Monitoring Services Guide

Overview

Absolute Monitors are used to evaluate the condition of any device and then perform an action when a threshold is reached. These monitors then generate alerts, by opening tickets, using the information obtained from the monitor.

Event Monitors

Table 1: Remote Monitors—Event Monitors

Monitor Name	Description	Groups	Interval	Alert Action	Report Category
EV - 4110 DAG Log Replay Suspended	Checks for *!!!0!!!MSExchangeRepl!!!4110!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 10 MinsMinutes	Default - Create Ticket	Eventlog Checks
EV - 4111 DAG Log Replay Resumed	Checks for *!!!0!!!MSExchangeRepl!!!4111!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 10 Minutes	Default - Create Ticket	Eventlog Checks
EV - 10036 DAG Block Mode	Checks for *!!!0!!!MSExchangeRepl!!!10036!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 10 Minutes	Default - Create Ticket	Eventlog Checks
EV - 1062 Cluster Online	Checks for *!!!0!!!FailoverClustering!!!1062!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 1069 Microsoft-Windows-FailoverClustering	Checks for System!!!1!!!Microsoft- Windows-FailoverClustering!!!1069 in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles	Every 60 Seconds	Default - Create Ticket	Eventlog Checks
EV - 1125 Cluster Online	Checks for *!!!0!!!FailoverClustering!!!1125!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks

EV - 1135 Microsoft-Windows-FailoverClustering	Checks for System!!!1!!!Microsoft- Windows-FailoverClustering!!!1135 in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles	Every 60 Seconds	Default - Create Ticket	Eventlog Checks
EV - 1177 Microsoft-Windows-FailoverClustering	Checks for System!!!1!!!Microsoft- Windows-FailoverClustering!!!1177 in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles	Every 60 Seconds	Default - Create Ticket	Eventlog Checks
EV - 1204 Cluster Offline	Checks for *!!!0!!!FailoverClustering!!!1204!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 1205 Microsoft-Windows-FailoverClustering	Checks for System!!!1!!!Microsoft- Windows-FailoverClustering!!!1205 in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles	Every 60 Seconds	Default - Create Ticket	Eventlog Checks
EV - 15002 Exchange Backpressure	Checks for *!!!0!!!MSExchangeTransport!!!15002!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers. Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 15004 Exchange Backpressure	Checks for *!!!0!!!MSExchangeTransport!!!15004!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 15006 Exchange Backpressure	Checks for *!!!0!!!MSExchangeTransport!!!15006!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 1561 Cluster Offline	Checks for *!!!0!!!FailoverClustering!!!1561!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 2090 DAG Failover	Checks for *!!!0!!!MSExchangeRepl!!!2090!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks
EV - 2153 DAG Communication	Checks for *!!!0!!!MSExchangeRepl!!!2153!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Eventlog Checks

EV - Exchange DB Size	Checks for *!!!0!!!MSExchangeIS Mailbox Store!!!9690!!!* in the event logs and if it exists, a ticket is created.	Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Eventlog Checks

File Monitors

Table 1: Remote Monitors—File Monitors

Monitor Name	Description	Groups	Interval	Alert Action	Report Category
Cluster Node Patching Ready	Checks to see if PatchReady.txt file is in the %windir%\temp directory and if it exists, runs the 'Install All Approved Patches' script.	_System Automation.Cluster Detected	Every 30 Seconds	Cluster Patch Ready	File Monitors

Network Monitors

Table 3: Remote Monitors—Network Monitors

Monitor Name	Description	Groups	Interval	Alert Action	Report Category
TCP – Connection Current	Monitors the number of established TCP connections	Service Plans.MAC Workstations. Managed 8x5 Service Plans.MAC Workstations. Managed 24x7 Service Plans.MAC Servers.Managed 8x5 Service Plans.MAC Servers.Managed 24x7	Every 5 minutes	Default – Raise Alert	Network Checks
TCP – Connection Current	Monitors the number of established TCP connections	Service Plans.LinuxMachines. Managed 8x5 Service Plans. LinuxMachines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Network Checks
TCP - DNS Port 53	Verifies the network port is open and communicating. If the port is not open, a ticket iscreated	Port Management.DNS- 53 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - FTP Port 21	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.FTP -21 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - HTTP Port 80	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.HTTP- 80 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks

TCP - HTTPS Port 443	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.HTTPS -443 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - ICA Port 1494	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.ICA - 1494 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - IMAP Port 143	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.IMAP - 143 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - LDAP Port 389	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.LDAP - 389 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - MSSQL Port 1433	Verifies the network port is open and communicating. If the port is not open, a ticket is created	PortManagement.MSSQL -1433 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - MySQL Port 3306	Verifies the network port is open and communicating. If the port is not open, a ticket is created	PortManagement.MySQL -3306 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - Oracle Port 1521	Verifies the network port is open and communicating. If the port is not open, a ticket is created	PortManagement.Oracle -1521 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - POP Port 110	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.POP3- 110 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - RDP Port 3389	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.RDP- 3389 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - SMTP Port 25	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.SMTP - 25TCP	Every 10 Minutes	Default - Create Ticket	Network Checks
TCP - SMTPAUTH Port 587	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.SMTPAUT H - 587 TCP	Every 10 Minutes	Default - Workstation 24x7	Network Checks
TCP - SSH Port 22	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.SSH -22 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks

UDP – Connection Current	Monitors the number of established TCP connections	Service Plans.MAC Workstations. Managed 8x5 Service Plans.MAC Workstations. Managed 24x7 Service Plans.MAC Servers.Managed 8x5 Service Plans.MAC Servers.Managed 24x7	Every 5 minutes	Default – Raise Alert	Network Checks
UDP– Connection Current	Monitors the number of established TCP connections	Service Plans.LinuxMachines. Managed 8x5 Service Plans. LinuxMachines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Network Checks
UDP - DHCP Port 67	Verifies the network port is open and communicating. If the port is not open, a ticket is created	PortManagement.DHCP -67 UDP	Every 10 Minutes	Default - Create Ticket	Network Checks
UDP - DNS Port 53	Verifies the network port is open and communicating. If the port is not open, a ticket is created	Port Management.DNS- 53 TCP	Every 10 Minutes	Default - Create Ticket	Network Checks

Performance Monitors

Table 4: Remote Monitors—Performance Monitors

Monitor Name	Description	Groups	Interval	Alert Action	Report Category
Perf - Accepting TCP Connections	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.ISA Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Active Mailbox Delivery Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Active Non-SMTP Delivery Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Active Remote Delivery Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Active Sessions	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Terminal Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Active Temp Tables	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - AD DB Cache % Hit	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers.Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Aggregate Delivery Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Application Resolution Time (ms)	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Citrix XenApp Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Available MBytes	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 120 Seconds	Create Ticket and Raise Alert	Performance Checks
Perf - Backlogged Packets	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.ISA Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Cache Page Fault Stalls/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Cache Page Faults/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Categorizer Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Connection Reset/sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf – CPU % Idle	Monitors to check the percentage of CPU time in idle mode.	Service Plans.Mac Servers. Managed 8x5 Service Plans.MacServers. Managed 24x7 Service Plans.Mac Workstations. Managed 8x5 Service Plans.Mac Workstations. Managed 8x5	Every 5 minutes	Default – Raise Alert	Performance Checks
Perf – CPU % Idle	Monitors to check if the percentage of CPU time in idle mode.	Service Plans.LinuxMachines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Performance Checks
Perf – CPU % IOWait	Monitors to check if the percentage of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.	Service Plans.Linux Machines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Performance Checks
Perf CPU % System	Monitors to check the percentage of CPU time in system mode.	Service Plans.Mac Servers. Managed 8x5 Service Plans.Mac Servers. Managed 24x7 Service Plans.Mac Workstations. Managed 8x5 Service Plans.Mac Workstations. Managed 8x5	Every 5 minutes	Default – Raise Alert	Antivirus Checks
Perf CPU % System	Monitors to check if the percentage of CPU time in system mode.	Service Plans.Linux Machines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Antivirus Checks
Perf – CPU % User	Monitors to check if the percentage of CPU time in user mode	Service Plans.Mac Servers. Managed 8x5 Service Plans.Mac Servers. Managed 24x7 Service Plans.Mac Workstations. Managed 8x5 Service Plans.Mac Workstations. Managed 8x5	Every 5 minutes	Default – Raise Alert	Performance Checks

Perf – CPU Load – 5 min avg	Monitors to check if the CPU load average for the past five minutes	Service Plans.Mac Servers. Managed 8x5 Service Plans.Mac Servers. Managed 24x7 Service Plans.Mac Workstations. Managed 8x5 Service Plans.Mac Workstations. Managed 8x5	Every 5 minutes	Default – Raise Alert	Performance Checks
Perf – CPU Load – 5 min avg	Monitors to check tthe CPU load average for the past five minutes	Service Plans.Linux Machines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Performance Checks
Perf - Current Cache Fetches Average Milliseconds/	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.ISA Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Current Disk Queue Length C Drive	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - Data Store Connection Failure	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Citrix XenApp Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Database Page Fault Stalls/sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - DHCP Acks / Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DHCP Active Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DHCP Conflict Check Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DHCP Declines Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DHCP Discovers Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers.Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DHCP Informs Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - DHCP Nacks Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DHCP Requests Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DHCP Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Disk % Idle Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows. Servers Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf – Disk Read – Primary Drive	Monitors to check the primary disk drive read rate in MB/second	Service Plans.Linux Machines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Antivirus Checks
Perf- Disk TPS – Primary Disk	Monitors to check if the primary disk drive transactions per second (TPS)	Service Plans.Linux Machines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Antivirus Checks
Perf – Disk Transfer – Primary Drive	Monitors to check if the primary disk transfer rate in MB/sec	Service Plans.Mac Servers. Managed 8x5 Service Plans.Mac Servers. Managed 24x7 Service Plans.Mac Workstations. Managed 8x5 Service Plans.Mac Workstations. Managed 8x5	Every 5 minutes	Default – Raise Alert	Performance Checks

Perf - Disk Transfers/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - Disk Utilization	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf – Disk Write – Primary Drive	Monitors to check if the primary disk drive write rate in MB/second	Service Plans.Linux Machines. Managed 8x5 Service Plans.Linux Machines. Managed 24x7	Every 2 minutes	Default – Raise Alert	Antivirus Checks
Perf - DNS Caching Memory	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DNS Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DNS Database Node Memory	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DNS Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DNS Dynamic Updates Timeouts	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DNS Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - DNS Nbstat Memory	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DNS Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DNS Zone Transfer Failure	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows DNS Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DRA Inbound Bytes Total/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DRA Inbound Object Updates Remaining in Pac	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DRA Outbound Bytes Total / Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DRA Pending Replication Synchronization	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Dropped Packets Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.ISA Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DS Threads in Use	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - DTC Calls	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Errors Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.Windows IIS Web Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - File Cache Hits %	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.Windows IIS Web Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - File Directory Searches	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows File Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Files Open	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows File Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Files Opened Total	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows File Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - HTTP Requests	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.Windows IIS Web Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Hyper V Logical Processors	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows HyperV Host	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Hyper V Machine Health Critical	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows HyperV Host	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Hyper V Partitions	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows HyperV Host	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Hyper V Total Pages	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows HyperV Host	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Inactive Sessions	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Terminal Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Jobs	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows Print Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Largest Delivery Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - LDAP Bind Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - LDAP Client Sessions	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - LDAP Read Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Performance Checks
Perf - LDAP Search Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 5 Minutes	Default - Create Ticket	Performance Checks
Perf - LDAP Searches / Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - LDAP Searches Timed Out	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Local Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Log Generation Checkpoint Depth	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Log Record Stalls/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Log Threads Waiting	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Logical Connections	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Long Running LDAP Operations	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Mars Deadlocks	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Memory Pages Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 90 Seconds	Default - Create Ticket	Performance Checks

Perf - Memory Utilization	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 30 Minutes	Default - Create Ticket	Performance Checks
Perf - Messages Queued for Submission	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Messages Queued for Submission Public	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Network Bandwidth	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - NIC Output Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - NIC Packets Received Errors	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks

Perf - Not Ready Errors	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows Print Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - OWA Average Response Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - OWA Average Search Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Pages Input/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - Poison Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Print Job Errors	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows Print Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Processes blocked	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Processor % Privileged Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - Processor % User Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - Processor Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7	Every 30 Minutes	Default - Create Ticket	Performance Checks
Perf - Processor Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 30 Minutes	Default - Create Ticket	Performance Checks
Perf - Processor Utilization	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 90 Seconds	Default - Create Ticket	Performance Checks

Perf - Receive Queue Size	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Remote Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Retry Remote Delivery Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - RPC Average Latency	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - RPC Average Latency IS	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - RPC Average Latency MBX	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles. Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - RPC Averaged Latency	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - RPC Requests	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - RPC Requests CAS	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - RPC Requests IS	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Send Queue Size	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Submission Queue length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - System Uptime	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Daily	Default - Create Ticket	Performance Checks
Perf - Table Open Cache Hits/Sec	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Total CPU Processor Time	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 90 Seconds	Default - Create Ticket	Performance Checks
Perf - Total Files Cached	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.Windows IIS Web Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Total Jobs Printed	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows Print Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Total Pages Printed	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows Print Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Total Sessions	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Terminal Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Transactions	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Unreachable Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - User Connections	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Version Buckets Allocated	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.WindowsMessaging Servers.Exchange 2010 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks
Perf - Work Queue Length	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Perf - Worker Threads	All performance monitors are named after what they are testing. All thresholds are based on Microsoft standards, where applicable, and if the condition exceeds the threshold, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.ISA Servers	Every 60 Seconds	Default - Create Ticket	Performance Checks

Service Monitors

Table 5: Remote Monitors—Service Monitors

Monitor Name	Description	Groups	Interval	Alert Action	Report Category
BAssist Service	Checks to see if the 'wBackupAssist' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.Backup Assist	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
BExec Engine	Checks to see if the 'BackupExecJobEngine' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.Backup Exec	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
BExec Service	Checks to see if the 'BackupExecRPCService' is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.Backup Exec	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
Shadow Protect Service	Checks to see if the 'ShadowProtectSvc' is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.Shadow Protect	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-AcrSch2Svc	Checks to see if the 'AcrSch2Svc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.Acronis	Every Minute	~Autofix Action Restart Service	Service Monitors

SVC-addressbook	Monitors to check if the Mac Server AddressBook service is running	Service Plans.MAC Servers.Server Roles.OS X Messaging Services.OS X Messaging -AddressBook	Every two minuts	~Autofix Action Restart Service	Service Monitors
SVC-afp	Monitors to check if the Mac Server Apple File Protocol AFP service is running	Service Plans.MAC Servers.Server Roles.OS X Core Services.OS X Core Services - File Sharing - AFP	Every two minuts	~Autofix Action Restart Service	Service Monitors
SVC-Apache2	Checks to see if the 'Apache2' service' is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Web/Proxy Servers.Windows Apache Web Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Apache2.2	Checks to see if the 'Apache2.2' service' is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Web/Proxy Servers.Windows Apache Web Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-avgwd	Checks to see if the 'avgwd' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Servers.Server Anti-Virus Only Service Plans.Windows Workstations. Managed 2 4x7	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-BBAttachServer	Checks to see if the 'BBAttachServer' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-BIND	Checks to see if the 'Named' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Servers Core Services. Windows DNS Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-BlackBerry Controller	Checks to see if the 'BlackBerry Controller' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-BlackBerry Dispatcher	Checks to see if the 'BlackBerry Dispatcher' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-BlackBerry Router	Checks to see if the 'BlackBerry Router' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-BlackBerry Server Alert	Checks to see if the 'BlackBerry Server Alert' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Blackberry Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-calendar	Monitors to check if the Mac Server Calendar service is running	Service Plans.MAC Servers.Server Roles.OS X Messaging Services.OS X Messaging - Calendar	Every two minutes	~Autofix Action Restart Service	Service Monitors
SVC-CASAD2DWebSvc	Checks to see if the 'CASAD2DWebSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.CA Backup	Every Minute	~Autofix Action Restart Service	Service Monitors
SVC-Citrix Encryption Service	Checks to see if the 'Citrix Encryption Servicet' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers. Citrix XenApp Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Citrix Licensing	Checks to see if the 'Citrix Licensing' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Citrix XenApp Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Citrix_GTLicensingProv	Checks to see if the 'Citrix_GTLicensingProvt' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Citrix XenApp Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-CitrixCseEngine	Checks to see if the 'CitrixCseEnginet' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Remote Access Servers.Citrix XenApp Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-CitrixHealthMon	Checks to see if the 'CitrixHealthMont' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers.Citrix XenApp Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC- ConnectWiseUpdaterService	Checks to see if the 'ConnectWiseUpdaterServicet' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.ConnectWise Server	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-CryptSvc	Checks to see if the 'CryptSvct' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans. WindowsWorkstations. Managed 24x7 Service Plans.WindowsWorkstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-cups	Monitors to check if the CUPS (Common Unix Printing System) service is running.	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux CUPS Print Servers	Every 60 seconds	~Autofix Action Restart Service	Service Monitors
SVC-DataCollectorSvc	Checks to see if the 'DataCollectorSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Small Business Servers.SBS 2008 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Dfs	Checks to see if the 'Dfs' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-DFSR	Checks to see if the 'DFSR' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Dhcp	Checks to see if the 'Dhcp' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors

SVC-dhcpd	Monitors to check if the DHCP service is running	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux DHCP Servers	Every 60 seconds	~Autofix Action Restart Service	Service Monitors
SVC-DHCPServer	Checks to see if the 'DHCPServer' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Windows DHCP Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-DNS	Checks to see if the 'DNS' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Windows DNS Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Dnscache	Checks to see if the 'Dnscache' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Workstations.Managed24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-EdgeCredentialSvc	Checks to see if the 'EdgeCredentialSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-ekrn	Checks to see if the 'ekrn' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Servers. Server	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-EmailRobot	Checks to see if the 'EmailRobot' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.ConnectWise Server	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors

SVC-ERA_SERVER	Checks to see if the 'ERA_SERVER' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Servers. Server Anti-Virus Only	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Eset_MSP_Service	Checks to see if the 'Eset_MSP_Service' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Servers.Server Anti-Virus Only	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-exim4	Monitors to check if the Exim4 SMTP service is running	Service Plans.Linux Machines.Server Roles.Linux Messaging Services.Linux SMTP-Exim4 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-FWSRV	Checks to see if the 'fwsrv' service is running and if it isn't, a ticket is created.	Service Plans.Windows Servers.Server Roles.Windows Web/Proxy Servers.ISA Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors
SVC-gpsvc	Checks to see if the 'gpsvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-httpd	Monitors to check if the httpd(apache2) service is running	Service Plans.Linux Machines.Server Roles.Linux Web/Proxy Servers.Linux HTTP-Apache2 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-IISADMIN	Checks to see if the 'IISAdmin' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Web/Proxy Servers.Windows IIS Web Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-IMAP4Svc	Checks to see if the 'IMAP4Svc' service is running and if it isn't a ticket is created.	Service Plans.Windows Servers.Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors

SVC-ipfilter	Monitors to check if the Mac Server Firewall(ipfilter) service is running	Service Plans.MAC Servers.Server Roles.OS X Core Services.OS X Core Services - Firewall IPFilter	Every 2 minutes	~Autofix Action Restart Service	Service Monitors
SVC-jabber	Monitors to check if the Mac Server Chat (jabber) service is running	Service Plans.MAC Servers.Server Roles.OS X Messaging Services.OS X Messaging - Chat	Every 2 minutes	~Autofix Action Restart Service	Service Monitors
SVC-kdc	Checks to see if the 'kdc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-LabMySQL	Checks to see if the 'LabMySQL' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.TAC Agent Server	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-LanmanServer	Checks to see if the 'LanmanServer' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.Windows Servers Core Services.Domain Controllers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-LTAgent	Checks to see if the 'LTAgent' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.TAC Agent Server	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-LTRedirSvc	Checks to see if the 'LTRedirSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.TAC Agent Server	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-mail	Monitors to check if the Mac Server Mail service is running.	Service Plans.MAC Servers.Server Roles.OS X Messaging Services.OS X Messaging - Mail	Every 2 minutes	~Autofix Action Restart Service	Service Monitors
SVC-MsDtsServer100	Checks to see if the 'MsDtsServer100' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-MSExchangeAB	Checks to see if the 'MSExchangeAB' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeADAM	Checks to see if the 'MSExchangeADAM' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeADTopology	Checks to see if the 'MSExchangeADTopology' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC- MSExchangeAntispamUpdate	Checks to see if the 'MSExchangeAntispamUpdate' service is running and if it isn't, will	Service Plans.Windows Servers. Server Roles.Windows	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
	call the Monitor Restart Service script to attempt to fix the issue.	Messaging Servers. Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers			
SVC-MSExchangeEdgeCred	Checks to see if the 'MSExchangeEdgeCred' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeEdgeSync	Checks to see if the 'MSExchangeEdgeSync' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeFBA	Checks to see if the 'MSExchangeFBA' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-MSExchangeFDS	Checks to see if the 'MSExchangeFDS' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeIMAP4	Checks to see if the 'MSExchangeIMAP4' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeIS	Checks to see if the 'MSExchangeIS' service is running and if it isn't, a ticket is created..	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers. Exchange 2007 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors
SVC-MSExchangeMailboxAssistants	Checks to see if the 'MSExchangeMailboxAssistants' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeMailboxReplication	Checks to see if the 'MSExchangeMailboxReplication' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC- MSExchangeMailSubmission	Checks to see if the 'MSExchangeMailSubmission' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeMGMT	Checks to see if the 'MSExchangeMGMT' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors
SVC-MSExchangeMTA	Checks to see if the 'MSExchangeMTA' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors

SVC-MSExchangePOP3	Checks to see if the 'MSExchangePOP3' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeProtectedServiceHo st	Checks to see if the 'MSExchangeProtecedServiceHost"service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeRepl	Checks to see if the 'MSExchangeRepl' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows MessagingServers. Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeRPC	Checks to see if the 'MSExchangeRPC' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeSA	Checks to see if the 'MSExchangeSA' service is running and if it isn't, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors
SVC-MSExchangeSearch	Checks to see if the 'MSExchangeSearch' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeServiceHost	Checks to see if the 'MSExchangeServiceHost' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeThrottling	Checks to see if the 'MSExchangeThrottling' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-MSExchangeTransport	Checks to see if the 'MSExchangeTransport' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeTransportLogSearch	Checks to see if the 'MSExchangeTransportLogSearch' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSExchangeUM	Checks to see if the 'MSExchangeUM' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MsMpSvc	Checks to see if the 'MsMpSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Servers. Server Anti-Virus Only Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Workstations. Workstation Anti-Virus Only	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSMQ	Checks to see if the 'MSMQ' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSSpeechService	Checks to see if the 'MSSpeechService' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2007 Servers Service Plans.Windows Servers. Server Roles.Windows Messaging Servers. Exchange 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-MSSQLSERVER	Checks to see if the 'MSSQLSERVER' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2005 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MSSQLServerOLAPService	Checks to see if the 'MSSQLServerOLAPService' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers.Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MySQL	Checks to see if the 'MySQL' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.Windows MYSQL Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-mysqld	Monitors to check if the Mysqld database service is running	Service Plans.Linux Machines.Server Roles.Linux Database Services.Linux MySQL Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-MySQL55	Checks to see if the 'MySQL55' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.Windows MYSQL Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-named	Monitors to check if the Bind(named) service is running	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux DNS-Bind Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Netman	Checks to see if the 'Netman' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors

SVC-nfs	Monitors to check if the Mac Server NFS (network file system) is running	Service Plans.MAC Servers.Server Roles.OS X Core Services.OS X Core Services - File Sharing - NFS	Every two minutes	~Autofix Action Restart Service	Service Monitors
SVC-notification	Monitors to check if the Mac Server Notification service is running.	Service Plans.MAC Servers.Server Roles.OS X Messaging Services.OS X Messaging - Mail -Notification	Every two minutes	~Autofix Action Restart Service	Service Monitors
SVC-NTDS	Checks to see if the 'NTDS' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Domain Controllers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-NtFrs	Checks to see if the 'NtFrs' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-ntpd	Monitors to check if the NTP(Network Time Protocol) service is running.	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux NTP Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-nvspwmi	Checks to see if the 'nvspwmi' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Windows HyperV Host	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-PlugPlay	Checks to see if the 'PlugPlay' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-POP3Svc	Checks to see if the 'POP3Svc' service is running and if it isn't, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors

SVC-ProfSvc	Checks to see if the 'ProfSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Workstations. Managed 24x7	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-ProfSvc	Checks to see if the 'ProfSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC-postfix	Monitors to check if the Postfix SMTP service is running	Service Plans.Linux Machines.Server Roles.Linux Messaging Services.Linux SMTP-Postfix Servers	Every 60 seconds	~Autofix Action Restart Service	Service Monitors
SVC –postgresql	Monitors to check if the Postgresql database service is running	Service Plans.Linux Machines.Server Roles.Linux Database Services.Linux PostgreSQL Servers	Every 60 seconds	~Autofix Action Restart Service	Service Monitors
SVC – radius	Monitors to check if the FreeRadius service is running	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux FreeRadius Servers	Every 60 seconds	~Autofix Action Restart Service	Service Monitors
SVC - Replay XML	Checks to see if the 'Reply XML Command' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.AppAssure	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC - ReplayAgent64	Checks to see if the 'Reply Agent64' service' is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.AppAssure	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors
SVC - ReplayServer64	Checks to see if the 'ReplyServer64' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Backup Management.AppAssure	Every 5 Minutes	~Autofix Action Restart Service	Service Monitors

SVC-ReportServer	Checks to see if the 'ReportServer' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-RESvc	Checks to see if the 'RESvc' service is running and if it isn't, a ticket is created.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors
SVC-RpcSs	Checks to see if the 'RpcSs' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Domain Controllers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SamSs	Checks to see if the 'SamSs' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5 Service Plans.Windows Workstations. Managed 24x7 Service Plans. Windows Workstations. Managed 8x5 Service Plans.WindowsWorkstations. Managed HAAS	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SBAMSvc	Checks to see if the 'SBAMSvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.WindowsServers. Managed 24x7 Service Plans.WindowsServers. Managed 8x5 Service Plans.Windows Servers.Server Anti-Virus Only	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SBCore	Checks to see if the 'SBCore' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Small Business Servers.SBS 2003 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-semsrv	Monitors to check if the Symantec Endpoint Protection Management service is running.	Service Plans.Windows Servers. Server Anti-virus only Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 seconds	~Autofix Action Restart Service	Antivirus Checks

SVC-SepMasterService	Monitors to check if the Symantec Endpoint Protection service is running	Service Plans.Windows Servers. Server Anti-virus only Service Plans.Windows Servers. Managed 24x7 Service Plans.WindowsServers. Managed 8x5 Service Plans.Windows Workstations. Workstation Anti-Virus Only	Every 60 seconds	~Autofix Action Restart Service	Antivirus Checks
		Service Plans.WindowsWorkstations. Managed 24x7 Service Plans.WindowsWorkstations .Managed 8x5 Service Plans.Windows Workstations. Managed HAAS			
SVC-smb	Monitors to check if the Mac Server SMB/Windows File Sharing service is running	Service Plans.MAC Servers.Server Roles.OS X Core Services.OS X Core Services - File Sharing - SMB/Windows	Every 2 minutes	~Autofix Action Restart Service	Service Monitors
SVC-SMTPSVC	Checks to see if the 'SMTPSVC' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Messaging Servers.Exchange 2003 Servers	Every 60 Seconds	Default - Create Ticket	Service Monitors
SVC-SPAdminV4	Checks to see if the 'SPAdminV4' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Foundation 2010 Servers Service Plans.Windows Servers. Server Roles. Windows Web/Proxy Servers. SharePoint Server 2007 (MOSS) Server Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Server 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-Spooler	Checks to see if the 'Spooler' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Windows Print Servers Service Plans.Windows Workstations. Managed 24x7 Service Plans.WindowsWorkstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-SPTimerV3	Checks to see if the 'SPTimerV3' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Services WSS v3 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SPTimerV4	Checks to see if the 'SPTimerV4' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Foundation 2010 Servers Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Server 2007 (MOSS) Server Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Server 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SPTrace	Checks to see if the 'SPTrace' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Services WSS v3 Servers Service Plans.WindowsServers. ServerRoles. Windows Web/Proxy Servers. SharePoint Server 2007 (MOSS) Server Service Plans.Windows Servers. Server Roles.WindowsWeb/Proxy Servers. SharePoint Server 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SPTraceV4	Checks to see if the 'SPTraceV4' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Foundation 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SPWriter	Checks to see if the 'SPWriter' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Services WSS v3 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SPWriterV4	Checks to see if the 'SPWriterV4' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers. SharePoint Foundation 2010 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-sshd	Monitors to check if the Secure Shell (SSH) service is running	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux SSH Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-SQLBrowser	Checks to see if the 'SQLBrowser' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2005 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers. MS SQL 2008 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-SQLWriter	Checks to see if the 'SQLWriter' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2005 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 R2 Servers Service Plans.Windows Servers. Server Roles.Windows Database Servers.MS SQL 2008 Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-tomcat6	Monitors to check if the tomcat6 Java Servlet Engine service is running	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux SSH Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-TSGateway	Checks to see if the 'TSGateway' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Remote Access Servers. Terminal Server Gateway	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-vhdsvc	Checks to see if the 'vhdsvc' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Windows HyperV Host	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-vmicheartbeat	Checks to see if the 'vmicheartbeat' service is running and if it isn't, will call the Monitor Restart Service script to attempt tofix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors
SVC-vmickvpexchange	Checks to see if the 'vmickvpexchange' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors

SVC-vmicshutdown	Checks to see if the 'vmicshutdown' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-vmictimesync	Checks to see if the 'vmictimesync' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Managed 24x7 Service Plans.Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-vmicvss	Checks to see if the 'vmicvss' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans. Windows Servers. Managed 24x7 Service Plans. Windows Servers. Managed 8x5	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-vmms	Checks to see if the 'vmms' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles. Windows Servers Core Services. Windows HyperV Host	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-vpn	Monitors to check if the Mac Server VPN service is running	Service Plans.MAC Servers.Server Roles.OS X Core Services.OS X Core Services - VPN	Every 2 minutes	~Autofix Action Restart Service	Service Monitors		
SVC-vsftpd	Monitors to check if the file transfer service (vsftpd) is running	Service Plans.Linux Machines.Server Roles.Linux Server Core Services.Linux FTP-vsftpd Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-W32Time	Checks to see if the 'W32Time' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services. Domain Controllers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-W3SVC	Checks to see if the 'W3SVC' service is running and if it isn't, will call the Monitor Restart Service script to attempt to fix the issue.	Service Plans.Windows Servers. Server Roles.Windows Web/Proxy Servers.Windows IIS Web Servers	Every 60 Seconds	~Autofix Action Restart Service	Service Monitors		
SVC-web	Monitors to check if the Mac Server Web Service is running	Service Plans.MAC Servers.Server Roles.OS X Web Services.OS X Web Services - Web Server	Every 2 minutes	~Autofix Action Restart Service	Service Monitors		

SVC-Wiki	Monitors to check if the Wiki Server is running	Service Plans.MAC Servers.Server Roles.OSX Web Services. OS X Web Services - Wiki Server	Every 2 minutes	~Autofix Action Restart Service	Service Monitors		

System Monitors

Table 6: Remote Monitors—System Monitors

Monitor Name	Description	Groups	Interval	Alert Action	Report Category
EXE - DNS Lookup Test	Tests DNS via nslookup against four known sources to validate that DNS is looking up addresses externally as designed. If not, a ticket is created.	PortManagement. DNS -53 UDP	Every 5 Minutes	Default - Create Ticket	Remote Monitors
EXE - Domain Controller Diagnostic	Analyzes the state of domain controllers in a forest or enterprise and reports any problems to help in troubleshooting. If any problems are reported, the ~Autofix Action DCDIAG script is called in an attempt fix the issue. This script will push down a copy of dcdiag to the server if missing, and re-run dcdiag with verbose output attaching the result to the ticket. See: http://technet.microsoft.com/en-	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every Hour	~Autofix Action DCDIAG	Remote Monitors
EXE - KCC Consistency Check	Tests KCC consistency via kcctest.bat. If a problem is found, the ~Autofix Action KCC script is called in an attempt to fix the issue. This script will push down a copy of Repadmin.exe. Repadmin helps administrators diagnose Active Directory replication problems between domain controllers running Microsoft Windows operating systems. See http://technet.microsoft.com/en-	Service Plans.Windows Servers. Server Roles.Windows Servers Core Services.Domain Controllers	Every 12 Hours	~Autofix Action KCC	Remote Monitors
LT - Perf Monitors Disable	This monitor watches for performance monitors that have been disabled at the computer level and places a noperf file on the computer to ensure that the performance monitoring is disabled. Performance monitors that have been disabled will all report as 'green' regardless of the current state of the monitor.	All Agents	Every 5 Minutes	~ Autofix Action Perf Monitors Disable	Antivirus Checks
LT - Perf Monitors Enable	This monitor removes the noperf file from a computer that has had performance monitors re-enabled by deselecting the Remove Performance Monitors extra data field checkbox.	All Agents	Every 5 Minutes	~ Autofix Action Perf Monitors Enable	Antivirus Checks

Antivirus

Table 7: Internal Monitor Types—Antivirus

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
AV - Disabled	Checks the computer for antivirus from all of the definitions that exist in TAC Agent and that it has been disabled. If these conditions are met, it will only create a ticket if the computer has checked in within the last 15 minutes.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Server Anti- Virus Only Service Plans. Windows Workstations. Managed 24x7 Service Plans. Windows Workstations. Managed 8x5 Service Plans. WindowsWorkstations. Managed HAAS Service Plans.Windows Workstations. Workstation Anti- Virus Only	Daily	Default - Create Ticket	Antivirus Checks
AV – Out of Date	Checks the computer for antivirus software and checks the virus definitions to check if they have been updated within the last 15 days. If they haven't been updated in the last 15 days and the computer has checked inwithin the last 15 minutes, the 'Update Virus Definitions' script is called to update the definitions automatically. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Server Anti- Virus Only Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Workstations. Workstation Anti- Virus Only	Daily	~Autofix Action Resend AV Definitions	Antivirus Checks
AV-Software Missing	Checks the computer for antivirus software based on the virus definitions that exist in TAC Agent and that the computer has checked in within the last 15 minutes. If both conditions are met, a ticket will be created; however, you will not be alerted if antivirus is missing if the role of the computer is defined as a database server, VM Host or mail server.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Server Anti- Virus Only Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Workstations. Workstation Anti- Virus Only	Daily	Default - Create Ticket	Antivirus Checks

Backups

Table 8: Internal Monitor Types—Backups

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
BU - !Job Running > 8 hrs	Checks the backup status and if the job has been running for more than 8 hours, a ticket will be created.	Backup Management.AppAssure Backup Management.Acronis Backup Management.CA Backup	Every Hour	Default - Create Ticket	Backup Checks
BU - Backup Failed to Configure Job	Checks the backup logs and looks for messages in the backup logs indicating that the backup configuration failed to save. If the Backup Manager plugin failed to save the backup configuration in the past 24 hours, a ticket will be created.	Backup Management.AppAssure Backup Management.Acronis Backup Management.CA Backup	Every Hour	Default - Create Ticket	Backup Checks
BU - Backup Job Failed	Checks the backup logs for backups that have failed within the past hour. If any backups have failed within the past hour, the ~Autofix Action Server Backup script will automatically run in an attempt to resolve the issue. Refer to notes in Overview for additional information on Autofix actions.	Backup Management.AppAssure Backup Management.Acronis Backup Management.CA Backup	Every Hour	~Autofix Action Server Backup	Backup Checks
BU – Backup Plugin Failed	Checks the backup logs and if the Backup Manager plugin has failed or is not found, a ticket will be created.	Backup Management.AppAssure Backup Management.Acronis Backup Management.CA Backup	Daily	Default - Create Ticket	Backup Checks
BU – Verify Backup Job Failed	Checks the backup logs for failures. If there is any indication that a backup job failed in the past 24 hours, a ticket will be created.	Backup Management.AppAssure Backup Management.Acronis Backup Management.CA Backup	Daily	Default - Create Ticket	Backup Checks

CIM

Table 9: Internal Monitor Types—CIM

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
CIM – Fan Offline	Monitors for a bad fan and if a bad fan is detected, a ticket is created.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	Default - Create Ticket	Antivirus Checks
CIM – Power Supply Offline	Monitors for a bad power supply and if a bad power supply is detected, a ticket is created.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	Default - Create Ticket	Antivirus Checks
CIM – Temperature Sensor	Monitors for a temperature higher than 90 degrees and will create a ticket.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	Default - Create Ticket	Antivirus Checks

Disk

Table 10: Internal Monitor Types—Disk

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
DRV – Disk Cleanup Servers	Checks the size of the server's temp files and if it's greater than 167772160 bytes (160 MB) and the computer has checked in within the last 15 minutes, the~Autofix Action Temp File Cleanup script will be called to attempt to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	~Autofix Action Temp File Cleanup	Disk Monitors
DRV – Disk Cleanup Workstations	Checks the fragmentation on the drive. If the fragmentation is greater than 30%, it will create a ticket because the ~Autofix Action Defragment Drive that would have run prior to it hitting 30% did not remediate the issue.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket	Disk Monitors
DRV – Fragmentation < 30%	Checks the fragmentation on drive. If the fragmentation on the drive is greater than 16% and less than 30% and the computer has checked in within the last 1400 minutes, the ~Autofix Action Defragment Drive script will be called to attempt to fix the issue. Drives that are excluded: drives that don't exist and are there for history only, USB drives, firewire drives and drives manually tagged as SSD. Additionally, defragmentation is based on software detected so if SP, Acronis, AppAssure, CA, VMHost, VM, MSSQL Server or Exchange is detected these machines will not be defragmented. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	~Autofix Action Defragment Drive	Disk Monitors

DRV – Fragmentation > 30%	Checks the size of the server's temp files and if it's greater than 167772160 bytes (160 MB) and the computer has checked in within the last 15 minutes, the~Autofix Action Temp File Cleanup script will be called to attempt to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	~Autofix Action Temp File Cleanup	Disk Monitors
DRV – Free Space Remaining < 10% Total Size	Checks the disk for available free space. If drive size is greater than 16384 MB (16 GB), available free space is less than 10% of the total drive size and file system is not CDFS, UNKFS, DVDFS, FAT, FAT32 or NetFS, monitor will create aticket.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Servers.Managed 24x7 Service Plans.Linux Machines.Managed 8x5 Service Plans.MAC Workstations.Managed 24x7 Service Plans.MAC Workstations.Managed 8x5 Service Plans.MAC Servers.Managed 24x7 Service Plans.MAC Servers.Managed 8x5	Daily	Default – Create Ticket	Disk Monitors

DRV – Free Space Remaining < 2 GB	Checks the disk for available free space. If drive size is greater than 16384 MB (16 GB), the available free space is less than 2048 (2 GB) and the file system is not CDFS, UNKFS, DVDFS, FAT, FAT32 or NetFS, the monitor will create a ticket.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Managed 24x7 Service Plans.Linux Machines.Managed 8x5 Service Plans.MAC Workstations.Managed 24x7 Service Plans.MAC Workstations.Managed 8x5 Service Plans.MAC Servers.Managed 24x7 Service Plans.MAC Servers.Managed 8x5	Every 6 hours	Default – Create Ticket	Disk Monitors
DRV – MFT Fragmentation	Monitors the MFT fragmentation of a drive (ignores SSD drives). When the fragmentation is greater than 15 percent and the computer has checked in within the last 15 minutes, it will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket Default – Server 24x7	Disk Monitors

DRV – Smart Failures	Smart Failures should not be ignored! Monitors the smart attributes' thresholds and if the value exceeds the threshold (VMs are excluded), then a ticket is created. If there are multiple failures, a single ticket is created per computer.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed 8x5 Service Plans.Windows Workstations. Managed HAAS Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Managed 24x7 Service Plans.Linux Machines.Managed 8x5 Service Plans.MAC Workstations.Managed 24x7 Service Plans.MAC Workstations.Managed 8x5 Service Plans.MAC Servers.Managed 24x7 Service Plans.MAC Servers.Managed 8x5	Every 12 hours	Default – Create Ticket	Disk Monitors

Table 11: Internal Monitor Types—ESX

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
ESX – Host CPU Usage	Monitors CPU usage of host and if CPU usage goes above 90%, a ticket is created.	Service Plans.Window Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX – Host Disk Resets	Monitors bus resets of disks on host and creates a ticket, if above 0.	Service Plans.Window Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX – Host Disk Usage	Monitors disk usage of host and creates a ticket if above 80%.	Service Plans.Window Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX – Host Memory Usage	Monitors memory usage of host and creates a ticket if above 90%.	Service Plans.Window Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX – Host Recently Restarted	Monitors the host system uptime and creates a ticket if time is less than 5 minutes.	Service Plans.Window Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX – VM Recently Restarted	Monitors VM system uptime and creates a ticket if time is less than 5 minutes.	Service Plans.Window Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX VM – CPU Usage	Monitors CPU usage of VM and creates a ticket if above 90%.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5	Every 4 hours	Default – Create Ticket	Antivirus Checks

ESX VM – Disk Usage	Monitors disk usage of VM and creates a ticket if above 80%	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX VM – Memory Ballooned	Monitors number of times memory balloons on the VM and creates a ticket if above 0.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks
ESX VM – Memory Usage	Monitors memory usage of VM and creates a ticket if above 90%.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Managed 24x7	Every 4 hours	Default – Create Ticket	Antivirus Checks

Events

Table 12: Internal Monitor Types—Events

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
EV – Blacklisted Events – Exchange Server	Monitors the blacklisted events for errors on the Exchange server only. If blacklisted events occur, the Monitor Exchange server script will be called, which creates a ticket and adds a comment for each Exchange Server Blacklist event detected. Will update a new or opened ticket, if ticket is closed, it will open a new one.	Service Plans.Windows Servers.Managed 24x7	Every hour	~Autofix Action Exchange Server	Exchange Errors
EV – Blacklisted Events – Informational Errors Only	Monitors the blacklisted events for error type 2 (informational only) and excludes Exchange events. Creates a ticket and appends all disk Informational blacklist events as a comment to the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	~Autofix Action Blacklist Events - Informational	Eventlog Checks
EV – Blacklisted Events – Symantec Backup Exec	Monitors the blacklisted events for warnings and errors that need to be addressed for Symantec Backup Exec. Creates a ticket and appends all events as a comment to the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Server Backup Only	Every hour	~Autofix Action Critical Symantec Backup Exec Events	Backup Checks

EV – Blacklisted Events – Symantec Endpoint Protection	Monitors the blacklisted events for warnings and errors that need to be addressed for Symantec Endpoint Protection. Creates a ticket and appends all events as a comment to the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Server Anti-Virus Only Service Plans.Windows Workstations.Managed 24x7	Every hour	~Autofix Action Critical Symantec Endpoint Security Events	Anti-Virus
EV – Blacklisted Events – Symantec Endpoint Protection Licensing	Monitors the blacklisted events for Symantec Endpoint Protection licenses that are about to expire. Creates a ticket and appends all events as a comment to the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Managed 8x5 Service Plans.Windows Servers.Server Anti-Virus Only Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Workstations.	Every hour	Default – Do Nothing	Anti-Virus
EV – Blacklisted Events – Warnings and Errors Only	Monitors the blacklisted events for warnings and errors that need to be addressed. Excludes Exchange events. Creates a ticket and appends all disk blacklist events as a commentto the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS	Every 4 hours	~Autofix Action Blacklist Events – Warnings and Errors	Eventlog Checks
EV – Chassis Intrusion	Monitors the event logs for the event ID of 1254 and the source is 'Server Administrator' with an event type of 1(error). Event ID1254 indicates that a chassis intrusion was detected. If any are detected, a ticket is created.	Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket	Internal Monitors
EV – Drive Errors and Raid Failures	Monitors the event logs for any disk errors. Creates a ticket and appends all raid blacklist events as a comment to the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS	Every hour	~Autofix Action Drive Errors and Raid Failures	Drive Errors
EV – Excessive Alerts Detected > 25 Like Events	Monitors event logs for excessive alerts. If there have been more than 25 alerts and the computer has checked in within the last 6 minutes, it will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS	Daily	Default- Server 24x7	Eventlog Checks

EV – Failed Load User Profile	Monitors the event logs where the LogName field equals 'application' and the event ID is1521. Event ID 1521 indicates that Windows cannot locate the server copy of your roaming profile and is attempting to log you on with your local profile. Changes to the profile will not be copied to the server when you logoff. Possible causes of this error include network problems or insufficient security rights. This event will automatically create a ticket.	Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket	Internal Monitors
EV – Failed Logins*	Monitors the event logs for the event ID 529, 644, 681 with the source of 'security'. Event ID 529 indicates a Logon Failure for unknown user name or bad password. Event ID 644 indicates that the user account has been locked out. Event ID 681 indicates that a log in attempt failed. A decimal error code is included in the event(i.e. 3221225578) that translates to the cause of the failure. Triggers the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Servers.Managed 24x7	Every 12 hours	Default – Server 24x7	Internal Monitors
EV – Folder Redirect Failed	Monitors event logs for failed folder redirects and event log type 1. If computer has checked in within last 15 min, a ticket will be created.	Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket	Internal Monitors
EV – Printer Driving Missing*	Monitors the event logs for the event ID 1111 where the source is 'UmrdpService', the eventtype is 1(error) and thecomputer has checked in within the last 15 minutes. Event 1111 indicates that the driver required for printer is unknown ormissing. Triggers the appropriate Alert	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Workstation 24x7	Internal Monitors
EV – Reoccurring Critical > 75 Occurrences	Monitors the event log for more than 75 reoccurring events and will create a ticket when this occurs.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Create Ticket	Eventlog Checks
E V – TCP Max Connections Reached	Monitors event logs with the event ID 4226 with a source of 'Tcpip' and the event type of 3 (warning/error) and the computer has checked in within the last 15 minutes. The event ID 4226 indicates that TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts. Creates a ticket when this occurs.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Create Ticket	Internal Monitors

Hardware

Table 12: Internal Monitor Types—Hardware

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
HDW – Hardware Changes Detected	Checks for any changes in hardware since yesterday. Any changes are indicated in a ticket.	Service Plans.Windows Servers. Managed. 24x7	Daily	Default – Create Ticket	Internal Monitors

TAC Agent 2.0

Table 13: Internal Monitor Types—TAC Agent 2.0

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
LT-Agent Out Dated	Monitors agent computers for the current service version for Windows, Mac and Linux. If the service version is not current, the script will try to remediate the issue. If it cannot, then the script is to execute the alert template that has been specified in the Properties.	All Agents	Daily	~Autofix Out of Date Agent	Internal Monitors
LT – Agents No Checkin for more than 30 days	Monitors agent computers for the last checkin. If greater than 30 days, will create a ticket.	Service Plans	Daily	Default – Create Ticket	Internal Monitors
LT – TAC Agent monitor disabled	This monitor detects Internal Monitors that have been disabled due to invalid or long running SQL queries.	All Agents	Every Hour	Default – Create Ticket	Internal Monitors
LT – New Computer Detected*	This monitor alerts on new network devices detected by the network probe within the past day that appear to be new computers on the network.	All Agents	Daily	-Autofix Action New Computer Detected	Internal Monitors
LT – New Device Detected*	This monitor alerts on new network devices detected by the network probe within the past day.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.TAC Agent Server	Every 12 hours	Default – Create Ticket	Internal Monitors
LT – New Unassigned Computers*	This monitor detects new computers that have been added to the New Computers location in the past two days that need to be moved to their proper location.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.TAC Agent Server	Daily	Default – Create Ticket	Internal Monitors

LT – Offline Locations*	This monitor detects locations that have no agents checking in.	All Agents	Every 5 minutes	Default – Do Nothing	Internal Monitors	
LT-Offline Master Servers	Monitors servers where the last time the server checked in was greater than 5 minutes ago. If greater than 5 minutes, the autofix action agent offline script will run. The script ensures the agent is actually down or if an entire site is down. If so, the script will try to remediate the issue. If it cannot, then the script executes the alert template that has been specified in the Properties.	Service Plans.Windows Servers. Managed. 24x7	Every 30 seconds	~Autofix Action Server Offline Script	Internal Monitors	
LT-Offline Servers	Monitors servers where the last time the server checked in was greater than 5 minutes ago. If greater than 5 minutes, the autofix action agent offline script will run. The script ensures the agent is actually down or if an entire site is down. If so, the script will try to remediate the issue. If it cannot, then the script executes the alert template that has been specified in the Properties.	Service Plans.Windows Servers. Managed. 24x7 Service Plans.Windows Servers.Managed.8x5	Every 5 minutes	~Autofix Action Server Offline Script	Internal Monitors	
	Monitors servers where the last time the server checked in was greater than 5 minutes ago. If greater than 5 minutes, a ticket is created.	Service Plans.Linux Machines.Managed 24x7 Service Plans.MAC Servers.Managed 24x7 Service Plans.MAC Servers.Managed 8x5	Every 5 minutes	Default – Create Ticket	Internal Monitors	
LT – Onboarding Incomplete – Missing Admin Credential	Detects locations that have been enabled for Onboarding, but do not have a credential selected for 'Login to use for Administrator Access' selected on the location's Deployment and Defaults tab.	All Agents	Every 12 hours	Default – Create Ticket	Internal Monitors	
LT – System MAC Address Changed	This monitor detects agents where the MAC address of the network card has changed. If the MAC address of an agent is changing this is used to detect when two different agent computers checking into the same server agentid.	Service Plans		Default – Create Ticket	Internal Monitors	

Mobile Device Management

Table 14: Internal Monitor Types—MDM

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
MDM – Devices Over Mobile Data	Checks for mobile devices that exceed their specified data plan.	Global monitor – not assigned to specific groups	Every 6 hours	Default – Create Ticket	Internal Monitors
MDM – Mobile Devices Not Checking In	Checks for mobile devices that are being managed through MDM that are not checking in.	Global monitor – not assigned to specific groups	Every 12 hours	Default – Create Ticket	Internal Monitors

No Contract

Table 15: Internal Monitor Types—No Contract

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
NC – AV Disabled	Checks the computer for antivirus from all of the definitions that exist in TAC Agent and that it has been disabled. If these conditions are met, it will only create a 'no contract' ticket if the computer has checked in within the last 15 minutes.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Antivirus Checks
NC – AV Out of Date	Monitors the computer for antivirus software and checks the virus definitions to determine if they have been updated within the last 15 days. If they haven't been updated in the last 15 days and the computer has checked in within the last 15 minutes, a 'no contract' ticket will be created.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Antivirus Checks
NC – AV Software Missing	Checks the computer for antivirus software based on the virus definitions that exist in TAC Agent and that the computer has checked in within the last 15 minutes. If both conditions are met, a 'no contract' ticket will be created; however, there is no alert if antivirus is missing or if the role of the computer is defined as a database server, VM Host or mail server.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Antivirus Checks
NC – Bad Processes Detected	Monitors for blacklisted processes. If a blacklisted process is detected, a 'no contract' ticket is created.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Process Monitors
NC – Drive – Drive Errors and Raid Failures	Monitors the event logs for any disk errors. Creates a 'no contract' ticket and appends all raid blacklist events as a comment to the ticket. Will only update a new or opened ticket, if the ticket is closed it will open a new one.	Service Plans.Windows Servers.No Contract		Default – No Contract Ticket	Drive Errors
NC – Drive – Disk Cleanup Servers	Checks the size of the server'stemp files and if greater than167772160 bytes (160 MB) and the computer has checked in within the last 15 minutes, a 'no contract' ticket will be created.	Service Plans.Windows Workstations.No Contract		Default – No Contract Ticket	Disk Monitors

NC – Disk Cleanup Workstations	Checks the size of the computer's temp files size, if greater than 50331648 bytes (48 MB) and the computer has checked in within the last 15 minutes, a 'no contract' ticket will be created.	Service Plans.Windows Workstations.No Contract		Default – No Contract Ticket	Disk Monitors
NC – Drive – Fragmentation	Checks the fragmentation on drive. If the fragmentation on the drive is greater than 15% and the computer has checked in within the last 1400 minutes, a 'no contract' ticket will be created. Drives that are excluded: drives that don't exist and are there for history only, USB drives, firewire drives and drives manually tagged as SSD.	Service Plans.Windows Workstations.No Contract		Default – No Contract Ticket	Disk Monitors
NC – Drive – Free Space <5% Free	Checks the disk for available free space. If drive size is greater than 4096 MB (4 GB), available free space is less than 5% of the total drive size and file system is not CDFS, UNKFS, DVDFS, FAT, FAT32 or NetFS, monitor will create a 'no contract' ticket.	Service Plans.Windows Workstations.No Contract Service Plans.Windows Servers.No Contract Service Plans.MAC Workstations.No Contract Service Plans.MAC Servers.No Contract		Default – No Contract Ticket	Disk Monitors
NC – Drive – Smart Failures	Smart Failures should not be ignored! Monitors the smart attributes' thresholds and if the value exceeds the threshold (VMs are excluded), then a non-contract ticket is created. If there are multiple failures, a single ticket is created per computer.	Service Plans.Windows Workstations.No Contract Service Plans.Windows Servers.No Contract Service Plans.Linux Machines.No Contract Service Plans.MAC Servers.No Contract	Daily	Default – No Contract Ticket	Drive Errors
NC – TCP – Duplicate IP in Network	Monitors the event logs for a duplicate IP address and that the computer has checked in within the last 1400 minutes. If these conditions are met, a no contract ticket will be created.	Service Plans.Windows Workstations.No Contract	Dail	Default – No Contract Ticket	Internal Monitors
NC – TCP – Suspicious Ports	Monitors for activity on specific ports that might indicate suspicious activity. Ports monitored: 1080, 2283, 2535, 2745, 3127, 3128, 3410, 5554, 8866, 9898, 12345, 17300 and 27374. Creates a 'no contract' ticket if any activity is detected on these ports and the computer has checked in within the last 1400 minutes.	Service Plans.Windows Workstations.No Contract Service Plans.Windows Servers.No Contract Service Plans.MAC Workstations.No Contract Service Plans.MAC Servers.No Contract	Daily	Default – No Contract Ticket	Internal Monitors
NC – Updates – Failed Automatic	Monitors for Windows Updates that have failed and that the computer has checked in within the last 1400 minutes. If these conditions are met, a 'no contract' ticket is created.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Internal Monitors

NC – Updates – Missing Service Pack	Monitors Windows and Macintosh machines for missing service packs. If there are missing service packs, a 'no contract' ticket is created.	Service Plans.Windows Workstations.No Contract Service Plans.Windows Servers.No Contract Service Plans.MAC Workstations.No Contract	Daily	Default – No Contract Ticket	Internal Monitors		
NC – Updates – Out of Date	Monitors Windows and VM machines for out of date updates. If out of date, a 'no contract' ticket is created.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Internal Monitors		
NC – Windows Appinit DLL Defined*	Checks to see if the Appinit DLL is defined on a computer and if so it could indicate that there is a virus infection on that computer or that the computer is a slow performing machine. If defined, a 'no contract' ticket is created.	Service Plans.Windows Servers.No Contract	Daily	Default – No Contract Ticket	Registry Monitors		
NC – Windows Shell Defined	Checks to see if the Windows Shell is being defined at startup on a computer and if so it could indicate that there is a virus infection. If defined, a 'no contract' ticket is created.	Service Plans.Windows Servers.No Contract	Daily	Default – No Contract Ticket	Registry Monitors		
NC – Windows Startup Overloaded	Monitors the number of startup programs. If greater than 15 and contact has been made within the last 8 days, a 'no contract' ticket is created.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Registry Monitors		
NC – Windows Userinit Defined	Checks to see if the Windows userinit is being defined at startup on a computer and if so it could indicate that there is a virus infection because userinit.exe can run logon scripts which could be malicious. If defined, a 'no contract' ticket is created.	Service Plans.Windows Workstations.No Contract	Daily	Default – No Contract Ticket	Registry Monitors		

Performance

Table 16: Internal Monitor Types—Performance

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
PF – Low Memory	Monitors the total memory. If less than 500, it will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Servers.Managed 24x7	Daily	Default – Server 24x7	Perf. Checks
		Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Workstations.Managed 8x5	Daily	Default – Workstation – 24x7	Perf. Checks
PF – 90% Plus Avg CPU	Monitors CPU usage greater than 90 percent and where the computer has checked in within the last 15 minutes.	Service Plans.Windows Servers.Managed 24x7	Daily	Default – Server 24x7	Perf. Checks
		Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Workstation – 24x7	Perf. Checks
		Service Plans.Windows Workstations.Managed 8x5	Daily	Default – Workstation – 8x5	Perf. Checks

Processes

Table 17: Internal Monitor Types—Processes

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
PROC – Bad Processed Detected	Monitors for blacklisted processes. If a blacklisted process is detected, the 'Monitor Kill Bad Process' script is called to kill the bad process.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations. Managed HAAS	Daily	~Autofix Action Kill Bad Process	Process Monitors

Printers

Table 18: Internal Monitor Types—Printers

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
PRT – Printer Low Consumables	Monitors printer consumable levels. If less than 20 percent and where the max capacity is greater than 0, the monitor will trigger the appropriate Alert Template based on the service plan this printer belongs to.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Workstation 24x7 (global default)	Internal Monitors

Passwords

Table 19: Internal Monitor Types—Passwords

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
PWD – Expired Passwords	Monitors the passwords table and checks to see if the expiration date is prior to today's date. If any are expired, a ticket is created.	Service Plans.Windows Workstations.Managed 24x7	Daily	Default – Create Ticket	Expired Items

Registry

Table 20: Internal Monitor Types—Registry

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
REG – Windows Appinit DLL Defined*	Checks to see if the Appinit DLL is defined on a computer and if so it could indicate that there is a virus infection on thatcomputer or that the computer is a slow performing machine. If defined, the 'Monitor Fix Appinit' script will be called to fix the Appinit DLL that is defined in the registry and will delete them.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	~Autofix Action Fix Appinit	Registry Monitors

REG – Windows CMD Autorun Defined	Checks to see if the Windows cmd is defined to auto start on a computer and if so could indicate a virus infection. If defined, the monitor will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Workstation 24x7	Registry Monitors
REG – Windows Shell Defined	Checks to see if the Windows Shell is being defined at startup on a computer and if so it could indicate that there is a virus infection. If defined, the 'Monitor Fix Shell' script will be called to fix the Windows Shell Registry and set it back to Explorer.exe. HKEY_LOCAL_MACHINE\SOF TWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	~Autofix Action Fix Shell	Registry Monitors
REG- Windows Startup Overloaded	Monitors the number of startup programs. If greater than 15 and contact has been made within the last 8 days, the monitor will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS	Daily Daily	Default – Create Ticket Default – Workstation 24x7 Default – Workstation 8x5	Registry Monitors
REG – Windows System Defined*	Checks to see if the Windows System is being defined at startup on a computer and if so it could indicate that is a virus infection. If defined, the 'Monitor Fix System' script will be called and will fix the defined system registry value. HKEY_LOCAL_MACHINE\SOF TWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Sy stem	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	~Autofix Action Fix System	Registry Monitors

REG – Windows Taskman Defined	Checks to see if the Windows Taskman is being defined at startup on a computer and if so it could indicate that there is a virus infection. If defined, the monitor will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Workstation 24x7	Registry Monitors		
REG – Windows Userinit Defined	Checks to see if the Windows userinit is being defined at startup on a computer and if so it could indicate that there is a virus infection because userinit.exe can run logon scripts which could be malicious. If defined, the 'Monitor Fix Userinit' script will be called and attempt to fix the issue.	Service Plans.Windows Workstations.Managed 24x7 ervice Plans.Windows Workstations.Managed HAAS		~Autofix Action Fix Userinit	Service Monitors		

Services

Table 21: Internal Monitor Types—Services

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
SVC – Auto Services Stopped	Checks the computer for auto services that are not running and the computer has checked in within the last 15 minutes and where the services.driver = 0 (to verify that drivers are not loading as services). Provided the service is not blacklisted and the other conditions are met, the 'Monitor Restart Service' script will be called and it will attempt to restart the failed service no more than three times before generating an alert and creating a ticket.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows.Servers.Managed 8x5 Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5	Every hour	~Autofix Action Restart Service	Service Monitors

Software

Table 22: Internal Monitor Types—Software

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
SW – Application Crash	Monitors the event logs for the event ID 1002 and source'Application Hang' with an event type 1(error) where the computer has checked in within the last 1400 minutes. Event ID 1002 indicates hanging application <application exe>, version <version>, hang module hungapp, version 0.0.0.0, hang address <hex address>. If defined, the monitor will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default – Workstation 24x7	Internal Monitors
		Service Plans.Windows Workstations.Managed 8x5	Daily	Default – Workstation 8x5	
		Service Plans.Windows Servers.Managed 24x7	Daily	Default Server – 24x7	
SW – Blacklisted Install	Monitors the software table to check if the selected software that appears on the Application Blacklist has been installed and if the computer has checked in within the last 1400 minutes. If these conditions are met, a ticket is created.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Every 12 hours	Default – Create Ticket	Internal Monitors
SW – Expired ProductKeys*	Monitors the product keys and checks the expiration date. If the expiration date is less than 43200 minutes from now and the day of week is not Sunday or Saturday, the monitor will create a ticket.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket	Expired Items
SW – Installed New*	Monitors new installations and determines if the application was installed within the last day, if the computer has been addedover two days ago and theapplication is not a patch. Many common apps excluded from alerting: java, Mozilla, Skype, Flash Player, Chrome, Adobe Reader, Apple application, CutePDF, Shockwave, QuickTime and iTunes. Additional software can be added to exclude. Information provided by this monitor may not be useful today but may be useful later for troubleshooting purposes.	Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5	Daily	~Autofix Action SW Installed Default – Workstation 24x7	Internal Monitors

SW – Over Licenses*	Determines if the license count is greater than the allocated license count. If license count is greater, a ticket will be created.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Every 12 hours	Default – Create Ticket	Internal Monitors
SW – Unclassified Apps	Monitors the software table for the selected software that appears on the Application whitelist. If application appears on the whitelist, the 'Monitor Unclassified Apps' script will be called to attempt to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Managed 8x5		~Autofix Action Unclassified Apps	Internal Monitors
SW – Uninstalled*	Checks for software that has been uninstalled within the last day. The monitor will trigger the appropriate Alert Template based on the service plan this computer belongs to. If computer belongs to a managed group with the ~Autofix Action as the Alert Template, the 'Monitor SW Uninstall' script is called and will attempt to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5		Default – Workstation 24x7	Internal Monitors
		Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7		~Autofix Action SW Uninstalled	

TCP

Table 23: Internal Monitor Types—TCP

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
TCP – Suspicious Ports	Monitors for activity on specific ports that might indicate suspicious activity. Ports monitored: 1080, 2283, 2535, 2745, 3127, 3128, 3410, 5554, 8866, 9898, 12345, 17300 and 27374. Monitor will trigger the appropriate Alert Template based on the service plan this computer belongs to.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7		Default – Create Ticket	Network Checks
		Service Plans.Windows Workstations.Managed 8x5		Default – Workstation 8x5	

Updates

Table 24: Internal Monitor Types—Updates

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
UPDATES – Daytime Patch Reboot Pending	This monitor detects Windows workstation agents that are online and have a pending reboot due to applied Windows Updates. The machine must be under patch contract.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS	Every hour	Default – Do Nothing	Internal Monitors
		_System Automation.Windows Updates Patch Window Control.Win Workstations.Windows Updates – Everyday Daytime Patch Override	Every hour	~Autofix Prompt User Reboot	Internal Monitors
UPDATES – Empty Patch Window	Checks computer for Windows OS, patch window is empty and computer has checked in within the past day. This indicates that Windows update is messed up or installer is out of date. Calls the 'Monitor Empty Patch Window' script and will attempt to fix the issue.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Servers.Managed 24x7 Service Plans.Windows Servers.Managed 8x5	Every four hours	~Autofix Empty Patch Window	Internal Monitors

UPDATES – Failed	Checks computer for updates that were pushed and failed and where the computer has checked in within the past day. If conditions are met, calls the 'Monitor Missing Critical Patches' script which will attempt to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	~Autofix Action Missing Critical Patches	Antivirus Checks
UPDATES – Failed Automatic Updates	Checks event logs for failed automatic updates and where computer has checked in within the last 1400 minutes. If these conditions are met, the 'Monitor Failed Patch Installs' script is called which will attempt to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	~Autofix Action Failed Patch Installs	Internal Monitors
UPDATES - Installed	Checks for patches installed within the last day.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	Default – Do Nothing	Updates Installed
UPDATES – Missing Service Pack	Monitors Windows and Macintosh machines for missing service packs. If there are missing service packs, a ticket is created.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7 Service Plans.MAC Workstations.Managed 24x7	Daily	Default - Create Ticket	Internal Monitors
UPDATES – New Unapproved*	Monitors new patches that have been detected within the past 24 hours.	Service Plans.Windows Servers.Server Roles.MSP Specific Servers.TAC Agent Server	Daily	~Autofix Action New Unapproved Patches	Internal Monitors
UPDATES – Out of Date	Checks for Windows updates that haven't run in the last 30 days. If there are updates that have not run in the past 30 days, a ticket is created.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5 Service Plans.Windows Workstations.Managed HAAS Service Plans.Windows Servers.Managed 24x7	Daily	Default – Create Ticket	Internal Monitors

UPDATES – Reboot Pending	Checks if patching requires a reboot and if computer is not a server and has checked in within the last 15 minutes will call the 'Monitor Prompt User Reboot' script which will prompt the user to restart the computer and if the user says no then it will reschedule itself for 60 mins later. This script will continuously ask the user to restart until the computer restarts and the flag is reset.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed 8x5	Every six hours	~Autofix Prompt User Reboot	Internal Monitors

Uptime

Table 25: Internal Monitor Types—Uptime

Monitor Name	Description	Groups	Interval	Alert Template	Report Category
UPTIME - Over 1 Month Without Reboot*	Checks computer's uptime to see if computer has not been rebooted in over a month and if it hasn't, creates a ticket.	Service Plans.Windows Workstations.Managed 24x7 Service Plans.Windows Workstations.Managed HAAS	Daily	Default - Create Ticket	Internal Monitors
UPTIME - SVR 1 Mo. Since Reboot*	Checks servers' uptime to see if server has not been rebooted in over a month and if it hasn't creates a ticket.	Service Plans.Windows Servers.Managed 24x7	Daily	Default - Create Ticket	Internal Monitors
UPTIME - WKS 2 Weeks Since Reboot*	Checks computer's uptime to see if computer has not been rebooted in two weeks. If it has not, the 'Monitor Reboot Computer' script will be called to fix the issue. Refer to notes in Overview for additional information on Autofix actions.	Service Plans.Windows Workstations. Managed 24x7 Service Plans.Windows Workstations. Managed HAAS	Daily	~Autofix Action Reboot Computer	Internal Monitors