system performance, health reporting, event logs, and more.

- **Windows Server 2003**

  ➢ *Policy View:*   zz[SYS] Policy - OS_Win 2003 Server

  ➢ *Description:*   Windows Server 2003 - Applies standard service monitoring for Windows 2003 Servers.

- **Windows Server 2008/2008 R2**

  ➢ *Policy View:*   zz[SYS] Policy - OS_Win 2008 Server

  ➢ *Description:*   Windows Server 2008/2008 R2 - Applies standard service monitoring for Windows 2008/2008 R2 Servers.

- **Windows Server 2012**

  ➢ *Policy View:*   zz[SYS] Policy - OS_Win 2012 Server

  ➢ *Description:* Windows Server 2012 - Applies standard service monitoring for Windows 2012 Servers.

[System].Core.Org Specific Policies.Monitoring.Server.Hardware

- **Dell PowerEdge**

  ➢ *Policy View:*   zz[SYS] Policy - HW_Dell PowerEdge

- ➢ *Description:* Dell PowerEdge - Applies Dell PowerEdge server hardware specific monitoring and alerting. This monitoring may require specific Dell PowerEdge server management tools to be installed on the server machine.
- ▪ **HP ProLiant**
  - ➢ *Policy View:* zz[SYS] Policy - HW_HP ProLiant
  - ➢ *Description:* HP ProLiant - Applies HP ProLiant server hardware specific monitoring and alerting. This monitoring may require specific HP ProLiant server management tools to be installed on the server machine.
- ▪ **IBM Series x**
  - ➢ *Policy View:* zz[SYS] Policy - HW_IBM Series X
  - ➢ *Description:* IBM Series x - Applies IBM Series X server hardware specific monitoring and alerting. This monitoring may require specific IBM Series X server management tools to be installed on the server machine.

[System].Core.Org Specific Policies.Monitoring.Server.Roles

- ▪ **Backup Exec Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Backup Exec Server
  - ➢ *Description:* Backup Exec Server - Applies monitoring to Backup Exec Servers.
- ▪ **Blackberry Enterprise Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Blackberry Server
  - ➢ *Description:* Blackberry Enterprise Server - Applies monitoring to Blackberry Enterprise Servers.
- ▪ **BrightStor ARCServe Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Brightstor ARCserve Server
  - ➢ *Description:* BrightStor ARCServe Server - Applies monitoring to BrightStor Servers.
- ▪ **Citrix Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Citrix Server
  - ➢ *Description:* Citrix Server - Applies monitoring to Citrix Servers.
- ▪ **DHCP Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_DHCP Server
  - ➢ *Description:* DHCP Server - Applies monitoring to DHCP Servers.
- ▪ **DNS Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_DNS Server
  - ➢ *Description:* DNS Server - Applies monitoring to DNS Servers.
- ▪ **Domain Controller**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Domain Controller
  - ➢ *Description:* Domain Controller - Applies monitoring to Domain Controllers.
- ▪ **Exchange 2003 Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Exchange 2003 Server
  - ➢ *Description:* Exchange 2003 Server - Applies monitoring to Exchange 2003 Servers.
- ▪ **Exchange 2007 Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Exchange 2007 Server
  - ➢ *Description:* Exchange 2007 Server - Applies monitoring to Exchange 2007 Servers.
- ▪ **Exchange 2010 Server**
  - ➢ *Policy View:* zz[SYS] Policy - Role_Exchange 2010 Server
  - ➢ *Description:* Exchange 2010 Server - Applies monitoring to Exchange 2010 Servers.
- ▪ **Exchange Server**

➤ *Policy View:*   zz[SYS] Policy - Role_Exchange Server

➤ *Description:*   Exchange Server - Applies monitoring to Exchange Servers

- **File Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_File Server
  - ➤ *Description:*   File Server - Applies monitoring to File Servers
- **FTP Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_FTP Server
  - ➤ *Description:*   FTP Server - Applies monitoring to FTP Servers.
- **IIS Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_IIS Server
  - ➤ *Description:*   IIS Server - Applies monitoring to IIS Servers
- **IMAP4 Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_IMAP4 Server
  - ➤ *Description:*   IMAP4 Server - Applies monitoring to IMAP4 Servers.
- **POP3 Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_POP3 Server
  - ➤ *Description:*   POP3 Server - Applies monitoring to POP3 Servers.
- **Print Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_Print Server
  - ➤ *Description:*   Print Server - Applies monitoring to Print Servers
- **SharePoint Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_SharePoint Server
  - ➤ *Description:*   SharePoint Server - Applies monitoring to SharePoint Servers
- **SMTP Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_SMTP Server
  - ➤ *Description:*   SMTP Server - Applies monitoring to SMTP Servers.
- **SQL Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_SQL Server
  - ➤ *Description:*   SQL Server - Applies monitoring to SQL Servers.
- **SQL Server 2005**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_SQL Server 2005
  - ➤ *Description:*   SQL Server 2005 - Applies monitoring to SQL 2005 Servers.
- **SQL Server 2008**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_SQL Server 2008
  - ➤ *Description:*   SQL Server 2008 - Applies monitoring to SQL 2008 Servers.
- **Terminal Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_Terminal Server
  - ➤ *Description:*   Terminal Server - Applies monitoring to Terminal Servers.
- **WINS Server**
  - ➤ *Policy View:*   zz[SYS] Policy - Role_WINS Server
  - ➤ *Description:*   WINS Server - Applies monitoring to WINS Servers.

[System].Core.Org Specific Policies.Monitoring.Workstation

- **Common Windows Workstation Monitoring**
  - ➤ *Policy View:*   zz[SYS] Policy - OS_All Windows Workstations

- ➢ *Description:* Common Windows Workstation Monitoring - Applies a common set of monitoring to all Windows Workstations. This includes hardware related Events Log, Windows Service, and common Windows Performance monitoring.

- **Windows Workstation (Core)**
  - ➢ *Policy View:* zz[SYS] Policy - OS_All Windows Workstations
  - ➢ *Description:* Windows Workstation (Core) - Applies an array of core Windows Workstation monitoring to Windows Workstations including monitoring for standard services, system performance, health reporting, and more.

- **Windows Vista**
  - ➢ *Policy View:* zz[SYS] Policy - OS_Win Vista
  - ➢ *Description:* Windows Vista - Applies standard service monitoring for Windows Vista machines.

- **Windows 7**
  - ➢ *Policy View:* zz[SYS] Policy - OS_Win 7
  - ➢ *Description:* Windows 7 - Applies standard service monitoring for Windows 7 machines.

- **Windows XP**
  - ➢ *Policy View:* zz[SYS] Policy - OS_Win XP
  - ➢ *Description:* Windows XP - Applies standard service monitoring for Windows XP machines.

- **Windows 8**
  - ➢ *Policy View:* zz[SYS] Policy - OS_Win 8
  - ➢ *Description:* Windows 8 - Applies standard service monitoring for Windows 8 machines.

[System].Core.Org Specific Policies.Monitoring.Security.Anti-Virus

- **AVG Tech**
  - ➢ *Policy View:* zz[SYS] Policy - AV_AVG Technologies
  - ➢ *Description:* AVG - Applies monitoring for AVG Technologies AntiVirus.

- **Kaspersky ES**
  - ➢ *Policy View:* zz[SYS] Policy - AV_Kaspersky ES
  - ➢ *Description:* Kaspersky ES - Applies monitoring for Kaspersky Endpoint Security.

- **McAfee**
  - ➢ *Policy View:* zz[SYS] Policy - AV_McAfee
  - ➢ *Description:* McAfee - Applies monitoring for McAfee AntiVirus.

- **Microsoft SE-FEP**
  - ➢ *Policy View:* zz[SYS] Policy - AV_Microsoft SE-FEP
  - ➢ *Description:* Microsoft SE-FEP - Applies monitoring for Microsoft Security Essentials and Forefront Endpoint Protection.

- **Sophos**
  - ➢ *Policy View:* zz[SYS] Policy - AV_Sophos
  - ➢ *Description:* Sophos - Applies monitoring for Sophos AntiVirus.

- **Symantec AV**
  - ➢ *Policy View:* zz[SYS] Policy - AV_Symantec AV
  - ➢ *Description:* Symantec zz[SYS] AV - Applies monitoring for Symantec AntiVirus.

- **Symantec EP**
  - ➢ *Policy View:* zz[SYS] Policy - AV_Symantec EP
  - ➢ *Description:* Symantec EP - Applies monitoring for Symantec Endpoint Protection.

- **Trend Micro**

➢ *Policy View:*   zz[SYS] Policy - AV_Trend Micro

➢ *Description:*   Trend Micro - Applies monitoring for Trend Micro AntiVirus.

[System].Core.Org Specific Policies.Monitoring.Utility

- **Update Lists By Scan**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows

  ➢ *Description:*   Update Lists By Scan - Applies a scheduled Update Lists By Scan to run on all Windows machines to keep performance counter, event log, and running services information current for each machine for accurate monitoring purposes.

- **Monitoring Cleanup**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows

  ➢ *Description:*   Monitoring Cleanup - As the last policy that contains Alerts and Monitor Sets, this policy effectively ensures that previously applied monitoring, (Event Logs Alerts and Monitor Sets assigned via other policies that are no longer needed due to role changes, etc.) gets removed.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Common Windows Patch Mgmt Settings

- **Deny Patch Settings**

  ➢ *Policy View:*   zz[SYS] Policy - Patch_Deny Patching Group

  ➢ *Description:*   Deny Patch Settings - Applies patch management settings to machines selected in the 'zz[SYS] Policy - Deny Patching Group' View. Sets Reboot Action to "If user logged in ask to reboot every 60 minutes until reboot occurs. Reboot if user not logged in". Sets Patch Policy Membership to the 'Deny Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".

- **Test Patch Settings**

  ➢ *Policy View:*   zz[SYS] Policy - Patch_Test Patching Group

  ➢ *Description:*   Test Patch Settings - Applies patch management settings to machines selected in the 'zz[SYS] Policy - Test Patching Group' View. Sets Reboot Action to "If user logged in ask to reboot every 60 minutes until reboot occurs. Reboot if user not logged in". Sets Patch Policy Membership to the 'Test Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".

- **Disable Windows Automatic Update**

  ➢ *Policy View:*   zz[SYS] Policy - Patch_Windows Auto Update Enabled

  ➢ *Description:*   Disable Windows Automatic Updates on machines that have Windows Automatic Update Enabled. If Windows Automatic Update is enabled and Kaseya patch management is being used, then Windows Automatic Update may conflict with the Kaseya patch management strategy and may result in the deployment of patches that have been denied or are still pending approval in Kaseya.

- **File Source Internet**

  ➢ *Policy View:*   zz[SYS] Policy - OS_All Windows

  ➢ *Description:*   File Source Internet - Sets the File Source for patch management to the Internet for all Windows machines so that patches are downloaded directly from the Microsoft patch and download servers. This policy is the default and can be overridden with an alternate policy that is applied to specific orgs or machine groups and which has precedence over this policy.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings

- **Workstation Patch Settings**
  - ➤ *Policy View:*   zz[SYS] Policy - OS_All Windows Workstations
  - ➤ *Description:*   Workstation Patch Settings - Applies patch management settings to Windows Workstations. Sets Reboot Action to "If user logged in ask to reboot every 60 minutes until reboot occurs. Reboot if user not logged in". Sets Patch Policy Membership to the 'Workstation Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".

- **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt)**
  - ➤ *Policy View:*   zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - ➤ *Description:*   Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt) - Applies Daily Auto Update schedules to Workstation Patching Policy members that are missing 10 or more approved patches. Auto Updates are scheduled M-F each week from 6am-6pm. This policy is generally used when customers have machines that are missing quite a few patches and they want to get those systems up to date over the course of days rather than weeks or months. Once the machines are patched, then they will not need to be patched on a daily basis anymore. Auto Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

- **Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt)**
  - ➤ *Policy View:*   zz[SYS] Policy - Patch_Workstation Patching Policy
  - ➤ *Description:*   Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt) - Applies Weekly Patch Scan and Auto Update schedules to Workstation Patching Policy members. Patch Scans are scheduled on Tue of each week from 6am-6pm and Auto Updates are scheduled on Wed of each week from 6am-6pm. This policy is generally used when customers want to take a more aggressive approach to patching to help minimize risk due to machines not being patched and thus want new patches deployed relatively quickly to machines. Auto Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Server Patch Mgmt Settings

- **Server Patch Settings**
  - ➤ *Policy View:*   zz[SYS] Policy - OS_All Windows Servers
  - ➤ *Description:*   Server Patch Settings - Applies patch management settings to Windows Servers. Sets Reboot Action to "Do not reboot after update", "When reboot required, send email to 'Patch Alerts' email address". Sets Patch Policy Membership to the 'Server Patching' patch policy. Sets Patch Alerts to generate an Alarm and Email the 'Patch Alerts' email address when a "Patch install fails" or the "Agent credential is invalid or missing".

- **Weekly Srvr Schedule (Scan W 6pm-6am)**
  - ➤ *Policy View:*   zz[SYS] Policy - OS_All Windows Servers
  - ➤ *Description:*   Weekly Srvr Schedule (Scan W 6pm-6am) - Applies Patch Scan schedule to Server Patch Policy members. Patch Scans are scheduled on Wed of each week from 6pm-6am. No patch Auto Update deployments are scheduled on servers by this policy.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings

- **File Source System Server**
    - ➢ *Policy View:*   zz[SYS] Policy - Network_10.11.12.x
    - ➢ *Description:*   File Source System Server - Sets the File Source for patch management to the System Server for all Windows machines so that patches are downloaded centrally by the System Server and then distributed from the System Server to the machines being patched.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings.Other Schedules.Daytime

- **Monthly Wkst Schedule (Scan 2nd W 6am-6pm/Auto Update 1st W 6am-6pm/Power Mgmt)**
    - ➢ *Policy View:*   zz[SYS] Policy - Patch_Workstation Patching Policy
    - ➢ *Description:*   Monthly Wkst Schedule (Scan 2nd W 6am-6pm/Auto Update 1st W 6am-6pm/Power Mgmt) - Applies Patch Scan and Automatic Update schedules to Workstation Patch Policy members. Patch Scans are scheduled on the 2nd Wed of the month from 6am-6pm. Automatic Updates are scheduled on the 1st Wed of the Month from 6am-6pm. This policy is generally used when customers want to take a conservative approach to patch management since scans and updates are performed only once a month, and updates are deployed at the beginning of the month. This means that the patches being deployed have been released for at least a month which allows for extensive testing of patches prior to their general deployment. Scans and Automatic Updates are performed in the day to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings.Nighttime

- **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6pm-6am/Power Mgmt)**
    - ➢ *Policy View:*   zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
    - ➢ *Description:*   Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6pm-6am/Power Mgmt) - Applies Daily Auto Update schedules to Workstation Patching Policy members that are missing 10 or more approved patches. Auto Updates are scheduled M-F each week from 6pm-6am. This policy is generally used when customers have machines that are missing quite a few patches and they want to get those systems up to date over the course of days rather than weeks or months. Once the machines are patched, then they will not need to be patched on a daily basis anymore. Automatic Updates are performed in the evening to help mitigate service disruption and the power management option is enabled on these schedules so that powered off machines can be woken up prior to performing these operations.

- **Weekly Wkst Schedule for 10+ Patches (Auto Update W 6pm-6am/Power Mgmt)**
    - ➢ *Policy View:*   zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
    - ➢ *Description:*   Weekly Wkst Schedule for 10+ Patches (Auto Update W 6pm-6am/Power Mgmt) - Applies Weekly Auto Update schedules to Workstation Patching Policy members that are missing 10 or more approved patches. Auto Updates are scheduled on Wed of each week from 6pm-6am. This policy is generally used when customers have machines that are missing quite a few patches and they want to get those systems up to date over the course of weeks rather than months. Once the machines are patched, then they will not need to be patched weekly anymore and will fall back to a monthly Patch Scan and Auto Update schedule. Auto Updates are performed in the evening to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

- **Weekly Wkst Schedule (Scan Tu 6pm-6am/Auto Update W 6pm-6am/Power Mgmt)**
  - ➤ *Policy View:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - ➤ *Description:* Weekly Wkst Schedule (Scan Tu 6pm-6am/Auto Update W 6pm-6am/Power Mgmt) - Applies Weekly Patch Scan and Auto Update schedules to Workstation Patching Policy members. Patch Scans are scheduled on Tue of each week from 6pm-6am and Auto Updates are scheduled on Wed of each week from 6pm-6am. This policy is generally used when customers want to take a more aggressive approach to patching to help minimize risk due to machines not being patched and thus want new patches deployed relatively quickly to machines. Scans and Automatic Updates are performed in the evening to help mitigate service disruption and the power management option is enabled on these schedules so that powered off machines can be woken up prior to performing these operations.

- **Monthly Wkst Schedule (Scan 2nd W 6pm-6am/Auto Update 1st W 6pm-6am/Power Mgmt)**
  - ➤ *Policy View:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - ➤ *Description:* Monthly Wkst Schedule (Scan 2nd W 6pm-6am/Auto Update 1st W 6pm-6am/Power Mgmt) - Applies Patch Scan and Automatic Update schedules to Workstation Patch Policy members. Patch Scans are scheduled on the 2nd Wed of the month from 6pm-6am. Automatic Updates are scheduled on the 1st Wed of the Month from 6pm-6am. Scans and Automatic Updates are performed in the evening to help mitigate service disruption and the power management option is enabled on these schedules so that powered off machines can be woken up prior to performing these operations. This policy is generally used when customers want to take a conservative approach to patch management since scans and updates are performed only once a month, and updates are deployed at the beginning of the month. This means that the patches being deployed have been released for at least a month which allows for extensive testing of patches prior to their general deployment.

- **Monthly Srvr Schedule (Scan 2nd W 6pm-6am)**
  - ➤ *Policy View:* zz[SYS] Policy - Patch_Server Patching Policy
  - ➤ *Description:* Monthly Srvr Schedule (Scan 2nd W 6pm-6am) - Applies Patch Scan schedule to Server Patch Policy members. Patch Scans are scheduled on the 2nd Wed of the month from 6pm-6am. No patch Auto Update deployments are scheduled on servers by this policy.

- **Monthly Srvr Schedule (Scan 2nd W 6pm-6am/Auto Update 1st Su 12am-4am)**
  - ➤ *Policy View:* zz[SYS] Policy - Patch_Server Patching Policy
  - ➤ *Description:* Monthly Srvr Schedule (Scan 2nd W 6pm-6am/Auto Update 1st Su 12am-4am) - Applies Patch Scan and Automatic Update schedules to Server Patch Policy members. Patch Scans are scheduled on the 2nd Wed of the month from 6am-6pm. Automatic Updates are scheduled on the 1st Sun of the Month from 12am-4am. This policy is generally used when customers want to take a conservative approach to patch management since scans and updates are performed only once a month, and updates are deployed at the beginning of the month. This means that the patches being deployed have been released for at least a month which allows for extensive testing of patches prior to their general deployment. Scans and Automatic Updates are performed on the weekend early in the morning so that production time and users are less affected by any service outages related to patching servers.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings

- **Weekly Macintosh Workstation Software Update (Install Recommended W 6am-6pm)**
  - ➤ *Policy View:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - ➤ *Description:* Weekly Macintosh Workstation Software Update (Install Recommended W 6am-6pm) - Applies a Mac Software Update to run Wed 6am-6pm every week that will install

recommended Macintosh Software updates on Macintosh Workstations. Software Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Server Software Update Settings

- **Monthly Macintosh Server Software Update (Install Recommended 1st Su 12am-4am)**
  - ➢ *Policy View:* zz[SYS] Policy - OS_All Mac OS X Servers
  - ➢ *Description:* Monthly Macintosh Server Software Update (Install Recommended 1st Su 12am-4am) - Applies a Mac Software Update to run on the 1st Sun of every month that will install recommended Macintosh Software updates on Macintosh Servers. This will keep the Mac Servers current with recommended updates.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Other Macintosh Software Update Settings

- **Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6am-6pm)**
  - ➢ *Policy View:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - ➢ *Description:* Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6am-6pm) - Applies a Mac Software Update to run on the 1st Wed of every month from 6am-6pm that will install recommended Macintosh Software updates on Macintosh Workstations. Software Updates are performed in the daytime to handle customers where machines are generally powered off at night, but the power management option is enabled on these schedules so that any machines powered off during the day can be woken up prior to performing these operations.
- **Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am)**
  - ➢ *Policy View:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - ➢ *Description:* Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am) - Applies a Mac Software Update to run on the 1st Wed of every month from 6pm-6am that will install recommended Macintosh Software updates on Macintosh Workstations. Software Updates are performed in the evening to help mitigate service disruption and the power management option is enabled on these schedules so that powered off machines can be woken up prior to performing these operations.
- **Monthly Macintosh Workstation Software Update (Install All 1st W 6pm-6am)**
  - ➢ *Policy View:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - ➢ *Description:* Monthly Macintosh Workstation Software Update (Install All 1st W 6pm-6am) - Applies a Mac Software Update to run on the 1st Wed of every month from 6pm-6am that will install all Macintosh Software updates on Macintosh Workstations. Software Updates are performed in the evening to help mitigate service disruption and the power management option is enabled on these schedules so that powered off machines can be woken up prior to performing these operations.

[System].Core.Org Specific Policies.Patch / Update Management.Linux

- **Monthly Linux Package Updates/Upgrades (Install 1st W 6pm-6am)**
  - ➢ *Policy View:* zz[SYS] Policy - OS_All Linux
  - ➢ *Description:* Monthly Linux Package Updates/Upgrades (Install 1st W 6pm-6am) - Applies a Linux Package Update/Upgrades procedure to run on the 1st Wed of every month. This will keep Linux machines updated and current for the various software components that are installed.

Patch Policy Details

Deny Patching	Default Approval Policy
Security Update - Critical (High Priority)	Denied
Security Update - Important (High Priority)	Denied
Security Update - Moderate (High Priority)	Denied
Security Update - Low (High Priority)	Denied
Security Update - Non-rated (High Priority)	Denied
Critical Update (High Priority)	Denied
Update Rollup (High Priority)	Denied
Service Pack (Optional - Software)	Denied
Update (Optional - Software)	Denied
Feature Pack (Optional - Software)	Denied
Tool (Optional - Software)	Denied

Server Patching	
Security Update - Critical (High Priority)	Pending Approval
Security Update - Important (High Priority)	Pending Approval
Security Update - Moderate (High Priority)	Pending Approval
Security Update - Low (High Priority)	Pending Approval
Security Update - Non-rated (High Priority)	Pending Approval
Critical Update (High Priority)	Pending Approval
Update Rollup (High Priority)	Pending Approval
Service Pack (Optional - Software)	Pending Approval
Update (Optional - Software)	Pending Approval
Feature Pack (Optional - Software)	Pending Approval
Tool (Optional - Software)	Pending Approval

Test Patching	
Security Update - Critical (High Priority)	Approved
Security Update - Important (High Priority)	Approved
Security Update - Moderate (High Priority)	Approved
Security Update - Low (High Priority)	Approved
Security Update - Non-rated (High Priority)	Approved
Critical Update (High Priority)	Approved
Update Rollup (High Priority)	Pending Approval
Service Pack (Optional - Software)	Pending Approval
Update (Optional - Software)	Pending Approval
Feature Pack (Optional - Software)	Pending Approval
Tool (Optional - Software)	Pending Approval

Workstation Patching

Security Update - Critical (High Priority)	Approved
Security Update - Important (High Priority)	Approved
Security Update - Moderate (High Priority)	Approved
Security Update - Low (High Priority)	Approved
Security Update - Non-rated (High Priority)	Approved
Critical Update (High Priority)	Approved
Update Rollup (High Priority)	Pending Approval
Service Pack (Optional - Software)	Pending Approval
Update (Optional - Software)	Pending Approval
Feature Pack (Optional - Software)	Pending Approval
Tool (Optional - Software)	Pending Approval

Agent Procedures

In This Section

Core.0 Common Procedures

Core.0 Common Procedures.Reboot/Shutdown/Logoff

- **Force User Logoff**
  - ➤ Logs off the currently logged on user.
- **Reboot-Ask-No**
  - ➤ If user is logged in, ask if it is OK to reboot; assume no after 5 min. If user is not logged in, go ahead and reboot. This script calls Reboot-Ask-No-2 to ask the user.
- **Reboot-Ask-No-2**
  - ➤ *** DO NOT SCHEDULE THIS SCRIPT!! *** This script is called by the Reboot-Ask-No script and must not be scheduled by itself.
- **Reboot-Ask-Yes**
  - ➤ If user is logged in, ask if it is OK to reboot; assume yes after 5 min. If user is not logged in, go ahead and reboot. This script calls Reboot-Ask-Yes-2 to ask the user.
- **Reboot-Ask-Yes-2**
  - ➤ *** DO NOT SCHEDULE THIS SCRIPT!! *** This script is called by the Reboot-Ask-Yes script and must not be scheduled by itself.
- **Reboot-Force**
  - ➤ Force an immediate reboot.
- **Reboot-Nag**

➢ If user is logged in, ask to reboot every 5 minutes until the user allows the reboot. If user is not logged in, go ahead and reboot. This script calls Reboot-Nag-2 to ask the user.

▪ **Reboot-Nag-2**

➢ *** DO NOT SCHEDULE THIS SCRIPT!! *** This script is called by the Reboot-Nag script and must not be scheduled by itself.

▪ **Reboot-No-User**

➢ Reboot the machine only is a user is not logged in.

▪ **Reboot-Warn**

➢ If the user is logged in, warn the user that a reboot will happen in 5 min. If the user is not logged in, go ahead and reboot.

▪ **Reboot - Prompt User to reboot every 15 mins until they answer Yes**

➢ This Script will prompt for a reboot every 15 Min

▪ **Shutdown Computer**

➢ Shutdown the agent machine using the windows shutdown.exe utility.

Core.1 Windows Procedures

Core.1 Windows Procedures.Desktops.Auditing

▪ **Audit BIOS Info via WMI**

➢ Uses WMIC to get BIOS Info, writes it to a file and retrieves the file to the system's GetFile() folder and writes an entry to the Agent Procedure log with the detected BIOS Info.

▪ **Audit BOOT.INI**

➢ Audits contents of C:\BOOT.INI if it exists, writes an entry to the Agent Procedure log, and retrieves a copy of BOOT.INI to the system's GetFile() folder.

▪ **Audit Files (Any File Types Entered)**

➢ Searches for all files by using a set of file masks you enter when scheduling the procedure and creates a simple TXT log file and CSV file based on file names you also enter that listi the files found with full path/filename, date and time last accessed, size in bytes, owner and filename.

  ✓ Output files are created in the #agenttemp# folder defined in Step 1.

  ✓ The TXT log file name is defined by the #logfile# variable in Step 2.

  ✓ The CSV file name is defined by the #csvfile# variable in Step 3.

  ✓ The file masks are defined by the #filemasks# variable in Step 4.

  ✓ Both output files are uploaded to the Kaseya server for review and anaysis under that machines profile Documents folder.

  ✓ The TXT log file is additionally written to the script log for reporting.

  ✓ This script can support alerts on file changes as well by altering Steps .

▪ **Audit Files (PST and OST)**

➢ Searches for all PST/OSTfiles by using a set of file masks and creates a simple TXT log file and CSV file listing of the files found with full path/filename, date and time last accessed, size in bytes, owner and filename.

  ✓ Output files are created in the #agenttemp# folder defined in Step 1.

  ✓ The TXT log file name is defined by the #logfile# variable in Step 2.

  ✓ The CSV file name is defined by the #csvfile# variable in Step 3.

  ✓ The file masks are defined by the #filemasks# variable in Step 4.

  ✓ Both output files are uploaded to the Kaseya server for review and anaysis under that machines profile Documents folder.

    ✓   The TXT log file is additionally written to the script log for reporting.

    ✓   This script can support alerts on file changes as well by altering Steps .

- **Audit Internet Speed (WEB100CLT)**
  - ➢ Uses the NDT client utility for Windows (web100clt.exe). Connects to the Public NDT Server you enter when running/scheduling the procedure (see http://e2epi.internet2.edu/ndt/ndt-server-list.html for a list of servers) and performs an Internet speed test (up/down) as well other network diagnostics. The output file (Internet_Speed.txt) is retrieved to the systems GetFile folder.

- **Audit IRPStackSize Registry Key**
  - ➢ Audits the IRPStackSize value. Event Id 2011 can be caused by Anti-Virus and a number of other types of software. See http://support.microsoft.com/kb/177078.

- **Audit Local Admin Accounts**
  - ➢ Logs the user accounts that are part of the Administrators group on the local machine to the Agent Procedure log.

- **Audit Local Guest Accounts**
  - ➢ Log the user accounts that are part of the Guests group on the local machine to the Agent Procedure log. If accounts are reported, they are enabled.

- **Audit Local User Accounts**
  - ➢ Log the user accounts defined on the machine to the Agent Procedure log.

- **Audit MP3 File Count**
  - ➢ Counts the number of MP3 files on the C: drive of the machine and writes an entry in the Agent Procedure log indicating this number.

- **Audit Open and Listening TCP Ports**
  - ➢ Audits open and listening TCP ports on Windows using NETSTAT and then retrieves the results to the systems GetFile folder

- **Audit PageFile Locations**
  - ➢ Audits the PageFile locations on Windows machines and writes an entry to the Agent Procedure log with the information.

- **Audit Running Services (NET START)**
  - ➢ Audits the currently started services on a Windows machine and retrieves the list of those services to the systems GetFile folder.

- **Audit Services (SC QUERY)**
  - ➢ Uses SC QUERY to audit the list of Windows Services to a file and retrieves the file to the systems Get File folder.

- **Audit Services Registry Key**
  - ➢ Use the REG command to query the HKLM\System\CurrentControlSet\Services registry key for an agent and retrieves the results to the systems GetFile folder.

- **Audit Uninstall Registry Key**
  - ➢ Use the REG command to query the HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall registry key for the machine and retrieve the results to the systems GetFile folder.

- **Audit USB Plug-N-Play Devices**
  - ➢ Uses a VBS and WMI (Win32_PnPEntity class) to audit the USB devices on a Windows machine. Results are retrieved to the systems GetFile folder.

- **Audit User Video Resolution**
  - ➢ Uses a VBS to audit the current users video diaplay resolution setting. Writes the result to the Agent Procedure Log as well as to a Custom System Information Field called User Video Resolution.

- **Audit Windows Monitor Info**
  - ➢ Uses a VBS and WMI (root\CIMV2:Win32_DesktopMonitor class) to audit Windows Monitor Information. Write output to a file and retrieves the file to the systems GetFile folder.
- **Audit Windows Monitor EDID Info**
  - ➢ Uses a VBS with WMI to detect Monitor EDID information (Monitor Manufacturer, Monitor Model, and Monitor Serial Number) and write the detected information to the Agent Procedure log and to Custom System Info fields.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS

- **Audit All Share Sessions and Users (NET SESSION)**
  - ➢ Uses NET SESSION to dump a basic listing of the sessions to shares on an agent and uploads to Docs\Shares-NTFS folder so that files can be viewed via Documents function/machine summary tab.
- **Audit All Shared Files Opened and Users (NET FILE)**
  - ➢ Uses NET FILE to dump a basic listing of the open files for all shares on an agent and uploads to Docs\Shares-NTFS folder so that files can be viewed via Documents function/machine summary tab.
- **Audit All Shares (NET SHARE)**
  - ➢ Uses NET SHARE to dump a basic listing of the shares on an agent and uploads to Docs\Shares-NTFS folder so that files can be viewed via Documents function/machine summary tab.
- **Audit Effective User/Group Fldr Perms (ACCESSCHK)**
  - ➢ Uses ACCESSCHK from Microsoft SysInternals to check the effective permissions of a local pc/domain based user/group object on a folder. Edit this script in Steps 2-6 for these variables:

    pcdom = computername or domain name of the user or group
    usrgrp = username or group name to evaluate
    drive = drive letter where the folder exists
    folder = full path of the folder to be audited
    fldrdesc = a descriptive name for folder to audit (no special chars)
- **Audit Non-Admin Shares (SRVCHECK)**
  - ➢ Uses SRVCHECK to dump a basic listing of the non-admin shares on an agent and uploads to Docs\Shares-NTFS folder so that files can be viewed via Documents function/machine summary tab.
- **Audit Shared Folders (DUMPSEC)**
  - ➢ Uses DUMPSEC to create a report of all shares with their paths, accounts, owners and access permissions, and uploads to Docs\Shares-NTFS folder so that files can be viewed via Documents function/machine summary tab.
- **Audit Shared Folders and ACLs (VBS/WMI)**
  - ➢ Uses a VBS with WMI to audit all local shares, share and NTFS permissions.
- **Audit Shared Printers (DUMPSEC)**
  - ➢ Uses DUMPSEC to create a report of all printers with names, accounts, owners and access permissions, and uploads to Docs\Shares-NTFS folder so that files can be viewed via Documents function/machine summary tab.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS.Audit Admin Shares

- **Audit Automatic Admin Shares**
  - ➢ Uses NET SHARE to audit automatic admin shares like C$, etc. The results are retrieved to the systems Documents folder under a Share-NFTS subfolder.
- **Audit Automatic Admin Shares Setting**

> ➢ Based on the OS of the machine, checks for the existence and value of AutoShareServer or AutoShareWkst in the Windows Registry and writes an Agent Procedure log entry indicating whether this feature is enabled or disabled.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Dell

- **Inventory Dell BIOS Settings via DCCU**
  - ➢ Uses the Dell Client Configuration Utility (DCCU) to inventory the BIOS of a Dell business class machine. The results are retrieved to the systems Get File folder.
- **Set Dell BIOS Settings via DCCU**
  - ➢ Sets Dell BIOS settings based on the setting and value supplied when scheduled. The format for the Dell BIOS setting supplied must be that used by the Dell Client Configuration Utility (DCCU).

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.HP

- **HP BiosConfigUtility GetConfig**
  - ➢ Uses the HP Bios Config Utility to inventory the BIOS of a HP business class machine. The results are retrieved to the systems Get File folder.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Lenovo

- **Get Lenovo BIOS Settings via WMI-VBS**
  - ➢ Uses VBS and WMI to get all BIOS Settings on Lenovo systems.
- **Set Lenovo BIOS Settings via WMI-VBS**
  - ➢ Uses VBS and WMI to configure BIOS settings on Lenovo systems. Prompts for the Lenovo BIOS Setting name and value when run/scheduled.

Core.1 Windows Procedures.Desktops.Machine Control.File Sharing

- **Disable Simple File Sharing (Sets ForceGuest=0) on Windows XP**
  - ➢ Disables the Simple File Sharing (Sets ForceGuest=0) feature on Windows XP systems and after doing so, stops and restarts the Server service so that the change goes into effect.
- **Enable Automatic Admin Shares**
  - ➢ Enables AutoShareWks feature on Windows Workstations so that Admin Shares are automatically created when the Server service starts. This agent procedure does NOT restart the Server (lanmanserver) service.
- **Enable Simple File Sharing (Sets ForceGuest=1) on Windows XP**
  - ➢ Enables the Simple File Sharing (ForceGuest=1) feature on Windows XP systems and after doing so, stops and restarts the Server service so that the change goes into effect.
- **Disable Automatic Admin Shares**
  - ➢ Disables AutoShareWks feature on Windows Workstations so that Admin Shares are automatically created when the Server service starts. This agent procedure does NOT restart the Server (lanmanserver) service.

Core.1 Windows Procedures.Desktops.Machine Control.File System

- **Convert File System on Drive to NTFS**
  - ➢ Convert the file system format on the system drive (i.e. the boot partition) to NTFS from FAT/FAT32. This only works on those operating systems which support NTFS (Windows NT4 / 2000 / XP / 2003 / Vista)
- **Delete Files Based on Modified Date**
  - ➢ Prompts for the Age of Files to Delete, Full Drive\Path to Start delete operation, and a File Mask to be deleted. Then uses FORFILES to recursively process all folders in the Full Drive/Path entered deleting files matching the File Mask if they are older than the Age entered.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Block Websites

- **Block "Any" Website**
  - ➢ This script will edit the windows hosts file and point any website that you enter in the prompt to localhost, essentially blocking access to the website from that endpoint. This can be useful to employers trying to improve productivity or just great for laughs.
- **Clear all blocked websites**
  - ➢ Used to remove all windows hosts file edits. Refreshes the default hosts file settings.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Diagnostics

- **Network Diagnostics Test (NETSH)**
  - ➢ Uses NETSH to perform a network diagnostic test and retrieves the results to the systems Documents folder under a Network Diags subfolder.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Network Connection

- **Configure Local Area Connection to Utilize DHCP**
  - ➢ Uses NETSH to change the configuration of the Windows named network connection called "Local Area Connection" to utilize DHCP for its IP Address, DNS and WINS settings.
- **Fix RAS DNS Priority**
  - ➢ Fixes the RAS DNS binding priority issue described in http://support.microsoft.com/kb/311218/en-us.
- **Get Windows IP Configuration (IPCONFIG /ALL)**
  - ➢ Uses IPCONFIG /ALL to get the IP Addressing Configuration of all enabled network connections on a Windows machine. The results are retrieved to the systems Get Files folder.
- **Release and Renew IP Address**
  - ➢ Uses a batch file to release and renew a Windows machines IP address.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Dell

- **Enable Wake-On-LAN in Dell BIOS (DCCU)**
  - ➢ Uses the Dell Client Configuration Utility (DCCU) to enable Wake-On-LAN within the BIOS of Dell business class machines.
- **Enable Wake-On-LAN in Dell BIOS (CCTK)**
  - ➢ Uses the Dell Client Configuration Tool Kit (CCTK) to enable Wake-On-LAN within the BIOS of Dell business class machines.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.HP

- **Enable Wake-On-LAN in HP BIOS**
  - ➢ Uses the HP BIOS Configuration Utility to enable Wake-On-LAN within the BIOS of HP business class machines.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Lenovo

- **Enable Wake-On-LAN in Lenovo BIOS**
  - ➢ Uses VBS and WMI to enable Wake-On-LAN within the BIOS of Lenovo business class machines.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Windows

- **Enable Wake-On-LAN In Windows for all NICs**
  - ➢ Uses VBS to enable the Power Management Wake-On-LAN feature on each Windows network interface. This allows the machine to be woken via magic packet when hibernated or suspended. WOL features within the BIOS must also be enabled for WOL to work.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wireless

- **Disable Wireless Networking Devices**
  - ➢ Uses DEVCON.EXE to disable Wireless Networking Devices on a Windows system.
- **Enable Wireless Networking Devices**
  - ➢ Uses DEVCON.EXE to enable Wireless Networking Devices on a Windows system.
- **Disable NIC on Wireless Network Connection**
  - ➢ Uses NETSH to disable the NIC associated with the Windows named network connection called "Wireless Network Connection".
- **Enable NIC on Wireless Network Connection**
  - ➢ Uses NETSH to enable the NIC associated with the Windows named network connection called "Wireless Network Connection".

Core.1 Windows Procedures.Desktops.Machine Control.Reboot/Shutdown

- **Hibernate Now**
  - ➢ Causes a Windows machine to go into a hibernate state immediately.
- **Suspend Now**
  - ➢ Causes a Windows machine to go into a suspend state immediately.
- **Shutdown Abort**
  - ➢ Shutdown the computer using Shutdown.exe
- **Shutdown in 60 Seconds**
  - ➢ Shutdown the computer using Shutdown.exe in 60 seconds
- **Lock Desktop**
  - ➢ Causes a Windows machines desktop to lock requiring the currently logged on user credentials to unlock the desktop.

Core.1 Windows Procedures.Desktops.Machine Control.System Restore

- **List All System Restore Points**
  - ➢ Uses WMIC to enumerate all System Restore Points and retrieves list to the systems Get File folder.
- **Enable System Restore on All Drives**
  - ➢ Uses DISKPART to enumerate all local partitions and then feeds this list of drives into WMIC to disable System Restore on each volume. This will remove any existing System Restore Points.
- **Disable System Restore All Drives**
  - ➢ Uses DISKPART to enumerate all local partitions and then feeds this list of drives into WMIC to disable System Restore on each volume. This will remove any existing System Restore Points.
- **Create a Named System Restore Point**
  - ➢ Uses WMIC to create a System Restore Point

Core.1 Windows Procedures.Desktops.Machine Control.Trusted Sites

- **Add Trusted Sites**
  - ➢ Runs a registry procedure on the machine to allow anything from the domain to run ActiveX. In this example it adds Kaseya.net.

Core.1 Windows Procedures.Desktops.Machine Control.USB/Disk Drive Control

- **Disable USB Drives**

➤ **Must reboot endpoint after making change via script** There is a simple registry change that will keep the USB storage drivers from starting when the system boots. Keeps people from walking up to a PC and copying data off with a USB key, but allows you to keep your scanner, keyboard, and mouse working.

➤ As always – back your system up before messing around in the registry. Just open regedit and browse to this key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Notice the value 'Start' Switch this value to 4, and USB storage devices are disabled. Switch this value to 3, and USB storage devices are enabled.

▪ **Enable USB Drives**

➤ **Must reboot endpoint after making change via script** There is a simple registry change that will keep the USB storage drivers from starting when the system boots. Keeps people from walking up to a PC and copying data off with a USB key, but allows you to keep your scanner, keyboard, and mouse working.

➤ As always – back your system up before messing around in the registry. Just open regedit and browse to this key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Notice the value 'Start' Switch this value to 4, and USB storage devices are disabled. Switch this value to 3, and USB storage devices are enabled.

▪ **Disable USB Drives Write Protection**

➤ Disables USB Device Write Protection on Windows machines running XP SP2 or later OSes (see http://technet.microsoft.com/en-us/library/bb457157.aspx)

▪ **Enable USB Drives Write Protection**

➤ Enables USB Device Write Protection on Windows machines running XP SP2 or later OSes (see http://technet.microsoft.com/en-us/library/bb457157.aspx)

▪ **Disable CD-ROM Drives**

➤ Disables CD-ROM Disk Devices

▪ **Enable CD-ROM Drives**

➤ Enables CD-ROM Disk Devices

▪ **Disable High Capacity Floppy Drives**

➤ Disables High Capacity Floppy Disk Devices

▪ **Enable High Capacity Floppy Drives**

➤ Enables High Capacity Floppy Disk Devices

▪ **Disable Floppy Disk Drives**

➤ Disables Floppy Disk Devices

▪ **Enable Floppy Disk Drives**

➤ Enables Floppy Disk Devices

▪ **Restrict Desktop Access**

➤ Restricts access to the "Desktop" in Explorer. The "Desktop" will appear empty and users will not be able to use or access it.

▪ **Unrestrict Desktop Access**

➤ Enables access to the "Desktop" in Explorer.

▪ **Hide and Restrict Access to All Drives (A-Z) in Explorer**

➤ Uses NoViewOnDrive and NoDrives registry settings to hide and restrict access to all drive letters A-Z on a Windows machine.

▪ **Hide and Restrict Access to C and D Drives in Explorer**

➤ you can choose "Block C only" or "Block D only" or "Block all drives" with one of among "01.Block" procedures

▪ **Hide and Restrict Access to Any List of Drives in Explorer**

➢ you can choose "Block C only" or "Block D only" or "Block all drives" with one of among "01.Block" procedures

▪ **Unhide and Unrestrict Access to All Drives (A-Z) in Explorer**

➢ Removes previous drive access restrictions that may be in place.

➢ Note: Windows supports the ability to block access to view various drive letters within Explorer. This restriction prevents users from using My Computer or Explorer to access the content of selected drives. Also, they cannot use Run, Map Network Drive, or the Dir command to view the directories on these drives. This Agent Procedure removes any restriction to that effect.

Core.1 Windows Procedures.Desktops.Machine Control.User Access Control

▪ **Set User Access Control (UAC) to Always Notify**

➢ Sets User Access Control to Always Notify in Windows Vista, Windows 7, and Windows 8.

▪ **Set User Access Control (UAC) to Default Notify**

➢ Sets User Access Control to Default Notify in Windows Vista, Windows 7, and Windows 8.

▪ **Set User Access Control (UAC) to Insecure Notify**

➢ Sets User Access Control to Insecure Notify in Windows Vista, Windows 7, and Windows 8.

▪ **Set User Access Control (UAC) to Never Notify**

➢ Disables User Access Control in Windows Vista, Windows 7, and Windows 8.

Core.1 Windows Procedures.Desktops.Machine Control.Windows Configuration

▪ **Hide an Account from Windows Fast User Switching Logon Screen**

➢ This script will add a DWORD value with the value of "support user" and data to 0. After a reboot, the PC will no longer display the "support user" at the welcome screen

▪ **Unhide an Account from Windows Fast User Switching Logon Screen**

➢ This script will add a DWORD value with the value of "support user" and data to 0. After a reboot, the PC will no longer display the "support user" at the welcome screen

▪ **Disable Show Hidden Operating System Files**

➢ Disables the Show Hidden Operating System Files option within Windows Explorer.

▪ **Enable Display the Contents of System Folders**

➢ Enables the Display Contents of System Folders option within Windows Explorer.

▪ **Enable Hide Extensions for Known File Types**

➢ Enables the Enable Hide Extensions for Known File Types option within Windows Explorer.

▪ **Enable Show Hidden Files and Folders**

➢ Enables the Show Hidden Files and Folders option within Windows Explorer.

▪ **Enforce Windows Minimum Password Length of 8 Characters**

➢ Forces Windows to reject passwords that do not meet a minimum password length. Useful to help stop people from using trivial passwords where security is an issue. Add a new REG_BINARY value of 'MinPwdLen', and set the data to the minimum number of characters required for a password to be accepted. The following example is 8. Note: This does not affect existing passwords, only new or changed.

▪ **Suppress Balloon Pop-Ups for Current Windows User**

➢ Suppresses All Balloon Pop-Ups in Windows for the logged on user. See http://msdn.microsoft.com/en-us/library/ms940877(v=winembedded.5).aspx

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Check Disk

▪ **Check Disk All Drives**

➢ Uses DISKPART to enumerate all local partitions and then feeds this list of drives into CHKDSK to repair each volume.

- **Check Disk System Drive (Schedule at Next Restart)**
  - ➢ Executes a CHKDSK command on the system drive. The results of the maintenance are evaluated by the Check Disk Verify script.
- **Check Disk System Drive (Analysis Only)**
  - ➢ Executes a CHKDSK command on the system drive. The results of the maintenance are evaluated, a log entry is written to the agent procedure log with the results, and the results are retrieved to the systems Get File folder.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Defragmentation

- **Defragment All Drives**
  - ➢ Uses DISKPART to enumerate all local partitions and then feeds this list of drives into DEFRAG to optimize each volume. Retrieves DEFRAG results for all drives to the systems GetFile folder.
- **Defragment System Drive (Analysis Only)**
  - ➢ Performs a defragmentation analysis on the system drive in Windows (usually C:). Defragmentation results are written to the agent procedure log.
- **Defragment Page File & Registry**
  - ➢ Use PageDefrag utility from Sysinternals to defrag the system pagefile and registry and reboot (Windows XP only).
- **Defragment System Drive (Analysis & Prompt User If Reqd)**
  - ➢ Performs a defragmentation analysis on the system drive in Windows (usually C:). Defragmentation results are written to the agent procedure log. If a user is logged onto the machine, then the procedure asks them if they want to run a full defragmentation on the drive and performs one if they answer yes.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Disk Cleanup

- **Windows Disk Cleanup**
  - ➢ Sets the "sageset" registry entries for cleanmgr.exe and then executes cleanmgr.exe with the "sagerun" parameter to automatically clean files in the following locations: Active Setup Temp Folder Content Indexer Cleaner Downloaded Program Files Internet Cache Files Memory Dump Files Old ChkDsk Files Recycle Bin Remote Desktop Cache Files Setup Log Files Temporary Files Temporary Offline Files WebClient and WebPublisher Cache

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Flush DNS

- **Flush DNS Resolver Cache**
  - ➢ Flushes and resets the contents of the DNS client resolver cache by performing IPCONFIG /FLUSHDNS

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.IE Files Management

- **Clear Internet Explorer Cookies**
  - ➢ Clears the Internet Explorer Cookies for the currently logged on user.
- **Clear Internet Explorer Form Data**
  - ➢ Clears the Internet Explorer Form Data for the currently logged on user.
- **Clear Internet Explorer History**
  - ➢ Clears the Internet Explorer History for the currently logged on user.
- **Clear Internet Explorer Passwords**
  - ➢ Clears the Internet Explorer Passwords for the currently logged on user.
- **Clear Internet Explorer Temp Files**

➢ Clears the Internet Explorer Temporary Files for the currently logged on user.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Create Weekly Desktop Maintenance System Restore Point**
  - ➢ Uses WMIC to create a System Restore Point called Weekly Desktop Maintenance. This agent procedure can be called at the beginning of the Workstation Weekly Maintenance Procedure.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Create Patch Management System Restore Point**
  - ➢ Uses WMIC to create a System Restore Point called Patch Management. This agent procedure can be called prior to a patch deployment through a Automatic Update Pre-Agent Procedure.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.TEMP Files

- **Clear User TEMP Folder**
  - ➢ Deletes all files and folders within and below the logged on users %TEMP% folder that are not currently locked/open by Windows.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Time Sync

- **Synchronize Time via SNTP**
  - ➢ Sets the windows clock to retrieve the time from time.windows.com

Core.1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance

- **Workstation Weekly Maintenance**
  - ➢ Executes all the Weekly Desktop Maintenance tasks, schedule this script to run during your maintenance window.

Core.1 Windows Procedures.Desktops.Maintenance.Maintenance Notifications

- **Weekly Desktop Maintenance Reminder**
  - ➢ This script is designed to run in the daytime prior to desktop Patching maintenance. Will send a message to a desktop end user indicating they should leave their machine on overnight.

Core.1 Windows Procedures.Desktops.Software Control.Internet Explorer

- **Set Default Internet Explorer Home Page**
  - ➢ Set Default Page on Internet Explorer. Just change the site in step 1.

Core.1 Windows Procedures.Desktops.Software Control.Windows Firewall

- **Disable Windows Firewall**
  - ➢ Uses NETSH to disable the Windows Firewall

Core.1 Windows Procedures.Servers.Active Directory.AD Replication

- **Perform an AD Replication Check Using REPADMIN**
  - ➢ Runs a Replication Check on Active Directory Services using teh REPADMIN utility. Sends results via email, you MUST update the email address to receive the results.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2003

- **ExBPA Report 2003 server**

➢ Designed for Exchange 2003. Uses the Exchange Best Practice Analyzer to create a report of any errors. MS Logparser 2.0 is then used to parse the results and email a final report to the email address of the admin that runs/schedules the agent procedure. The Exchange Best Practice Analyzer must be installed prior to using this agent procedure.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2007

- **ExBPA Report 2007 server**
  - ➢ Designed for Exchange 2007. Uses the Exchange Best Practice Analyzer to create a report of any errors. MS Logparser 2.0 is then used to parse the results and email a final report to the email address of the admin that runs/schedules the agent procedure. The Exchange Best Practice Analyzer must be installed prior to using this agent procedure.

Core.1 Windows Procedures.Servers.IIS Server

- **Perform an IISRESET on IIS Server**
  - ➢ Performs an IISReset on machine.

Core.1 Windows Procedures.Servers.Maintenance

- **Weekly Server Maintenance**
  - ➢ Executes all the Weekly Desktop Maintenance tasks.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Disk Usage

- **DiskUsage.GetDirTree.C-D-E-F-G-M-N**
  - ➢ Returns disk usage on C, D, E, F, G, M and N Drives. Writes the disk usage tree results to the Agent Procedure Log. Drives that do not exist will not display any disk usage results.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Get Process List

- **Performance.Get Process List**
  - ➢ Uses kperfmon.exe to obtain the process list, CPU % and memory consumption. This script may be configured to execute when performance monitor counters raise an alarm. Writes results to Agent Procedure Log.

Core.1 Windows Procedures.Servers.Print Server

- **Clear Print Spooler Queues**
  - ➢ Stops the Print Spooler, clears out queues and restarts the Print Spooler.

Core.1 Windows Procedures.Servers.Service Control Manager

- **Compile SCM**
  - ➢ Recompiles the Service Control Manager to verify SCM events are logged to the system log.

Core.1 Windows Procedures.Servers.Terminal Server

- **Terminal Server - Logoff Disconnected Sessions**
  - ➢ Logs off all disconnected sessions of a Terminal Server.
- **Terminal Server - Logoff Session X**
  - ➢ Reference URL:
    http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Terminal Server - Logoff Session 1**
  - ➢ Reference URL:
    http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true

- **Terminal Server - Query Sessions**
  - ➢ Uses QUERY USER to generate a list of all Terminal Server Sessions and writes the session information list to the agent procedure log.
- **Terminal Server - Reboot in 60 Seconds**
  - ➢ Reboots a Terminal Server giving logged on users 60 seconds to close applications and save their work.
- **Terminal Server - Shutdown in 60 Seconds**
  - ➢ Shuts down a Terminal Server giving logged on users 60 seconds to close applications and save their work.

Core.2 Macintosh Procedures

Core.2 Macintosh Procedures.Machine Control.Auditing

- **Collect HDD, User, Process, Network info**
  - ➢ Gathers some info about a Mac. Will also work on almost any Linux distribution once we support it. Executes DF (Mount point, disk space information) uname -a (Os Information) ls /users/ (User information) ifconfig (NIC information) netstat (network connection information) ps aux (process information). Results are sent to /tmp/macinfo.txt and returned to the Kaseya server.   View them under Audit -> Documents for the agent.
- **Retrieve List of Disks and Email to Me**
  - ➢ Uses DISKUTIL to list all Mac OS X disks, retrieves list of disks to the systems Get File Folder, and sends an email to the admin that ran/scheduled the agent procedure.

Core.2 Macintosh Procedures.Machine Control.Monitoring

- **Check SMART Status of Disk0**
  - ➢ Uses DISKUTIL to get Self-Monitoring, Analysis and Reporting Technology (SMART) status of Disk0 on the Mac and sends an email to the admin that ran/scheduled the procedure if the SMART status is Failing.

Core.2 Macintosh Procedures.Machine Control.Networking

- **Bind Mac to an Active Directory Domain**
  - ➢ Uses DSCONFIGAD to bind a Mac OS X system to an Active Directory Domain. Prompts for Full AD Domain Name, AD Domain "Administrator" Credentials, and Target OU.

Core.2 Macintosh Procedures.Machine Control.System

- **Configure Mac Energy Saver Settings**
  - ➢ Uses PMSET to configure Energy Saver settings for the Battery Profile under Mac System Preferences. Uses PMSET to configure the Power Adapter profile (i.e. when the Mac is plugged into AC Power), as follows: The display sleeps after 45 minutes of inactivity. The computer sleeps after 1 hour of inactivity.
- **Update Mac IP/Name Configuration Records.**
  - ➢ Uses CHANGEIP to fix IP/name changes on Mac OS X Severs. Prompst for Old Name and New Name CHANGEIP is used to manually update configuration records when a server's IP address or hostname changed in a way that affected services were unable to properly process, for example when the server is behind a NAT device and the WAN identity changed. In typical usage, this command is used by an administrator to correct affected services when a server's network information changes. CHANGEIP can be invoked before the change is applied; in such an invocation, the arguments consist of the server's current and pending IP addresses, and optionally the existing and new host name.
- **Change Mac Computer Name**
  - ➢ Rename Mac with SCUTIL

Core.2 Macintosh Procedures.Machine ControlSystem Preferences.Energy Saver.Battery Profile

- **Energy Saver - Battery Set Auto Reduce Brightness Before Display Sleep Off**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Auto Reduce Brightness Before Display Sleep Off".
- **Energy Saver - Battery Set Auto Reduce Brightness Before Display Sleep On**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Auto Reduce Brightness Before Display Sleep On".
- **Energy Saver - Battery Set Computer Sleep 120 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Computer Sleep 120 Mins".
- **Energy Saver - Battery Set Computer Sleep 15 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Computer Sleep 15 Mins".
- **Energy Saver - Battery Set Computer Sleep 30 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Computer Sleep 30 Mins".
- **Energy Saver - Battery Set Computer Sleep 45 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Computer Sleep 45 Mins".
- **Energy Saver - Battery Set Computer Sleep 60 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Computer Sleep 60 Mins".
- **Energy Saver - Battery Set Computer Sleep 90 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Computer Sleep 90 Mins".
- **Energy Saver - Battery Set Display Sleep 120 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Display Sleep 120 Mins".
- **Energy Saver - Battery Set Display Sleep 15 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Display Sleep 15 Mins".
- **Energy Saver - Battery Set Display Sleep 30 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Display Sleep 30 Mins".
- **Energy Saver - Battery Set Display Sleep 45 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Display Sleep 45 Mins".
- **Energy Saver - Battery Set Display Sleep 60 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Display Sleep 60 Mins".
- **Energy Saver - Battery Set Display Sleep 90 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Display Sleep 90 Mins".
- **Energy Saver - Battery Set Hard Disk(s) to Sleep When Possible Off**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Hard Disk(s) to Sleep When Possible Off".
- **Energy Saver - Battery Set Hard Disk(s) to Sleep When Possible On**

- ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Hard Disk(s) to Sleep When Possible On".
  - ▪ **Energy Saver - Battery Set Hibernation Mode 0 (Wake from Memory)**
    - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Hibernation Mode 0 (Wake from Memory)".
  - ▪ **Energy Saver - Battery Set Hibernation Mode 25 (Wake from Disk)**
    - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Hibernation Mode 25 (Wake from Disk)".
  - ▪ **Energy Saver - Battery Set Hibernation Mode 3 (Wake from Memory or Disk)**
    - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Hibernation Mode 3 (Wake from Memory or Disk)".
  - ▪ **Energy Saver - Battery Set Slightly Dim Display Off**
    - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Slightly Dim Display Off".
  - ▪ **Energy Saver - Battery Set Slightly Dim Display On**
    - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Battery Profile. Procedure will set "Slightly Dim Display On".

Core.2 Macintosh Procedures.Machine Control.System Preferences.Energy Saver.Power Adapter Profile

- ▪ **Energy Saver - Power Adapter Set Auto Reduce Brightness Before Display Sleep Off**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Auto Reduce Brightness Before Display Sleep Off".
- ▪ **Energy Saver - Power Adapter Set Auto Reduce Brightness Before Display Sleep On**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Auto Reduce Brightness Before Display Sleep On".
- ▪ **Energy Saver - Power Adapter Set Computer Sleep 120 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Computer Sleep 120 Mins".
- ▪ **Energy Saver - Power Adapter Set Computer Sleep 15 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Computer Sleep 15 Mins".
- ▪ **Energy Saver - Power Adapter Set Computer Sleep 30 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Computer Sleep 30 Mins".
- ▪ **Energy Saver - Power Adapter Set Computer Sleep 45 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Computer Sleep 45 Mins".
- ▪ **Energy Saver - Power Adapter Set Computer Sleep 60 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Computer Sleep 60 Mins".
- ▪ **Energy Saver - Power Adapter Set Computer Sleep 90 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Computer Sleep 90 Mins".
- ▪ **Energy Saver - Power Adapter Set Display Sleep 120 Mins**
  - ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Display Sleep 120 Mins".
- ▪ **Energy Saver - Power Adapter Set Display Sleep 15 Mins**

> ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Display Sleep 15 Mins".

- **Energy Saver - Power Adapter Set Display Sleep 30 Mins**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Display Sleep 30 Mins".

- **Energy Saver - Power Adapter Set Display Sleep 45 Mins**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Display Sleep 45 Mins".

- **Energy Saver - Power Adapter Set Display Sleep 60 Mins**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Display Sleep 60 Mins".

- **Energy Saver - Power Adapter Set Display Sleep 90 Mins**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Display Sleep 90 Mins".

- **Energy Saver - Power Adapter Set Hard Disk(s) to Sleep When Possible Off**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Hard Disk(s) to Sleep When Possible Off".

- **Energy Saver - Power Adapter Set Hard Disk(s) to Sleep When Possible On**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Hard Disk(s) to Sleep When Possible On".

- **Energy Saver - Power Adapter Set Hibernation Mode 0 (Wake from Memory)**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Hibernation Mode 0 (Wake from Memory)".

- **Energy Saver - Power Adapter Set Hibernation Mode 25 (Wake from Disk)**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Hibernation Mode 25 (Wake from Disk)".

- **Energy Saver - Power Adapter Set Hibernation Mode 3 (Wake from Memory or Disk)**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Hibernation Mode 3 (Wake from Memory or Disk)".

- **Energy Saver - Power Adapter Set Wake for AirPort Network Access Off**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Wake for AirPort Network Access Off".

- **Energy Saver - Power Adapter Set Wake for AirPort Network Access On**
  > ➢ Uses PMSET to configure Mac System Preferences...Energy Saver settings for the Power Adapter Profile. Procedure will set "Wake for AirPort Network Access On".

Core.2 Macintosh Procedures.Machine Control.System Preferences.Security

- **Security - General Set Disable Automatic Login On**
  > ➢ Uses DEFAULTS to configure Mac System Preferences...Security settings for General. Procedure will set "Disable Automatic Logon On" and will remove existing Automatic Logon account information.

Core.2 Macintosh Procedures.Machine Control.Utils

- **Restart OS X Dock**
  > ➢ Restarts the Mac Dock

- **Send a Text To Speech Message to OS X**
  > ➢ Uses OSASCRIPT and SAY to playback the message entered on the Mac audio (i.e. Text To Speech).

- **Take a Camera Picture on OS X**

- ➢ Uses the mac port 'isightcapture' to use the camera on any Mac to take a picture.
  - ▪ **Take a Screen Capture of Current Users OS X Desktop**
    - ➢ Performs a Screen Capture of the current Mac OS X desktop of logged in user. The Screen Capture file is stored in the systems Documents folder on the server.

Core.2 Macintosh Procedures.Maintenance

- ▪ **Macintosh Weekly Maintenance**
  - ➢ Performs a number of routing maintenance tasks on a Macintosh OS X machine.
- ▪ **General OS X House Cleaning**
  - ➢ Performs system cleaning, removes old log files, "scratch" and "junk" files, clears user and system caches, rotates system and application logs, rebuilds DYLD cache, and rebuilds the Spotlight index.
- ▪ **Verify and Repair OS X Disk Volumes**
  - ➢ Performs disk verification and repair operations using DISKUTIL.
- ▪ **Repair OS X Disk Permissions**
  - ➢ Performs a disk repair permissions operation using DISKUTIL.

Core.2 Macintosh Procedures.Software Update

- ▪ **Mac Software Update - Install All Updates and Alert If Any**
  - ➢ Mac Software Update -- Install ALL updates. If new updates are installed, send alert. See "Mac Software Update - Install all updates" under Reports -> Logs for details. Details also saved for agent under Audit -> Documents.
- ▪ **Mac Software Update - Install All Updates and Retrieve/Log Results**
  - ➢ Uses SOFTWAREUPDATE to install all Mac software updates,
- ▪ **Mac Software Update - Install All Updates and Reboot After**
  - ➢ Uses SOFTWAREUPDATE to install all Mac software updates and reboots after.
- ▪ **Mac Software Update - Retrieve and Email List of All Updates to Me**
  - ➢ Uses SOFTWAREUPDATE to list all Mac software updates to a file and retrieves the file and emails the list to the email address of the VSA user that executes/schedules the procedure.
- ▪ **Mac Software Update - Download All Updates and Alert If Any**
  - ➢ Uses SOFTWAREUPDATE to download all Mac software updates, list them to a file, retrieves the file generating an Alert if updates are available.
- ▪ **Mac Software Update - Download Recommended Updates and Alert If Any**
  - ➢ Mac Software Update - Download Recommended updates   If new updates are downloaded, send alert. See "Mac Software Update - Download Recommended updates" under Reports -> Logs for details. Details also saved for agent under Audit -> Documents.
- ▪ **Mac Software Update - Install Recommended Updates and Retrieve/Log Results**
  - ➢ Uses SOFTWAREUPDATE to install recommended Mac software updates,
- ▪ **Mac Software Update - Retrieve List of All Updates and Alert If Any**
  - ➢ Mac Software Update - List ALL updates. If new updates are detected, send alert. See "Mac Software Update - List ALL updates" under Reports -> Logs for details. Details also saved for agent under Audit -> Documents.

Core.3 Linux Procedures

Core.3 Linux Procedures.Machine Control.Audit Info

- ▪ **Get Current Memory information**
  - ➢ Retrieve current memory availability information.
- ▪ **Get Linux and Kernel Version**

➢ Retrieves current linux version (Name) and Kernel information

Core.3 Linux Procedures.Machine Control.DNS

- **Create HOSTS File**
  - ➢ This procedure will create a new hosts file with variables and information you supply.
- **Edit DNS Servers**
  - ➢ Edit your DNS Servers
- **Set Hostname**
  - ➢ This procedure will setup your Servers/Workstations Hostname

Core.3 Linux Procedures.Machine Control.Files/Folder Control

- **Change File/Folder Permissions**
  - ➢ Read - Write - Execute 4 2 1
- **Change Group Ownership**
  - ➢ chgrp groupName folderName
- **Change Ownership**
  - ➢ chown userName fileFolderName
- **Delete any file or any folder - Dangerous**
  - ➢ This procedure will delete any file or folder without asking for permission

Core.3 Linux Procedures.Machine Control.Linux Kernel

- **Create an initrd image**
  - ➢ Creates an initrd image of the Linux system and names it initrd.image-#version# based on a version value you enter.

Core.3 Linux Procedures.Machine Control.Monitoring

- **Get SNMP Conf file**
  - ➢ Retrieve the SNMP configuration file using GET FILE

Core.3 Linux Procedures.Machine Control.Networking

- **Setup DHCP Client**
  - ➢ Adds entries for interface to pickup DHCP Server
- **Setup Networking (1 interface)**
  - ➢ This will create a new interfaces file in /etc/networking with new IP address information. This will only setup networking for the 1 single interface. Once the file has been created, the networking service will be restarted.

Core.3 Linux Procedures.Machine Control.Networking.Get DOMAIN info

- **Query All Domain Information**
  - ➢ Performs a full DNS lookup of a domain name you specify using DIG with the ANY (omnibus - All Domain Information) switch and retrieves the resulting log file, dig-#domain#-all.log, to the systems GetFile folder.
- **Query DNS Server for Domain Details**
  - ➢ Performs a DNS lookup of a domain name you specify using DIG and retrieves the resulting log file, dig-#domain#.log, to the systems GetFile folder.
- **Query DNS Servers Authoritative for a Domain**
  - ➢ Performs an Authoratative Name Server lookup of a domain name you specify using DIG with the NS (Authoritative DNS Servers for Domain) switch and retrieves the resulting log file, dig-#domain#-Auth.log, to the systems GetFile folder.

- **Query Domain Address Records**
  - ➢ Performs an Address (A) Records DNS lookup of a domain name you specify using DIG with the NS (Authoritative DNS Server for Domain) switch and retrieves the resulting log file, dig-#domain#-A.log, to the systems GetFile folder.
- **Query Domain Email Servers**
  - ➢ Performs an Email Servers/Mail Exchanger (MX) Records DNS lookup of a domain name you specify using DIG with the MX (Mail Exchangers for Domain) switch and retrieves the resulting log file, dig-#domain#-MX.log, to the systems GetFile folder.
- **Query Statistics Including Round-Trip Time**
  - ➢ Performs a DNS Statisics (including round-trip time) query of a domain name you specify using DIG and retrieves the resulting log file, dig-#domain#-stats.log, to the systems GetFile folder.
- **Query the TTL for Each Resource Record**
  - ➢ Performs a DNS Time To Live (TTL) query of a domain name you specify using DIG and retrieves the resulting log file, dig-#domain#-TTL.log, to the systems GetFile folder.

Core.3 Linux Procedures.Machine Control.Networking.Routing

- **Get Routes**
  - ➢ Retrieves current routes setup
- **Trace Path to Domain/IP**
  - ➢ Trace HOPS to domain/IP Address - Uses GET File to view results

Core.3 Linux Procedures.Machine Control.Reboot/Shutdown

- **Reboot Linux**
  - ➢ Restarts the system
- **Shutdown Linux**
  - ➢ Shutdown the Linux System

Core.3 Linux Procedures.Machine Control.Runlevel Control

- **Custom Runlevel**
  - ➢ Explanation of runlevels in Linux http://http://en.wikipedia.org/wiki/Runlevel
- **Runlevel 1**
  - ➢ Runlevel 1 is usually for very basic commands. This is the equivalent to "safe mode" used by Windows. This level is usually only used to asses repairs or maintenance to the system. This is a single-user mode and does not allow other users to login to the machine.
- **Runlevel 2**
  - ➢ Runlevel 2 is used to start most of the machines services. However, it does not start the network file sharing service (SMB, NFS). This will allows multiple users to login to the machine.
- **Runlevel 3**
  - ➢ Runlevel 3 is commonly used by servers. This loads all services except the X windows system. This means the system will boot to the equivalent of DOS. No GUIs (KDE, Gnome) will start. This level allows multiple users to login to the machine.
- **Runlevel 4**
  - ➢ Runlevel 4 is usually a "custom" level. By default it will start a few more services than level 3. This level is usually only used under special circumstances.
- **Runlevel 5**
  - ➢ Runlevel 5 is everything! This will start any GUIs, extra services for printing, and 3rd party services. Full multi-users support also. This runlevel is generally used on by workstations.

Core.3 Linux Procedures.Machine Control.Services Control

- **Custom Services Control**
  - ➢ Start, Stop and Restart any service on the System
- **Restart HTTPD/Apache2**
  - ➢ Restarts your Web Service HTTPD/Apache2
- **Restart Networking**
  - ➢ Restarts the networking daemon
- **Restart NFS**
  - ➢ Restarts the NFS Daemon Service
- **Restart Postfix**
  - ➢ Restart Postfix Email Server
- **Restart SSH**
  - ➢ Restart SSH Server
- **Restart VMWare Tools**
  - ➢ Restarts VMWare Tools

Core.3 Linux Procedures.Machine Control.User/Group Control.Groups

- **Create new group**
  - ➢ Uses GROUPADD to create a new group that you specify.
- **Delete Group**
  - ➢ Uses GROUPDEL to delete an existing group that you specify.

Core.3 Linux Procedures.Machine Control.User/Group Control.Password Control

- **Change Root Password**
  - ➢ Changes the root password on the system.
- **Change user password**
  - ➢ Asks for the username and resets the password.

Core.3 Linux Procedures.Machine Control.User/Group Control.Users

- **Add New User**
  - ➢ Add new Linux User
- **Delete User**
  - ➢ Delete User from Server/Machine

Core.3 Linux Procedures.Machine Control.Utils

- **Add custom commands**
  - ➢ Adds a number of aliased custom commands to the /root/.bashrc file and then executes it to make these commands go into effect. The custom commands are:

    ll = ls –l
    la = ls -A
    l = ls -CF

  > Note: Extend the list by adding more aliased commands.

- **Synchronize the System Clock**
  - ➢ Installs and Syncs Clock
- **Update File Database**
  - ➢ Updates the Filesystem Database for using the "locate" command

Core.3 Linux Procedures.Maintenance

- **Collect inode usage statistics**
  - ➢ Check inode usage.
- **Force Logical File System Check (FSCK) at Next Reboot**
  - ➢ Forces an FSCK to run at next reboot.
- **Get Disk Usage**
  - ➢ Generates a Disk Usage listing using DF, writes results to the agent procedure log and retrieves the results to the systems Get File folder.
- **Linux Weekly Maintenance**
  - ➢ Performs a number of routine maintenance tasks on Linux machines including time sync, apt-get repository cleanup, package upgrades/updates and disk checks and performance statistics.
- **Remove User Adobe Flash/Macromedia Permanent Objects**
  - ➢ Removes User Adobe Flash and Macromedia permanent objects.
- **Remove User Temporary Files**
  - ➢ Removes temporary files (i.e. *~) from the current users home folder.

Core.3 Linux Procedures.Process Control.Get All Processes with PID

  - ➢ Retrieves all processes with Process ID, uses the GET FILE feature to retrieve the results
- **Get process Tree**
  - ➢ Generates a TREE of Parent and Child processes - uses GET FILE feature to retrieve the results.
- **Kill Process**
  - ➢ The variable with the correct PID will be used to kill the outline process
- **Locate a file**
  - ➢ This will use the locate function in Kaseya to search for files as specified and use the GET FILE Feature to retrieve the results

Core.3 Linux Procedures.Setup/Configs.Backup Servers

- **MySQL Backups With AutoMySQLBackup On Ubuntu 9.10**
  - ➢ Postfix Install required before installing AutoMySQLBackup - Postfix is required http://sourceforge.net/projects/automysqlbackup/ http://www.mysql.com/
- **Ubuntu Server 9.04 Bacula Bweb GUI**
  - ➢ Not tested----

Core.3 Linux Procedures.Setup/Configs.CRM Servers.SugarCRM

  - ➢ Full LAMP Server install required before installing SugarCRM - MySQL, Apached, PHP - Once the script has completed please run the following: http://Server IP Address/sugarcrm

Core.3 Linux Procedures.Setup/Configs.DNS

- **Setup Chrooted DNS Server**
  - ➢ Configures BIND to run in a chrooted environment

Core.3 Linux Procedures.Setup/Configs.Email Server

- **(2) Configure Postix Email Server**
  - ➢ Configure the Postfix Email Server
- **(2.1) Configure SMTP-AUTH**
  - ➢ Configure Secure SMTP authentication using SASLAUTHD

- **(3) Create the certificates for TLS**
  - ➢ Generates TLS Certificates
- **(4) Configure Postfix for TLS**
  - ➢ Configures TLS Secure Keys for using Postfix
- **(5) Configure SASLAUTHD to work with Chrooted Postfix**
  - ➢ Authentication will be done by saslauthd. We have to change a few things to make it work properly. Because Postfix runs chrooted in /var/spool/postfix we have to do the following:
- **(6) Install Courier-IMAP/Courier-POP3**
  - ➢ Install and configure IMAP and POP3 using courier - ... and modify the following two files; replace CN=localhost with CN=server1.example.com (you can also modify the other values, if necessary): vim /etc/courier/imapd.cnf vim /etc/courier/pop3d.cnf
- **(7) Configure Maildir**
  - ➢ Configures Maildir for email messages and user mailboxes

Core.3 Linux Procedures.Setup/Configs.FTP Servers

- **Configure Proftpd**
  - ➢ Configures the Proftpd Server - Remember to install the software first

Core.3 Linux Procedures.Setup/Configs.MySQL Server

- **MySQL Server Installation**
  - ➢ Install MySQL Server and set root password

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Client

- **Install and config for NFS Client**
  - ➢ NFS Setup for Client machines to mount drives as exported/shared by the Server

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Server

- **Install and Setup NFS Server**
  - ➢ Installs and configures NFS Server with the HOME directory and 1 optional Shared with Clients

Core.3 Linux Procedures.Setup/Configs.Security.AppArmor

- **Disable AppArmor**
  - ➢ AppArmor is a security extension (similar to SELinux) that should provide extended security. In my opinion you don't need it to configure a secure system, and it usually causes more problems than advantages (think of it after you have done a week of trouble-shooting because some service wasn't working as expected, and then you find out that everything was ok, only AppArmor was causing the problem). Therefore I disable it

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Forward Rules

- **Deny Access to a Specific Subnet**
  - ➢ Denies access to a subnet you specify by adding appropriate iptables firewall rules.
- **Forward Traffic (DNAT)**
  - ➢ Allows DNAT forwarding of a particular TCP port to the internal server. You specify the public interface, public address, internal server address, and port, and the procedure adds tha appropriate iptables firewall rules.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Global Rules (REJECT, ACCEPT)

- **# Forwarding Traffic (DROP ALL)**

- ➢ Reject all traffic from the forwarding chain
- ▪ **# Incoming Traffic (ALLOW ALL)**
  - ➢ Allow all incoming traffic through the `INPUT` chain
- ▪ **# Incoming Traffic (DROP ALL)**
  - ➢ REJECT all incoming traffic
- ▪ **# Outgoing Traffic (ALLOW ALL)**
  - ➢ Allow all traffic from your internal network out
- ▪ **# Outgoing Traffic (DROP ALL)**
  - ➢ Reject all internal traffic from exiting the firewall
- ▪ **_### NB! - Enable Routing - NB! ###_**
  - ➢ Enable Routing and NAT for iptables - Important for traffic to be processed through the firewall
- ▪ **Don't Accept ICMP Redirect Messages**
  - ➢ Configures system to not accept ICMP redirects.
- ▪ **Don't Send ICMP Redirect Messages**
  - ➢ Configures system to not send ICMP redirects.
- ▪ **Drop ICMP echo-request Messages Sent to Broadcast or Multicast Addresses**
  - ➢ Configures system to drop ICMP echo-request messages sent to broadcast or multicast addresses.
- ▪ **Drop Source Routed Packets**
  - ➢ Configures system to drop source routed packets.
- ▪ **Enable Logging**
  - ➢ Enables iptables firewall event logging.
- ▪ **Enable Source Address Spoofing Protection**
  - ➢ Enables Source Address Spoofing Prtection on system.
- ▪ **Enable TCP SYN cookie protection from SYN floods**
  - ➢ Enable TCP SYN Cookie Protection from SYN Floods on system.
- ▪ **Flush All Chains**
  - ➢ This will flush all iptables rules - Dangerous, use at own risk!
- ▪ **Log Packets with Impossible Source Addresses**
  - ➢ Enables logging of packets with impossible source addresses on system.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Inbound Rules

- ▪ **Allow CUSTOM Port Inbound**
  - ➢ Allows you to enter an interface, protocol and TCP/UDP port you would like added to the iptables firewall rules.
- ▪ **Allow DNS Inbound**
  - ➢ Allows inbound DNS traffic by adding appropriate iptables firewall rules. Applies not only for firewalls acting as DNS clients but also for firewalls working in a caching or regular DNS server role.
- ▪ **Allow FTP Inbound**
  - ➢ Allows inbound FTP traffic by adding appropriate iptables firewall rules.
- ▪ **Allow ICMP Inbound**
  - ➢ Allows inbound ICMP traffic by adding appropriate iptables firewall rules. iptables is configured to allow the firewall to send ICMP echo-requests (pings) and in turn, accept the expected ICMP echo-replies.

- **Allow IMAP Inbound**
  - ➢ Allows inbound IMAP traffic by adding appropriate iptables firewall rules.
- **Allow IMAPS Inbound**
  - ➢ Allows inbound IMAPS traffic by adding appropriate iptables firewall rules.
- **Allow Kaseya Inbound**
  - ➢ Allows inbound Kaseya traffic by adding appropriate iptables firewall rules.
- **Allow Loopback interface**
  - ➢ Allows inbound Loopback interface traffic by adding appropriate iptables firewall rules.
- **Allow MySQL**
  - ➢ Allows inbound MySQL traffic by adding appropriate iptables firewall rules.
- **Allow Network to Access Firewall**
  - ➢ eth1 is directly connected to a private network using IP addresses from the 192.168.1.0 network. All traffic between this network and the firewall is simplistically assumed to be trusted and allowed. Further rules will be needed for the interface connected to the Internet to allow only specific ports, types of connections and possibly even remote servers to have access to your firewall and home network.
- **Allow POP3 Inbound**
  - ➢ Allows inbound POP3 traffic by adding appropriate iptables firewall rules.
- **Allow POP3S Inbound**
  - ➢ Allows inbound POP3S traffic by adding appropriate iptables firewall rules.
- **Allow SMTP Inbound**
  - ➢ Allows inbound SMTP traffic by adding appropriate iptables firewall rules.
- **Allow SSH Inbound**
  - ➢ Allows inbound SSH traffic by adding appropriate iptables firewall rules.
- **Allow Traffic from Localhost**
  - ➢ Allow inbound traffic from the Localhost address by adding appropriate iptables firewall rules.
- **Allow WWW Inbound**
  - ➢ Inbound packets destined for ports 80 and 22 are allowed thereby making the first steps in establishing a connection. It isn't necessary to specify these ports for the return leg as outbound packets for all established connections are allowed. Connections initiated by persons logged into the Web server will be denied as outbound NEW connection packets aren't allowed.
- **Allow Established Sessions Inbound**
  - ➢ Allow inbound traffic from established connections by adding appropriate iptables firewall rules.
- **Block IP Address**
  - ➢ Block an IP Address you specify from entering your network via the public interface.
- **Block IRC Inbound**
  - ➢ Block inbound IRC traffic by adding appropriate iptables firewall rules.
- **Block Network**
  - ➢ Block an entire network from accessing your network
- **List all iptables Rules**
  - ➢ This will pipe all iptables rules to /var/tmp/iptables.log and the GET procedure will upload this to the server for review
- **Restart IPTables**
  - ➢ Restart IPTables firewall

- **Save iptables Rules**
  - ➢ Tested on Ubuntu

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Outbound Rules

- **# Allow Kaseya Outbound**
  - ➢ Allows outbound Kaseya traffic by adding appropriate iptables firewall rules.
- **Allow CUSTOM Port Outbound**
  - ➢ Allow a custom port from your internal network to access the outside world
- **Allow DNS Outbound**
  - ➢ The following statements will apply not only for firewalls acting as DNS clients but also for firewalls working in a caching or regular DNS server role.
- **Allow Established Connections Outbound**
  - ➢ Allows all established connections with ACK back.
- **Allow FTP Outbound**
  - ➢ Allows outbound FTP traffic by adding appropriate iptables firewall rules.
- **Allow ICMP Packets Outbound**
  - ➢ Allows outbound ICMP packets by adding appropriate iptables firewall rules.
- **Allow IMAP Outbound**
  - ➢ Allows outbound IMAP traffic by adding appropriate iptables firewall rules.
- **Allow IMAPS Outbound**
  - ➢ Allows outbound IMAPS traffic by adding appropriate iptables firewall rules.
- **Allow Loopback Interface**
  - ➢ Allows outbound Loopback traffic by adding appropriate iptables firewall rules.
- **Allow MySQL Outbound**
  - ➢ Allows outbound MySQL traffic by adding appropriate iptables firewall rules.
- **Allow POP3 Outbound**
  - ➢ Allows outbound POP3 traffic by adding appropriate iptables firewall rules.
- **Allow POP3S Outbound**
  - ➢ Allows outbound POP3S traffic by adding appropriate iptables firewall rules.
- **Allow SMTP Outbound**
  - ➢ Allows outbound SMTP traffic by adding appropriate iptables firewall rules.
- **Allow SSH**
  - ➢ Allows outbound SSH traffic by adding appropriate iptables firewall rules.
- **Allow WWW**
  - ➢ Allows outbound WWW traffic by adding appropriate iptables firewall rules.
- **Deny Access to a Specific Outbound IP Address with Logging**
  - ➢ Denies access with logging to an outbound IP address you specify by adding appropriate iptables firewall rules.
- **FLUSH OUTBOUND Rules**
  - ➢ Flushes iptables OUTBOUND rules. Dangerous, use at own risk!
- **Run all OUTBOUND Rules**
  - ➢ Applies all OUTBOUND rules with ability to optionally flush all OUTBOUND rules first.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Postrouting Rules

- **Allow routing for private network through Firewall**

➢ You'll notice that the private network is a non-public routed IP network. This requires address translation at a router with a public IP address or nothing on the public network will be able to return packets to the private network. Address translation is easily enabled with iptables. The addresses that are being translated are the "source" of sessions so the mode is called Source NAT (SNAT):

Core.3 Linux Procedures.Setup/Configs.Security.SELinux

▪ **Disable SELinux after reboot**

➢ This will disable SELinux for good and after the first reboot

▪ **Disable SELinux Immediately**

➢ Disables SELinux for the current logged in runlevel. This will not be configured to be disabled after reboot.

Core.3 Linux Procedures.Setup/Configs.Shell Control

▪ **Change The Default Shell**

➢ /bin/sh is a symlink to /bin/dash, however we need /bin/bash, not /bin/dash

Core.3 Linux Procedures.Setup/Configs.Web Servers.Apache2

▪ **Enable Modules**

➢ Apache modules (SSL, rewrite, suexec, include, and WebDAV):

▪ **Install Apache2**

➢ Uses APT-GET to install Apache2 web server, CHKCONFIG to set for automatic startup, and starts Apache daemon.

▪ **Install PHPMyAdmin**

➢ Be sure to change the Apache configuration so that phpMyAdmin allows connections not just from localhost (by commenting out the <Directory /usr/share/phpMyAdmin/> stanza):

Core.3 Linux Procedures.Setup/Configs.Web Servers.Scripting

▪ **Install PHP5**

➢ Install PHP5 for Apache 2

Core.3 Linux Procedures.Software Control.Applications

▪ **Install CHKCONFIG**

➢ Installs CHKCONFIG package. This package enables you to start a specific daemon package on system boot.

▪ **Install CHKCONFIG Simple**

➢ Uses APT-GET to install CHKCONFIG.

▪ **Install Common needed packages**

➢ This will install commonly needed packages for Ubuntu. binutils cpp fetchmail flex gcc libarchive-zip-perl libc6-dev libcompress-zlib-perl libdb4.6-dev libpcre3 libpopt-dev lynx m4 make ncftp nmap openssl perl perl-modules unzip zip zlib1g-dev autoconf automake1.9 libtool bison autotools-dev g++ build-essential

▪ **install SNMP**

➢ This will install SNMP which allows you to monitor Linux Servers. Remember to set your SNMP Community String

▪ **Install Software**

➢ Prompts the user for the software package name that needs to be installed, and then uses APT-GET to install that package.

▪ **Install software from Image List**

➢ This allows you to to PIPE (|) a list of software to the apt-get install command which will install all missin software from the list. You have to create the list first! NB (Look in Software Updates/Upgrades Folder for the create image list procedure

- **Install SSH**
  - ➢ Install the SSH Server for remote access
- **Install VIM**
  - ➢ This installs VIM which is an easy to use text file editor for LInux
- **Install vim-nox**
  - ➢ The default vi program has some strange behaviour on Ubuntu and Debian; to fix this, we install vim-nox:
- **Install XPDF**
  - ➢ PDF Reader for Linux

Core.3 Linux Procedures.Software Control.apt-get

- **Autoclean apt-get**
  - ➢ apt-get autoclean removes only package files that can no longer be downloaded.
- **Clean apt-get repository**
  - ➢ Removes everything except lock files from /var/cache/apt/archives/ and /var/cache/apt/archives/partial/. Thus, if you need to reinstall a package APT should retrieve it again
- **Install Software**
  - ➢ Prompts the user for the software package name that needs to be installed, and then uses APT-GET to install that package.
- **Remove Software**
  - ➢ Removes the Package as prompted by the procedure

Core.3 Linux Procedures.Software Control.DNS

- **Install Bind9**
  - ➢ DNS Server for linux

Core.3 Linux Procedures.Software Control.Email Servers

- **Download Zimbra Email**
  - ➢ This will download the Zimbra email collaboration suite for Linux.

Core.3 Linux Procedures.Software Control.File Server

- **Install Quota**
  - ➢ This will install the quota application needed for Quota control on specific folders. It is strongly recommended that you edit your /etc/fstab file manually as this can break your server and not mount any filesystem. Here is an example of a working fstab with quota enabled:

```
# <file system> <mount point>  <type> <options>      <dump> <pass>
proc            /proc          proc   nodev,noexec,nosuid 0      0
/dev/mapper/server1-root /            ext4
errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0
1
# /boot was on /dev/sda1 during installation
UUID=a8f37dcf-5836-485c-a451-3ae2f0f47720 /boot       ext2    defaults
0      2
/dev/mapper/server1-swap_1 none       swap   sw            0      0
/dev/fd0        /media/floppy0  auto   rw,user,noauto,exec,utf8 0     0
```

- **Set Quota on**

➢ Enable quota management for File Servers

Core.3 Linux Procedures.Software Control.FTP Servers

- **Install Proftpd**
  - ➢ This will install the Proftp Server for Linux

Core.3 Linux Procedures.Software Control.iptables (Firewall)

- **Install iptables**
  - ➢ Uses APT-GET to install iptables firewall.

Core.3 Linux Procedures.Software Control.Management Software

- **Download Webmin**
  - ➢ Webmin is a GUI used for full management of Linux using your Web Browser

Core.3 Linux Procedures.Software Control.Repository's

- **Enable Multiverse Repository**
  - ➢ This will add the sources to the `source.list` file. It will not recreate the file.
- **Enable Universe Repository**
  - ➢ This procedure will add these repository's sources to the `source.list` file. It will not recreate the file.
- **Update Repository's**
  - ➢ Updates all packages - Run this after you added the Repo's

Core.3 Linux Procedures.Software Control.System

- **Install NTP Daemon**
  - ➢ It is a good idea to synchronize the system clock with an NTP (network time protocol) server over the internet. Simply run

Core.3 Linux Procedures.Software Control.Updates/Upgrades

- **Create Image List of Installed Software**
  - ➢ Create image list of installed software
- **Full System Update**
  - ➢ Updates all system packages
- **Upgrade Packages**
  - ➢ Use this procedure to upgrade packages within the same distribution
- **Upgrade to New Release**
  - ➢ Upgrades your Linux Distro to the latets available version - You will see a Reboot Request on the desktop when finished
- **Linux Package Updates/Upgrades**
  - ➢ Performs a Full System Update and Upgrades all Installed Packages

Core.4 Other Tools and Utility Procedures

Core.4 Other Tools and Utility Procedures.AntiVirus

- **EICAR Virus Test**
  - ➢ Creates a file in the Agent Working Directory that contains the EICAR test virus pattern. This agent procedure can be used to verify that any antivirus software is working on a machine. NOTE: This is not a real virus and poses no potential risk. For more information, see http://eicar.org.

- **Run a Malicious Software Removal Tool Full Scan-Clean**
  - ➤ Uses MRT (Microsoft Malicious Software Removal Tool) to perform a full scan and clean. Results of the operation are logged to an MRT.LOG file and to the agent procedure log. The log file is retrieved to the systems GetFile folder.

Core.4 Other Tools and Utility Procedures.AntiVirus.Defender

- **Windows Defender - Full System Scan**
  - ➤ Run a Windows Defender Full System Scan
- **Windows Defender - Quick System Scan**
  - ➤ Run a Windows Defender Quick System Scan
- **Windows Defender - Signature Update**
  - ➤ Run a Windows Defender Signature Update

Core.4 Other Tools and Utility Procedures.AutoAdminLogon

- **Disable AutoAdminLogon**
  - ➤ Disables any previously enabled AutoAdminLogon configuration on a Windows machine.
- **Enable AutoAdminLogon with AUTOLOGON**
  - ➤ Enables AutoAdminLogon with secure password encryption using SysInternals AutoLogon utility. This Agent Procedure only works on 32bit versions of Windows.XP or later.
- **Enable AutoAdminLogon with Cleat Text Method**
  - ➤ Prompts for the username and password to be used for AutoAdminLogin and then enables the clear text AutoAdminLogon configuration on a Windows machine using those supplied credentials.

Core.4 Other Tools and Utility Procedures.Kaseya Agent Management

- **Agent - Force Check-in**
  - ➤ This is the world's shortest procedure. This procedure has no steps at all. Its sole job is to force the agent to check in with the KServer. Use Force Check-in to determine if an agent is online or not.
- **Agent - Remove Kaseya from Start Menu and Add-Remove Programs**
  - ➤ Remove the Agent folder from the Start Menu. Hide the System Tray Icon (blue K) by disabling the Agent Menu (Agent Tab - Agent Menu). Run this script on machines you do not want to give anyone the ability to uninstall, exit, or stop the Agent.
- **Agent - Reset Audit Cache**
  - ➤ Deletes the cached audit results file saved by the agent. Run this procedure to reset all application results from an audit and start over.
- **Agent - Terminate Remote Control Sessions**
  - ➤ This script Terminates all Remote Control sessions that Kaseya Supports within the Remote Control function of The VSA (K-VNC, WinVNC, Terminal Services, FTP, RAdmin and pcAnyWhere).
- **VNC - Hide System Tray Icon**
  - ➤ Disables the VNC system tray icon on Windows machines when the VNC service is running.
- **VNC - Set Idle Timeout to 0 (Never Timeout)**
  - ➤ Sets the VNC Idle Timeout to 0 so that an idle VNC RC session is not disconnected. Useful when performing remote operations on machines that take a long time to complete and where you do not want the VNC session to automatically time out after 1 hour (default) of inactivity.
- **VNC - Enable Wallpaper when Remoting**

➢ Enable Wallpaper when remote controlling a system. Couple with Disable VNC Icon for completely silent remote control of an agent.

▪ **VNC - Remove RealVNC from Start Menu**

➢ Remove the RealVNC entry from the Start Menu.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Ping Check

▪ **Ping IP Address 1**

➢ This procedure pings an IP address to get results you can use in another procedure. This could also be a port or any other device.

▪ **Ping IP Address 2**

➢ This procedure tests the variable from Ping IP Address to see if the address can be pinged without packet loss. If there is packet loss, the system sends an e-mail with the results of the ping. If there is no packet loss, it logs an All OK result.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Port Check

▪ **Port Monitor 1**

➢ Part 1 of 2: Monitor a port on a host or IP address and send out an email when the port fails to respond. Edit step 1 with the hostname or IP address, edit step 2 to enter the port number you wish to monitor, and edit step 3 to specify the email addresses (comma separate multiple addresses) to send an alert to when the port fails to respond. Edit the procedure Port Monitor 2 to modify the email subject and body.

▪ **Port Monitor 2**

➢ Do NOT schedule this procedure. It is a child procedure called by Port Monitor 1. Schedule Port Monitor 1 to run on a machine to monitor a port on a host or IP Address.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Web Check

▪ **Check Web 1**

➢ Procedure pulls the output of the webpage configured as the siteURL variable. The Check Web 2 script will verify that expected content exists in the output. You must configure the siteURL variable and Test File search string in Check Web 2 in order to customize this procedure. This Sample checks www.google.com/index.html for the word "google".

▪ **Check Web 2**

➢ Check Web 2 verifies that expected content exists in the output from the URL request. You must change the Test File command for content that would be found when the URL tested is functional. In this Sample, we check for the word "google" on the google homepage.

Core.4 Other Tools and Utility Procedures.Managed Services.Policy Management

▪ **Windows Group Policy Update (GPUPDATE /FORCE)**

➢ Reloads the Group Policy on Windows Machines.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Services Remediation

▪ **Start Service (W32Time)**

➢ This procedure restarts the windows time service. This is a sample procedure demonstrating how to start a service using Kaseya Agent procedures.

▪ **Stop Service (W32Time)**

➢ This procedure stops the windows time service. This is a sample procedure demonstrating how to stop a service using Kaseya Agent procedures.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Terminal Services

- **Change Terminal Services RDP Listening Port**
  - ➢ This procedure changes the default Terminal Services RDP port from 3389 to a new port of your choosing.

Core.4 Other Tools and Utility Procedures.Managed Services.System Management

- **Download SysInternals Process Explorer**
  - ➢ This sample demonstrates how to download files from remote sources using the Get URL agent procedure command. Simply specify the URL to download and the target location. In this sample we are downloading directly from the vender website, however a popular method of distributing your files is to store them in a public accessible ftp or website (cloud storage) using this method to download them to your endpoints. This sample simply downloads the file, however you can extend the functionality to install or execute files using the execute shell command in agent procedures. Also note that in this script we are using a variable for the agent temp directory of the agent. See **Agent Working Directory Path** in **Using Variables** *(http://help.kaseya.com/webhelp/EN/VSA/R8/index.asp#2855.htm)* in the VSA online help.
- **Send Message if Logged On**
  - ➢ This procedure sends a message to all your users if you need to do maintenance. On a system, you can use the remote control tab to send a message but there is no a way to send a message if they are logged on.

Core.4 Other Tools and Utility Procedures.Operational Communications

- **Copy OpComm Messages**
  - ➢ Copies down all the latest OpComm message files from the Server to the target machine.
- **Get User name - Then Welcome**
  - ➢ Retrieves the currently logged in user from a SQL View and then sends a "Welcome to our IT Support service" message to that user. If no user is logged on, the agent procedure reschedules itself to run again in 10 minutes.
- **OpComm-ActionRequired**
  - ➢ Displays the ActionRequired OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.
- **OpComm-Backup**
  - ➢ Displays the Backup OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.
- **OpComm-Emergency**
  - ➢ Displays the Emergency OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.
- **OpComm-MachineAudit**
  - ➢ Displays the MachineAudit OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of

end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.

- **OpComm-MaintSchedule**
  - ➢ Displays the MaintSchedule OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.

- **OpComm-NetworkDowntime**
  - ➢ Displays the NetworkDowntime OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.

- **OpComm-PatchUpdate**
  - ➢ Displays the PatchUpdate OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.

- **OpComm-RegularMaintenance**
  - ➢ Displays the RegularMaintenance OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.

- **OpComm-VirusScan**
  - ➢ Displays the VirusScan OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server.

- **OpComm-VirusThreat**
  - ➢ Displays the VirusThreat OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server."

- **OpComm-Welcome**
  - ➢ Displays the Welcome OpComm message to the logged on user. OpComm messages are for communication of standard operational activities, notifications and reminders. The folder of OpComm messages can be customized and extended to support other forms of end user communications. These files are located in the Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm folder on the Kaseya server."

Core.4 Other Tools and Utility Procedures.Patch Management

- **WinAutoUpdate Status Check**
  - ➢ Checks the last known status of Windows Automatic Update based on the most recent Patch Scan and runs "WinAutoUpdate Enabled" if it is enabled, or "WinAutoUpdate Disabled" if it is disabled. Used to create Views showing machines with Windows Automatic Update enabled or disabled.
- **WinAutoUpdate Disabled**

> ➢ DO NOT RUN/SCHEDULE THIS PROCEDURE. It is called by "WinAutoUpdate Status Check" if Windows Automatic Update is disabled on a machine.

- **WinAutoUpdate Enabled**
  - ➢ DO NOT RUN/SCHEDULE THIS PROCEDURE. It is called by "WinAutoUpdate Status Check" if Windows Automatic Update is enabled on a machine.

- **Create Repository Share**
  - ➢ Creates the File Source Local folder and Network Share to act as the repository for Windows patches downloaded from the Internet via Patch Management.

- **Patch Pre-Warning**
  - ➢ Sends a message to the logged on user that Patches and Security Updates abe about to be installed on the machine. Designed to be used as a Pre-Procedure for Patch Automatic Updates.

- **Patch Reboot**
  - ➢ On Windows Workstations the procedure prompts a logged on user to reboot due to Security patches/updates having been installed. If user responds Yes, then it notifies them that their system will be rebooted in one minute, and to save work and close their applications. If user responds No, then it schedules again to run in 60 minutes. If no user is logged on to the workstation, then the system is rebooted. If the machine is a server, and the Patch Reboot E-Mail address is configured, then the procedure sends an email to that email address indicating that the machine needs attention (a reboot).

Core.4 Other Tools and Utility Procedures.Patch Management.Suspend Alarms After Patch

- **Patch Post-Unsuspend Alarms**
  - ➢ Resumes Monitoring related Alarming. Designed to be used as a Post-Procedure for Patch Automatic Updates when the machine is rebooted immediately after patching.

- **Suspend Alarms for 10mins**
  - ➢ Suspends Monitoring related Alarms for 10 minutes. Designed to run as a Post-Procedure for Patch Automatic Updates when reboot takes place automatically after patching.

- **Suspend Alarms for 10mins - Recurring**
  - ➢ Suspends Monitoring related Alarms for 10 minutes and then schedules itself again to run in 5 minutes so that there are no possible gaps in the suspended alarm interval. Designed to run as a Post-Procedure for Patch Automatic Updates when a reboot may not take place immediately.

- **Suspend Alarms for 120mins**
  - ➢ Suspends Monitoring related Alarms for 120 minutes. Designed to run as a Post-Procedure for Patch Automatic Updates when reboot does not take place automatically after patching.

Core.4 Other Tools and Utility Procedures.Run Now System Scripts

- **Run Now Baseline Audit**
  - ➢ Executes the System Agent Procedure "Baseline Audit".

- **Run Now Disable Windows Automatic Update**
  - ➢ Executes the System Agent Procedure "Disable Windows Automatic Update".

- **Run Now Latest Audit**
  - ➢ Executes the System Agent Procedure "Latest Audit".

- **Run Now Patch Scan**
  - ➢ Executes the System Agent Procedure "Patch Scan".

- **Run Now Server Roles Audit**
  - ➢ Executes the client side LUA system script to perform a Server Roles Audit.

- **Run Now System Info**

> ➢ Executes the System Agent Procedure "System Info".
- ▪ **Run Now Update Lists By Scan**
  > ➢ Executes the System Agent Procedure "Update Lists By Scan".
- ▪ **Run Now Uninstall Agent (Retains Agent Data)**
  > ➢ Executes the System Agent Procedure "Uninstall Agent". After the Agent is uninstalled the system retains that Agents data in the system until it is manually deleted.
- ▪ **Run Now Reset Windows Automatic Update**
  > ➢ Executes the System Agent Procedure "Reset Windows Automatic Update".

Monitor Sets

Backup

- ▪ **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  > ➢ Monitors Backup Exec Continuous Protection Services on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Backup - Backup Exec DLO Agent Services - {Severity3}**
  > ➢ Monitors Backup Exec DLO Agent Services on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Backup - Backup Exec Services - {Severity3}**
  > ➢ Monitors Backup Exec Services on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Backup - Backup Exec System Recovery Service - {Severity3}**
  > ➢ Monitors Backup Exec System Recovery Service on Backup Exec Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  > ➢ Monitors BrightStor ARCServe Backup Services on BrightStor ARCServe Backup Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Database

- ▪ **Database - SQL Server (All Instances) Services - {Severity3}**
  > ➢ Monitors SQL Server Services on SQL Server Servers using wildcard MSSQL* Service. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Database - SQL Server (Default Instance) - {Severity0}**
  > ➢ Collects SQL Server (Default Instance) performance counters on SQL Servers. Used for Monitor Log display and Reporting purposes only.
- ▪ **Database - SQL Server (Default Instance) Performance - {Severity2}**
  > ➢ Monitors SQL Server (Default Instance) Performance on SQL Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- ▪ **Database - SQL Server (Default Instance) Services - {Severity3}**
  > ➢ Monitors SQL Server (Default Instance) Services on SQL Server Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Database - SQL Server 2005 Optional Services - {Severity3}**
  > ➢ Monitors SQL Server 2005 Optional Services on SQL Server 2005 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- ▪ **Database - SQL Server 2005 Services - {Severity3}**

> ➢ Monitors SQL Server 2005 Services on SQL Server 2005 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Database - SQL Server 2008 Optional Services - {Severity3}**
  > ➢ Monitors SQL Server 2008 Optional Services on SQL Server 2008 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Database - SQL Server 2008 Services - {Severity3}**
  > ➢ Monitors SQL Server 2008 Services on SQL Server 2008 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Email

- **Email - Blackberry Server Performance - {Severity2}**
  > ➢ Monitors Blackberry Server Performance on Blackberry Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Email - BlackBerry Server Services - {Severity3}**
  > ➢ Monitors BlackBerry Server Services on BlackBerry Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2003 Services - {Severity3}**
  > ➢ Monitors Exchange 2003 Services on Exchange 2003 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2007 Services - {Severity3}**
  > ➢ Monitors Exchange 2007 Services on Exchange 2007 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**
  > ➢ Collects Exchange 2010 Edge Transport Queues performance counters on Exchange 2010 Servers. Used for Monitor Log display and Reporting purposes only.

- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  > ➢ Monitors Exchange 2010 Edge Transport Queues Performance on Exchange 2010 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  > ➢ Monitors Exchange 2010 Edge Transport Queues Performance on Exchange 2010 Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange 2010 Services - {Severity3}**
  > ➢ Monitors Exchange 2010 Services on Exchange 2010 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange Client Active Logons - {Severity0}**
  > ➢ Collects Exchange Client Active Logons performance counter on Exchange Servers. Used for Monitor Log display and Reporting purposes only.

- **Email - Exchange IMAP4 Service - {Severity3}**
  > ➢ Monitors Exchange IMAP4 Service on Exchange Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange POP3 Service - {Severity3}**
  > ➢ Monitors Exchange POP3 Service on Exchange Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange Server (Core) Performance - {Severity2}**
  > ➢ Monitors Exchange Server Performance on Exchange Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Email - Exchange Server (Core) Services - {Severity3}**

> ➢ Monitors Exchange Server (Core) Services on Exchange Server (Core) machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - Exchange Server (Core) Store and Database - {Severity0}**

> ➢ Collects Exchange Server Store and Database performance counters on Exchange Servers. Used for Monitor Log display and Reporting purposes only.

- **Email - SMTP Queue Performance - {Severity3}**

> ➢ Monitors SMTP Queue Performance on SMTP Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Email - SMTP Server Service - {Severity3}**

> ➢ Monitors SMTP Server Service on SMTP Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

File / Print

- **File / Print - DFS Service - {Severity3}**

> ➢ Monitors DFS Service on DFS machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **File / Print - DFSR Service - {Severity3}**

> ➢ Monitors DFSR Service on DFSR machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **File / Print - NTFRS Service - {Severity3}**

> ➢ Monitors NTFRS Service on NTFRS machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **File / Print - Print Queue Job Errors Performance - {Severity1}**

> ➢ Monitors Print Queue Job Errors Performance on File & Print Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **File / Print - Spooler Service - {Severity3}**

> ➢ Monitors Spooler Service on File & Print Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Network Infrastructure

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**

> ➢ Monitors Active Directory Domain Controller Services on Active Directory Domain Controllers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Network Infrastructure - AD Domain Controller Performance - {Severity2}**

> ➢ Monitors AD Domain Controller Performance on Active Directory Domain Controllers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2

- **Network Infrastructure - DHCP Server Performance - {Severity2}**

> ➢ Monitors DHCP Server Performance on DHCP Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Network Infrastructure - DHCP Server Service - {Severity3}**

> ➢ Monitors DHCP Server Service on DHCP Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Network Infrastructure - DNS Server Performance - {Severity2}**

> ➢ Monitors DNS Server Performance on DNS Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Network Infrastructure - DNS Server Service - {Severity3}**

> ➢ Monitors DNS Server Service on DNS Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Network Infrastructure - WINS Server Service - {Severity3}**
  - ➤ Monitors WINS Server Service on WINS Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Disk Space.Disk Space

- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - ➤ Monitors Free Disk Space on Any Drive Below 1GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - ➤ Monitors Free Disk Space on Any Drive Below 2GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - ➤ Monitors Free Disk Space on Any Drive Below 750MB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - ➤ Monitors Free Disk Space on Drive C on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - ➤ Monitors Free Disk Space on Drive C Below 1GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - ➤ Monitors Free Disk Space on Drive C Below 750MB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - ➤ Monitors Free Disk Space on Drive D on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - ➤ Monitors Free Disk Space on Drive E on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - ➤ Monitors Free Disk Space on Drive F on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - ➤ Monitors Free Disk Space on Drive G on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - ➤ Monitors Free Space on C Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on C Drive Below 2GB - {Severity1}**
  - ➤ Monitors Free Disk Space on Drive C Below 2GB on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - ➤ Monitors Free Space on D Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - ➤ Monitors Free Space on E Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**

> ➢ Monitors Free Space on F Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  > ➢ Monitors Free Space on G Drive Below 15 Percent on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  > ➢ Collects service status for All Automatic Services on Windows machines. Used for Monitor Log display and Reporting purposes only.

- **Windows (Core) - CPU and Memory - {Severity0}**
  > ➢ Collects CPU and Memory performance counters on Windows machines. Used for Monitor Log display and Reporting purposes only.

- **Windows (Core) - Machine Health - {Severity0}**
  > ➢ Collects Machine Health performance counters on Windows machines. Used for Monitor Log display and Reporting purposes only.

- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  > ➢ Monitors Processor and Memory Performance on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  > ➢ Monitors TCPv4 Connections Performance on Windows machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

Windows Servers

- **Windows Server (Core) - Cluster Services - {Severity3}**
  > ➢ Monitors Cluster Services on Windows Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  > ➢ Monitors Disk Time and Queue Length Performance on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

- **Windows Server (Core) - Drive C Performance - {Severity1}**
  > ➢ Monitors Drive C Performance on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Server (Core) - General System Performance - {Severity1}**
  > ➢ Monitors General System Performance on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Server (Core) - Server Reboots - {Severity1}**
  > ➢ Monitors Server Reboots on Windows Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Server (Core) - Standard Services - {Severity3}**
  > ➢ Monitors Standard Services on Windows Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Windows Server 2003 - Standard Services - {Severity3}**
  > ➢ Monitors Standard Services on Windows Server 2003 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Windows Server 2008 - Standard Services - {Severity3}**
  > ➢ Monitors Standard Services on Windows Server 2008 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Windows Server 2012 - Standard Services - {Severity3}**

➢ Description: Monitors Standard Services on Windows Server 2012 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Windows Workstations

- **Windows 7 - Standard Services - {Severity1}**

  ➢ Monitors Standard Services on Windows 7 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows 8 - Standard Services - {Severity1}**

  ➢ Monitors Standard Services on Windows 8 machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows Vista - Standard Services - {Severity1}**

  ➢ Monitors Standard Services on Windows Vista machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

- **Windows XP - Standard Services - {Severity1}**

  ➢ Monitors Standard Services on Windows XP machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity1.

Remote Access

- **Remote Access - Citrix Licensing Service - {Severity3}**

  ➢ Monitors Citrix Licensing Service on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix Licensing WMI Service - {Severity3}**

  ➢ Monitors Citrix Licensing WMI Service on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix MetaFrame Services - {Severity3}**

  ➢ Monitors Citrix MetaFrame Services on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix Server Services - {Severity3}**

  ➢ Monitors Citrix Server Services on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**

  ➢ Monitors Citrix Virtual Memory Optimization Service on Citrix Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Terminal Server Services - {Severity3}**

  ➢ Monitors Terminal Server Services on Terminal Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **Remote Access - Terminal Server Session Performance - {Severity2}**

  ➢ Monitors Terminal Server Session Performance on Terminal Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity2.

Security/Anti-Virus

- **AV - AVG Tech AVG Services - {Severity3}**

  ➢ Monitors AVG Tech AVG Services on AVG Tech AVG machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **AV - McAfee Enterprise Services - {Severity3}**

  ➢ Monitors McAfee Enterprise Services on McAfee Enterprise machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

- **AV - Microsoft SE-FEP Services {Severity3}**

➢ Monitors Microsoft SE-FEP Services on Microsoft SE-FEP machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity

▪ **AV - Sophos Antivirus Services - {Severity3}**

➢ Monitors Sophos Antivirus Services on Sophos Antivirus machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Symantec Antivirus Services - {Severity3}**

➢ Monitors Symantec Antivirus Services on Symantec Antivirus machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Symantec Endpoint Protection Services - {Severity3}**

➢ Monitors Symantec Endpoint Protection Services on Symantec Endpoint Protection machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Trend Micro Client Server Security Services - {Severity3}**

➢ Monitors Trend Micro Client Server Security Services on Trend Micro Client Server Security machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **AV - Trend Micro OfficeScan Services - {Severity3}**

➢ Monitors Trend Micro OfficeScan Services on Trend Micro OfficeScan machines. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Web Systems

▪ **Web Systems - FTP Server Service - {Severity3}**

➢ Monitors FTP Server Service on FTP Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **Web Systems - IIS Performance - {Severity3}**

➢ Monitors IIS Performance on IIS Servers. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **Web Systems - IIS Server - {Severity0}**

➢ Collects IIS Server performance counters on IIS Servers. Used for Monitor Log display and Reporting purposes only.

▪ **Web Systems - IIS Server Services - {Severity3}**

➢ Monitors IIS Server Services on IIS Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

▪ **Web Systems - SharePoint Server Services - {Severity3}**

➢ Monitors SharePoint Server Services on SharePoint Servers.. Used for Monitor Log display, Reporting, and Alerting purposes. Alarms are considered Severity3.

Event Sets

Security/Anti-Virus

▪ **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**

➢ Monitors for specific McAfee Anti-Virus Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**

➢ Monitors for specific Microsoft Security Essentials/Forefront Endpoint Protection Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] AV - Microsoft SE-FEP (I) - SYS - {Severity0}**

- ➢ Monitors for specific Microsoft Security Essentials/Forefront Endpoint Protection Informational events in the Application Event Log. Used for logging and reporting purposes only.
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - ➢ Monitors for specific Misc AntiVirus Error and Warning events in the Application & System Event Logs. Alarms are considered Severity3.
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - ➢ Monitors for specific Misc AntiVirus Informational events in the Application & System Event Logs. Alarms are considered Severity1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Error and Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - ➢ Monitors for specific Symantec/Norton AntiVirus Informational events in the Application Event Log. Used for logging and reporting purposes only.

Backup

- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the Application Event Log. Alarms are considered Severity1.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Backup Exec Error and Warning events in the System Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}**
  - ➢ Monitors for specific Backup Exec events in the Application Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}**
  - ➢ Monitors for specific Backup Exec Job Failure/Cancellation Error and Warning events in the Application Event Log. Alarms are considered Severity2.
- **zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}**
  - ➢ Monitors for specific Backup Exec Job Success events in the Application Event Log. Used for logging and reporting purposes only.
- **zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}**
  - ➢ Monitors for specific BrightStor ARCserve Error and Warning events in the Application Event Log. Alarms are considered Severity3.
- **zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}**

➢ Monitors for specific BrightStor ARCServe Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}**

  ➢ Monitors for specific Microsoft Windows Backup Error events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}**

  ➢ Monitors for specific Misc Backup Error events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}**

  ➢ Monitors for specific Misc Backup Informational events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}**

  ➢ Monitors for specific Misc Backup Warning events in the Application Event Log. Alarms are considered Severity1.

Database

- **zz[SYS] Database - SQL Server (E) - APP - {Severity2}**

  ➢ Monitors for specific SQL Server Error events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server (E) - APP - {Severity3}**

  ➢ Monitors for specific SQL Server Error events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}**

  ➢ Monitors for specific SQL Server - ACID Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}**

  ➢ Monitors for specific SQL Server - ACID Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}**

  ➢ Monitors for specific SQL Server - ACID Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}**

  ➢ Monitors for specific SQL Server - ACID events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}**

  ➢ Monitors for specific SQL Server - Backup Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}**

  ➢ Monitors for specific SQL Server - Backup Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}**

  ➢ Monitors for specific SQL Server - Backup events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}**

  ➢ Monitors for specific SQL Server - DB Resources Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}**

- ➢ Monitors for specific SQL Server - DB Resources Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}**
    - ➢ Monitors for specific SQL Server - DB Resources Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - **zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}**
    - ➢ Monitors for specific SQL Server - DB Resources events in the Application Event Log. Used for logging and reporting purposes only.
  - **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}**
    - ➢ Monitors for specific SQL Server - MSDTC Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}**
    - ➢ Monitors for specific SQL Server - MSDTC Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}**
    - ➢ Monitors for specific SQL Server - MSDTC Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - **zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}**
    - ➢ Monitors for specific SQL Server - MSDTC events in the Application Event Log. Used for logging and reporting purposes only.
  - **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**
    - ➢ Monitors for specific SQL Server - Network Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**
    - ➢ Monitors for specific SQL Server - Network Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**
    - ➢ Monitors for specific SQL Server - Query Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**
    - ➢ Monitors for specific SQL Server - Query Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**
    - ➢ Monitors for specific SQL Server - Replication Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**
    - ➢ Monitors for specific SQL Server - Replication Error and Warning events in the Application Event Log. Alarms are considered Severity2.
  - **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**
    - ➢ Monitors for specific SQL Server - Replication Error and Warning events in the Application Event Log. Alarms are considered Severity3.
  - **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**
    - ➢ Monitors for specific SQL Server - Replication events in the Application Event Log. Used for logging and reporting purposes only.
  - **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**
    - ➢ Monitors for specific SQL Server - Reporting Error and Warning events in the Application Event Log. Alarms are considered Severity1.
  - **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server - Reporting Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server - Reporting events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**

➢ Monitors for specific SQL Server Agent - Multiple Instances Error and Warning events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server Agent - Multiple Instances Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**

➢ Monitors for specific SQL Server Agent - Multiple Instances Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server Agent - Multiple Instances events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**

➢ Monitors for specific SQL Server Agent - Single Instance Error and Warning events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**

➢ Monitors for specific SQL Server Agent - Single Instance Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**

➢ Monitors for specific SQL Server Agent - Single Instance Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**

➢ Monitors for specific SQL Server Agent - Single Instance events in the Application Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**

➢ Monitors for specific SQL Server Cluster Informational events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**

➢ Monitors for specific SQL/Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.

Email

▪ **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**

➢ Monitors for specific Blackberry Server Error events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**

➢ Monitors for specific Blackberry Server Warning events in the Application Event Log. Alarms are considered Severity1.

▪ **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**

➢ Monitors for specific Blackberry Server Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}**

> ➢ Monitors for specific Blackberry Server Events Error events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}**
  > ➢ Monitors for specific Blackberry Server Events Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}**
  > ➢ Monitors for specific Exchange 2000 and 2003 Error events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}**
  > ➢ Monitors for specific Exchange 2000 and 2003 Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}**
  > ➢ Monitors for specific Exchange 2000 and 2003 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}**
  > ➢ Monitors for specific Exchange 2000 and 2003 and 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}**
  > ➢ Monitors for specific Exchange 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**
  > ➢ Monitors for specific Exchange 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
  > ➢ Monitors for specific Exchange 2007 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
  > ➢ Monitors for specific Exchange 2007 events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
  > ➢ Monitors for specific Exchange 2007 - Client Access Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**
  > ➢ Monitors for specific Exchange 2007 - Client Access Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
  > ➢ Monitors for specific Exchange 2007 - Client Access Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
  > ➢ Monitors for specific Exchange 2007 - Edge Transport Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  > ➢ Monitors for specific Exchange 2007 - Edge Transport Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  > ➢ Monitors for specific Exchange 2007 - Edge Transport Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**

> ➢ Monitors for specific Exchange 2007 - Hub Transport Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**

> ➢ Monitors for specific Exchange 2007 - Hub Transport Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**

> ➢ Monitors for specific Exchange 2007 - Hub Transport Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**

> ➢ Monitors for specific Exchange 2007 - Mailbox Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**

> ➢ Monitors for specific Exchange 2007 - Mailbox Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**

> ➢ Monitors for specific Exchange 2007 - Mailbox Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**

> ➢ Monitors for specific Exchange 2007 - Mailbox events in the Application Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**

> ➢ Monitors for specific Exchange 2007 - Transport Services Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**

> ➢ Monitors for specific Exchange 2007 - Transport Services Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**

> ➢ Monitors for specific Exchange 2007 - Transport Services Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**

> ➢ Monitors for specific Exchange 2007 - Unified Messaging Error and Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**

> ➢ Monitors for specific Exchange 2007 - Unified Messaging Error and Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**

> ➢ Monitors for specific Exchange 2007 - Unified Messaging Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**

> ➢ Monitors for specific Exchange 2010 Server Error events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**

> ➢ Monitors for specific Exchange 2010 Server Warning events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**

> ➢ Monitors for specific Exchange 2010 Server Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**

- ➢ Monitors for specific Exchange 2010 Server Warning events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
    - ➢ Monitors for specific Exchange Server Error events in the Application Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange Server Error events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
    - ➢ Monitors for specific Exchange Server Informational events in the System Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
    - ➢ Monitors for specific Exchange Server 5.5 Error events in the Application Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**
    - ➢ Monitors for specific Exchange/Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
    - ➢ Monitors for specific SMTP/Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.

Hardware

  - ▪ **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
    - ➢ Monitors for specific Dell Battery Error and Warning events in the System Event Log. Alarms are considered Severity1.
  - ▪ **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
    - ➢ Monitors for specific Dell Battery Error and Warning events in the System Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
    - ➢ Monitors for specific Dell Battery Error and Warning events in the System Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
    - ➢ Monitors for specific Dell Battery events in the System Event Log. Used for logging and reporting purposes only.
  - ▪ **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
    - ➢ Monitors for specific Dell Controller Error and Warning events in the System Event Log. Alarms are considered Severity1.
  - ▪ **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
    - ➢ Monitors for specific Dell Controller Error and Warning events in the System Event Log. Alarms are considered Severity2.
  - ▪ **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
    - ➢ Monitors for specific Dell Controller Error and Warning events in the System Event Log. Alarms are considered Severity3.
  - ▪ **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
    - ➢ Monitors for specific Dell Controller events in the System Event Log. Used for logging and reporting purposes only.
  - ▪ **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**

- ➢ Monitors for specific Dell Electrical Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**

  - ➢ Monitors for specific Dell Electrical Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**

  - ➢ Monitors for specific Dell Electrical Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**

  - ➢ Monitors for specific Dell Electrical events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**

  - ➢ Monitors for specific Dell Enclosure Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**

  - ➢ Monitors for specific Dell Enclosure Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**

  - ➢ Monitors for specific Dell Enclosure Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**

  - ➢ Monitors for specific Dell Enclosure events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**

  - ➢ Monitors for specific Dell Environmental Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**

  - ➢ Monitors for specific Dell Environmental Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**

  - ➢ Monitors for specific Dell Environmental Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**

  - ➢ Monitors for specific Dell Environmental events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**

  - ➢ Monitors for specific Dell Fan Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**

  - ➢ Monitors for specific Dell Fan Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**

  - ➢ Monitors for specific Dell Fan Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**

  - ➢ Monitors for specific Dell Fan events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**

- Monitors for specific Dell Hardware Changes Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**

  - Monitors for specific Dell Hardware Changes Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**

  - Monitors for specific Dell Hardware Changes Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**

  - Monitors for specific Dell Hardware Changes events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**

  - Monitors for specific Dell Hardware Log Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**

  - Monitors for specific Dell Hardware Log Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**

  - Monitors for specific Dell Hardware Log events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**

  - Monitors for specific Dell Media Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**

  - Monitors for specific Dell Media Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**

  - Monitors for specific Dell Media Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**

  - Monitors for specific Dell Media events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**

  - Monitors for specific Dell Memory Prefailure Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**

  - Monitors for specific Dell Memory Prefailure Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**

  - Monitors for specific Dell OMSA System Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**

  - Monitors for specific Dell OMSA System Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**

  - Monitors for specific Dell OMSA System Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**

- ➢ Monitors for specific Dell OMSA System events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell OMSM System Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell OMSM System Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Physical Disk Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Physical Disk Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell Physical Disk Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitors for specific Dell Physical Disk events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Power Management Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Power Management Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}**
  - ➢ Monitors for specific Dell Power Management Error and Warning events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitors for specific Dell Power Management events in the System Event Log. Alarms are considered Severity0.

- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Processor Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Processor Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitors for specific Dell Processor events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}**
  - ➢ Monitors for specific Dell Redundancy Mirror Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}**
  - ➢ Monitors for specific Dell Redundancy Mirror Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Dell Redundancy Mirror events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**

  ➢ Monitors for specific Dell Temperature Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**

  ➢ Monitors for specific Dell Temperature Error and Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**

  ➢ Monitors for specific Dell Temperature Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**

  ➢ Monitors for specific Dell Temperature events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**

  ➢ Monitors for specific Dell Virtual Disk Error and Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}**

  ➢ Monitors for specific Dell Virtual Disk Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}**

  ➢ Monitors for specific Dell Virtual Disk events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}**

  ➢ Monitors for specific HP Top Tools Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}**

  ➢ Monitors for specific HP/Compaq Insight Manager Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}**

  ➢ Monitors for specific HP/Compaq StorageWorks Error and Warning events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}**

  ➢ Monitors for specific IBM SeriesX Events Error events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}**

  ➢ Monitors for specific Misc HW Error events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}**

  ➢ Monitors for specific Misc HW Error events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}**

  ➢ Monitors for specific Misc HW Warning events in the System Event Log. Alarms are considered Severity1.

Network Infrastructure

- **zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}**

➢ Monitors for specific Active Directory Error events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**
  ➢ Monitors for specific Active Directory Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**
  ➢ Monitors for specific Active Directory Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**
  ➢ Monitors for specific Active Directory Events Error events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**
  ➢ Monitors for specific Active Directory Events Warning events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**
  ➢ Monitors for specific Active Directory Logon/Logoff/Lockout Activity Failure Audit events in the Security Event Log. Alarms are considered Severity3.

- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
  ➢ Monitors for specific Active Directory NTDS Error events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
  ➢ Monitors for specific Active Directory NTDS Error events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  ➢ Monitors for specific Active Directory NTDS Informational events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  ➢ Monitors for specific DHCP Server Error events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  ➢ Monitors for specific DHCP Server Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  ➢ Monitors for specific DNS Server Error events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  ➢ Monitors for specific DNS Server Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  ➢ Monitors for specific WINS Server Error events in the System Event Log. Alarms are considered Severity1.

Remote Access

- **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  ➢ Monitors for specific Citrix MetaFrame Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**

➢ Monitors for specific Citrix Server Events Error events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**

  ➢ Monitors for specific Terminal Server Events Error events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**

  ➢ Monitors for specific Terminal Server Events Error events in the Application Event Log. Alarms are considered Severity3.

Web Systems

- **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**

  ➢ Monitors for specific IIS 6 Events Error and Warning events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**

  ➢ Monitors for specific IIS 7 Events Error events in the Application Event Log. Alarms are considered Severity2.

- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**

  ➢ Monitors for specific IIS 7 Events Error events in the Application Event Log. Alarms are considered Severity3.

- **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**

  ➢ Monitors for specific IIS Server Error events in the Application Event Log. Alarms are considered Severity1.

- **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**

  ➢ Monitors for specific IIS Server Warning events in the Application Event Log. Alarms are considered Severity1.

OS Platforms

- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}**

  ➢ Monitors for specific Common Windows Server Error events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}**

  ➢ Monitors for specific Common Windows Server Error events in the System Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}**

  ➢ Monitors for specific Common Windows Server events in the System Event Log. Used for logging and reporting purposes only.

- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}**

  ➢ Monitors for specific Common Windows Server Failure Audit events in the Security Event Log. Alarms are considered Severity1.

- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}**

  ➢ Monitors for specific Common Windows Server Failure Audit events in the Security Event Log. Alarms are considered Severity3.

- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}**

  ➢ Monitors for specific Common Windows Server Warning events in the System Event Log. Alarms are considered Severity1.

- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}**

  ➢ Monitors for specific Common Windows Server Warning events in the System Event Log. Alarms are considered Severity2.

- **zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}**

➢ Ignores monitoring for specific Common Windows Server Error and Warning events in the Application & System Event Logs.

▪ **zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}**

➢ Monitors for specific Windows Server Print Spooler Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}**

➢ Monitors for specific Windows Server Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}**

➢ Monitors for specific Windows Server Service Control Manager Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}**

➢ Monitors for specific Windows Server Service Control Manager Informational events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}**

➢ Monitors for specific Windows Server System Shutdown Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}**

➢ Monitors for specific Common Windows Server 2008 Error events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}**

➢ Monitors for specific Common Windows Server 2008 Error events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**

➢ Monitors for specific Common Windows Server 2008 Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**

➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the Application Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**

➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the Application Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**

➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**

➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**

➢ Monitors for specific Advanced Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Advanced Windows Server 2008 events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**

➢ Monitors for specific Basic Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**

➢ Monitors for specific Basic Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**

➢ Monitors for specific Basic Windows Server 2008 Error and Warning events in the System Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**

➢ Monitors for specific Basic Windows Server 2008 events in the System Event Log. Used for logging and reporting purposes only.

▪ **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**

➢ Monitors for specific Basic Windows Server 2008 Failure Audit events in the Security Event Log. Alarms are considered Severity1.

▪ **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**

➢ Monitors for specific Basic Windows Server 2008 Failure Audit events in the Security Event Log. Alarms are considered Severity2.

▪ **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**

➢ Monitors for specific Basic Windows Server 2008 Failure Audit events in the Security Event Log. Alarms are considered Severity3.

▪ **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**

➢ Monitors for specific Common Windows Workstation Error events in the System Event Log. Alarms are considered Severity1.

Index