The RMM Suite
Operations & Customization Guide

Monitoring

MSP Builder, LLC
Version 3.0 / Release 22-175
Glenn Barnas

Last Updated: 2024/12/03

MSP Builder RMM Suite

The MSP Builder RMM Suite contains proprietary software, including unpublished source code. All software is (and remains) the property of MSP Builder LLC and no transfer of ownership is granted or implied.

The MSP Builder RMM Suite software is designed to audit, monitor and manage computers that use a number of RMM platforms. It is not designed or configured to collect personally identifiable information and should not be configured to do so without the consent of the individual or to be used in any unlawful manner, or in a manner that requires the consent of an individual.

MSP Builder LLC ("COMPANY") CONFIDENTIAL

NOTICE: All information contained herein is and remains the property of COMPANY. The intellectual and technical concepts contained herein are proprietary to COMPANY and may be covered by U.S. and Foreign Patents, patents in process, and are protected by trade secret or copyright law.

Dissemination of this information or reproduction of this material is strictly forbidden unless prior written permission is obtained from COMPANY. Access to the source code contained herein is hereby forbidden to anyone except current COMPANY employees, managers or contractors who have executed Confidentiality and Non-disclosure agreements explicitly covering such access.

The copyright notice above does not evidence any actual or intended publication or disclosure of this source code, which includes information that is confidential and/or proprietary, and is a trade secret, of COMPANY. ANY REPRODUCTION, MODIFICATION, DISTRIBUTION, PUBLIC PERFORMANCE, OR PUBLIC DISPLAY OF OR THROUGH USE OF THIS SOURCE CODE WITHOUT THE EXPRESS WRITTEN CONSENT OF COMPANY IS STRICTLY PROHIBITED, AND IN VIOLATION OF APPLICABLE LAWS AND INTERNATIONAL TREATIES. THE RECEIPT OR POSSESSION OF THIS SOURCE CODE AND/OR RELATED INFORMATION DOES NOT CONVEY OR IMPLY ANY RIGHTS TO REPRODUCE, DISCLOSE OR DISTRIBUTE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE, IN WHOLE OR IN PART.

MSP BUILDER

MSP Builder LLC
385 Falmouth Ave
Elmwood Park, NJ 07407
201-300-8277

Contents

Introduction

The MSP Builder RMM Suite includes a highly optimized set of monitors. Some of these may be specific to the platform where the RMM Suite is used and can vary slightly between platforms. This document will detail the common settings and monitor sets that the RMM Suite provides.

Before we delve into the monitor sets, it is important to distinguish between three types of monitors that the RMM Suite provides.

1. **Cloud Monitors**
   These are endpoint monitors that are deployed directly through the RMM Suite software and consist of Windows Event Log and Windows Service monitors. These monitor alarm and status events as well as system services. These can utilize Direct-Remediation technology to rapidly respond to alerts with remediation actions.
2. **Smart Monitors**
   Smart Monitors are unique to the RMM Suite. These are applications that replace some of the traditional RMM Platform monitors. By using an application, the Smart Monitor can automatically adjust thresholds based on the environment, suppress or delay non-critical alarms, and attempt to automatically resolve many conditions. Smart Monitors are discussed in detail in a separate Operations Guide and will not be covered here.
3. **RMM Platform Monitors**
   These are endpoint monitors that are deployed through and processed by the RMM Platform directly. These primarily consist of Windows Event Log monitors and Windows Service Monitors. These can monitor alarm and status events as well as system services and are often used for custom monitoring.

Both Cloud and RMM Platform monitors generally do not utilize thresholds for monitoring, but instead depend on detecting when a service has stopped *running* or specific events have been logged. Both types represent nearly 400 distinct monitoring items, utilize the same detection, auto-deployment, and control methods. The key benefits of Cloud Monitors are:

- Automatic maintenance - as MSP Builder creates new or enhanced monitoring sets, they are available to all customers and endpoints within 5 minutes of release.
- Cloud Monitors support Direct Remediation capability - select monitors have RMM-Suite supplied remediation functionality that is triggered immediately upon detection of the alarm event. There are no delays caused by reporting the alarm event first to the RMM, then to ITP, and using ITP to trigger the remediation action. ITP can still provide additional, customized remediation actions to augment the standard RMM Suite actions.
- Unlike RMM Platform monitors that expect a monitored service to be enabled and running, the RMM Suite monitor service will not monitor services in a disabled state, preventing unwanted alarms while modifying or decommissioning a server role.
- Not dependent on the RMM platform or agent to function. This allows uninterrupted monitoring during RMM platform updates, outages, or even migrations to same or different RMM products.

Cloud Monitors are the preferred monitoring method, with RMM Platform monitors being generally reserved for custom, LOB application monitoring. The RMM Suite can easily consolidate alarms from the MSPB cloud and one or more RMM platforms using ITP. Note that some RMM platforms supported by the RMM Suite will only utilize Cloud Monitors for the core monitoring.

There are two key parts to the RMM Suite's monitoring:

Standardized Subject Lines
An RMM Suite alarm subject contains 6 parts delimited with vertical bars as shown here:

```
Name | Type | Data 1 | Data 2 | Data 3 | MonSetID
```

Spaces have been added for clarity but are not present in an actual alarm subject.

Name The unique name of the monitor.

Type The alarm type - usually Alarm or Warning.

Data 1-3 Up to 3 optional values to qualify/quantify the alarm condition.

MonSetID The Monitor Set ID, described below.

Monitor Set ID
The Monitor Set ID allows ITP to quickly determine information about the alarm. This is usually the name or identity of the Monitor Set defined in the RMM Platform. A *monitor set* can consist of one or more specific monitors but will always contain the same *type* of monitor. For example, a service monitor set might contain the names of 3 distinct services and an Event monitor might contain as many as a dozen individual Event IDs, but Service monitor sets will never contain Event monitors and vice-versa. A monitor set looks like this:/

```
Name . Category . P-Type . Priority . Action
```

Again, spaces have been added for clarity.

Name The unique name of the Monitor Set ID. When used for Event Logs, it may also include a code to identify a specific event log being monitored.

Category A 3-4 character code to categorize similar alarms.

P-Type The Platform Type identifier, such as "W" for workstations, "S" for servers, or "X" for a generic monitor.

Priority The initial priority associated with the monitor set. This is the letter "P" followed by a digit in the range of 1-5. Our classifications are Critical (1), High (2), Medium (3), Low (4), Informational (5).

Action A code that tells the Intelligent Ticket Processing system how to respond to the alarm. ITP no longer requires an Action ID to map remediation actions, but this can help distinguish Actionable (ACT) monitors from basic Alarm (ALM) monitors.

Non-Standard / Custom Monitoring

Non-Standard alarms usually result from email-based notifications from non-agent devices that are sent to the RMM platform. The RMM Suite can dynamically translate these alarms by locating key words or phrases in the subject line and either rewrite the subject in an RMM Suite format or invoke a code module that can analyze the subject and body content to create an alarm that can be fully processed.

The RMM Suite also fully supports custom monitoring developed by the MSP/IT department. The alarm must follow the subject format outlined earlier.

The RMM Platform must be able to receive email alert notices for ITP to process them.

How Monitors Are Applied

While the process of deploying monitors will vary slightly between RMM platforms, the general method is described here.

Monitor Packages

A Monitor Package will consist of one or more Monitor Sets related to a specific Role, Feature, Service, or Application. This package can contain a combination of service and log monitors, and each may represent multiple alarm priorities. For RMM Platform monitors, the RMM Suite uses the RMM platform's automation components to deploy the entire contents of a Monitor Package with the related component is detected as installed. This detection defines an identification "TAG" that is stored in the System Roles custom field.

Monitor Packages can be disabled on a per-endpoint basis by defining a corresponding TAG in the Policy Control custom field. This tag can be specific to turn off a specific package (eg: DHCP) or generic to disable all enhanced monitoring (eg: EXMON). Cloud monitors use the same TAG data to enable or disable the monitor packages.

Monitor Sets

A Monitor Set is a specific combination of monitoring parameters at a specific priority. For example, the RMM Suite DHCP Server Monitor Package consists of three Monitor Sets:

- A *service* monitor that checks the DHCP Server Service running state
- An *Event Log* monitor that checks for one critical event
- An *Event Log* monitor that checks for eighteen non-critical events

Controlling Monitors and Alerting

Control is available at the Monitor Package level. It is not possible to disable monitors at the Monitor Set level or specific services or Event Log IDs within a Monitor Set. If this were possible the DHCP example above would require twenty separate RMM Automation Sets (Filter + Policy) to manage twenty separate monitor sets! You can, however, *suppress* individual service or event ID alarms via ITP. This is discussed in the ITP Operations Guide.

A common situation that arises is the need to disable a system Role or Feature. When a role is retired (again, using DHCP as an example), the service cannot simply be set to disabled. The RMM Suite Daily Audit will detect that the DHCP Role is installed and apply the Monitor Package. The RMM platform – when told to monitor a service – will generally report a failure if the service is not running, even if the service is disabled.

Disabling a service does not decommission the role for monitoring! To properly decommission a server role, the Role (or Feature) must be removed from the platform using the Role Administration module. After the Role is removed, the next cycle of RMM Suite Daily Tasks will remove the corresponding role Tag from the agent's System Roles field, and the Monitor Package will no longer be applied.

If a role is to be temporarily suspended, then the Policy Control tag can be set to stop applying the Monitor Package, but this should not be considered a permanent "solution".

Suspending Monitoring

Monitoring may need to be suspended for periods of time. Each monitor type may require specific actions:

1. Cloud Monitoring - run `RSRUN RMEMAS --CW:<minutes>`
   Suspends Service, Event Log, and SAM monitors.
2. Smart Monitors - Apply the SMON policy control to suspend all Smart Monitors. Consult the Smart Monitor Operations Guide for additional information related to suspending individual Smart Monitors.
3. RMM Platform Monitors - use the method specific to the RMM platform.

Alarm Processing

The RMM Suite includes a Windows Service that performs alarm processing and provides the integration between the monitoring platforms and the PSA. This service is called Intelligent Ticket Processing, or "ITP" for short. The ITP service is installed on a computer in the RMM Suite customer's environment, and it is essential that this service remain running to process the alarms and deliver tickets to the PSA.

ITP will check in regularly to the MSPB Cloud Service, and then one or more RMM platforms to determine if any new alarm events are present. When a new alarm is detected, the alarm data is collected, the alarm event is Closed, and the data is passed to an ITP Processing Thread. This component evaluates the alarm, initiates any RMM-based automation response, and ultimately delivers the ticket into the PSA. By using ITP to process alarm events from all monitoring platforms, a consistent interface is used to deliver alarm data from all platforms into the PSA.

Custom monitors should be defined in ITP so that they can be properly evaluated and classified. MSP Builder provides an Excel spreadsheet that defines all of our standard alarms. This allows our default classifications to be customized as well as custom alarms to be handled properly. The spreadsheet creates the entire subject rewrite section used in the configuration file.

ITP operation and configuration is described in detail in the **RMM_Suite_Operations_Guide_-_08_-_Configuration_Management** document.

Standard Monitor Sets

There are two common types of monitors provided by the RMM Suite - Windows Event Log and Windows Service monitors. All alerts generated by RMM Suite tools create Windows Event Log events and will not be treated separately in this document.

A **Monitor Set** is a collection of related monitors that are applied to a computer as a single unit.

Windows Service Monitor Sets

The following Windows Service Monitor Sets are included with the RMM Suite and are deployed automatically when the services or roles are detected. Note that in some cases, the detection is Windows Role based and the monitors will be applied even if the services have been disabled. This is not a proper way to decommission a role - the role should be removed from the server to prevent the monitor set from being deployed.

These monitors and IDs are the same for both Cloud and RMM Platform monitors.

ADDC.SVC.S.P1.Act: Services Monitor Set for AD Domain Controller Services

IsmServ
kdc
W32Time

Altigen.SVC.S.P3.Act:
Altigen Phone Server Services

AGJServ
AltiBack
AltiCTProxy
AltiExchIntg
AltiFTPUploader
AltiGateway
AltiGen External Features Server
AltiGen TAPI Proxy Server
AltiKeep
AltiLogger
AltiMA
AltiPhoneServ
AltiPop3
AltiServ
AltiSmtp
AltiVMServ
AUService
GphoneService
OpenLDAP-slapd
postman

Azure.SVC.S.P3.Act: Services Monitor Set for Azure Services

ADSync
AzureADConnectHealthSyncInsights
AzureADConnectHealthSyncMonitor
AzureNetworkWatcherAgent
frxsvc

frxccds
RdAgent
RDAgentBootLoader
WindowsAzureGuestAgent
WindowsAzureNetAgentSvc

Core-ND.SVC.S.P2.Act:
Services Monitor Set for Common Server Services - Non-Domain Members

Spooler
BFE
CryptSvc
DcomLaunch
Dhcp
Dnscache
Eventlog
EventSystem
iphlpsvc
LmHosts
MpsSvc
netprofm
NlaSvc
PlugPlay
ProfSvc
RpcEptMapper
RpcSs
SamSs
Schedule
SENS
SessionEnv
TermService
TrkWks
UmRdpService
W32Time
winmgmt
ClusSvc

Core-ND.SVC.W.P3.Act: Services Monitor Set for common Workstation services - NON-DOMAIN

Spooler
AudioEndpointBuilder
Audiosrv
BFE
CryptSvc
DcomLaunch
Dhcp
DPS
Eventlog
EventSystem
iphlpsvc
lanmanserver
lanmanworkstation
LmHosts
MpsSvc
netprofm
NlaSvc
PcaSvc
PlugPlay
Power
ProfSvc
RpcEptMapper
RpcSs
SamSs
Schedule
SENS
SessionEnv
TermService
TrkWks
UmRdpService
W32Time
winmgmt

Core.SVC.S.P2.Act: Services Monitor Set for Common Server Services

Spooler
BFE
CryptSvc
DcomLaunch
Dhcp
Dnscache
Eventlog
EventSystem
iphlpsvc
lanmanserver
lanmanworkstation
LmHosts
Netlogon

MpsSvc
netprofm
NlaSvc
PlugPlay
ProfSvc
RpcEptMapper
RpcSs
SamSs
Schedule
SENS
SessionEnv
TermService
TrkWks
UmRdpService
W32Time
winmgmt
Kaseya Network Monitor Gateway
ClusSvc

Core.SVC.W.P3.Act: Services Monitor Set for Common Workstation Services

Note that since Windows 10, Windows performs regular maintenance during the day and will stop/start services. The RMM Suite no longer automatically monitors these services on workstation-class systems.

Spooler
AudioEndpointBuilder
Audiosrv
BFE
CryptSvc
DcomLaunch
Dhcp
DPS
Eventlog
EventSystem
iphlpsvc
lanmanserver
lanmanworkstation
Netlogon
MpsSvc
netprofm
NlaSvc
PcaSvc
PlugPlay
Power
ProfSvc
RpcEptMapper
RpcSs
SamSs
Schedule
SENS
SessionEnv

TermService
TrkWks
UmRdpService
W32Time
winmgmt

DHCPSvr.SVC.S.P1.Act: Services Monitor Set for DHCP Server

DHCPServer

DNS.SVC.S.P1.Act: DNS Server Service Monitor

DNS

Exchange.SVC.S.P1.Act:
Services Monitor Set for Exchange Server Services
MSExchangeADTopology
MSExchangeAntispamUpdate
MSExchangeEdgeSync
MSExchangeIS
MSExchangeMailboxAssistants
MSExchangeMonitoring
MSExchangeMTA
MSExchangePop3
MSExchangeImap4
MSExchangeRepl
MSExchangeTransport
MSExchangeTransportLogSearch
MSExchangeServiceHost
MSExchangeFBA
MSExchangeMailboxReplication
MSExchangeProtectedServiceHost
MSExchangeRPC
MSExchangeSubmission
MSExchangeSA
ADAM_MSExchange
EdgeCredentialSvc
IMAP4Svc
Pop3Svc
SMTPSVC

FileSvr.SVC.S.P2.Act: File Services including DFS, FRS

Dfs
DFSR

GFI.SVC.S.P1.Act: Service Set for GFI Archiver

MARCore
MarIMAP
MARMAIS

MARSearch
MARStore
MARVSS

HMail.SVC.S.P3.Act:
Services Monitor Set for HMail Server

hMailServer

IIS.SVC.S.P1.Act:
Services Monitor Set for IIS Web/FTP server

AppHostSvc
FTPSVC
IISADMIN
MSFtpsvc
w3svc
WAS
WMSVC

PSV.SVC.S.P3.Act:
Services Monitor Set for the Print Spooler services

Spooler

RDSCB.SVC.S.P1.Act:
Services Monitor Set for RDS Connection Broker Services

TScPubRPC
Tssdis

RDSGW.SVC.S.P2.ACT:
Monitor the RDS Gateway service

TSGateway

RDSLS.SVC.S.P1.Act:
Services Monitor Set for RDS Licensing

TermServLicensing

ShadowProt.SVC.S.P3.Act:
Shadow Protect backup services monitor

ShadowProtectSvc
ShadowControl ImageManager

SharePoint.SVC.S.P1.Act:
Sharepoint Server Services

SPAdmin
SPTimer
SPTrace
MSSEARCH

SMTP.SVC.S.P2.Act:
Monitors for SMTP Service in IIS

SMTPSVC

SQL.SVC.S.P1.Act: SQL Server Core Services

MSSQLSERVER
SQLSERVERAGENT
ReportServer
MySql

Hyper-V.SVC.S.P3.Act: Service Monitor Set for Hyper-V Services

Vmms

Windows Event Log Monitor Sets

The following Event Log Monitors are included in the RMM Suite. Whenever possible/appropriate, the monitor must match the Event Source, Event ID, and Description. The Description may be a wildcard (*) when no other combination of Event Source and Event ID are generated by the application or operating system.

MB-ADDC-S.EVT.S.P3.Alm

Security-Kerberos	EvtID: 9	Desc: *

MB-ADDC.EVT.S.P2.Alm

ActiveDirectory_DomainService	EvtID: 1150	Desc: *
ActiveDirectory_DomainService	EvtID: 1311	Desc: *

MB-ADDC.EVT.S.P3.Alm

ActiveDirectory_DomainService	EvtID: 1008	Desc: *
ActiveDirectory_DomainService	EvtID: 1016	Desc: *
ActiveDirectory_DomainService	EvtID: 1084	Desc: *
ActiveDirectory_DomainService	EvtID: 1126	Desc: *
ActiveDirectory_DomainService	EvtID: 1136	Desc: *
ActiveDirectory_DomainService	EvtID: 1312	Desc: *
ActiveDirectory_DomainService	EvtID: 1411	Desc: *
ActiveDirectory_DomainService	EvtID: 1473	Desc: *
ActiveDirectory_DomainService	EvtID: 1546	Desc: *
ActiveDirectory_DomainService	EvtID: 1567	Desc: *
ActiveDirectory_DomainService	EvtID: 1844	Desc: *
ActiveDirectory_DomainService	EvtID: 1865	Desc: *
ActiveDirectory_DomainService	EvtID: 1925	Desc: *
ActiveDirectory_DomainService	EvtID: 1964	Desc: *
ActiveDirectory_DomainService	EvtID: 1977	Desc: *
ActiveDirectory_DomainService	EvtID: 2042	Desc: *
ActiveDirectory_DomainService	EvtID: 2087	Desc: *
ActiveDirectory_DomainService	EvtID: 2088	Desc: *

MB-ADLK-C.EVT.S.P3.Alm

Security-Auditing	EvtID: 4740	Desc: *

MB-AINS-A.EVT.S.P2.Alm

KaseyaAlertCaller	EvtID: 100	Desc: *Failed Checking Queued Calls*
KaseyaAlertCaller	EvtID: 100	Desc: *Failed Checking Instant Calls*
KaseyaAlertCaller	EvtID: 100	Desc: *calling credits remain*
KaseyaAlertCaller	EvtID: 120	Desc: *Call Response Exception*

MB-AppChange-A.EVT.X.P3.Alm

RMM-AUDIT	EvtID: 211	Desc: * RMASDU: Software ADDED -*
RMM-AUDIT	EvtID: 212	Desc: * RMASDU: Software REMOVED -*
RMM-AUDIT	EvtID: 213	Desc: * RMASDU: Software CHANGED -*

MB-ASM-A.EVT.S.P3.Alm

RMM-ASMonitor	EvtID: 101	Desc: *AutoStart Monitor: No config file - ABORT!*
RMM-ASMonitor	EvtID: 102	Desc: *AutoStart Monitor: No/wrong user logged in.*
RMM-ASMonitor	EvtID: 105	Desc: *AutoStart Monitor: Multiple start failures*

MB-CORE-S.EVT.S.P3.Alm

Application Popup	EvtID: 333	Desc: *An I/O operation initiated by the Registry failed unrecoverably.*
VolSnap	EvtID: 8	Desc: *timed out while waiting for a release writes command*
Srv	EvtID: 2020	Desc: *unable to allocate from the system paged pool*

MB-CORE.EVT.S.P2.Alm

Microsoft-Windows-TaskScheduler	EvtID: 401	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 412	Desc: *
Server	EvtID: 2001	Desc: *
Server	EvtID: 2505	Desc: *
Microsoft-Windows-Wininit	EvtID: 3002	Desc: *

MB-CORE.EVT.S.P3.Alm

Microsoft-Windows-GroupPolicy	EvtID: 1002	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1125	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1127	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1126	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1130	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1096	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 311	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 403	Desc: *
Microsoft-Windows-Wininit	EvtID: 1015	Desc: *

Microsoft-Windows-Winlogon	EvtID: 4102	Desc: *
Microsoft-Windows-Winlogon	EvtID: 4103	Desc: *
Resource-Exhaustion-Detector	EvtID: 2004	Desc: *
Server Agents	EvtID: 1123	Desc: *Post Errors were detected*
Service Control Manager	EvtID: 7003	Desc: *
Service Control Manager	EvtID: 7016	Desc: *
Service Control Manager	EvtID: 7022	Desc: *
Service Control Manager	EvtID: 7023	Desc: *
Service Control Manager	EvtID: 7024	Desc: *
Service Control Manager	EvtID: 7033	Desc: *
Service Control Manager	EvtID: 7034	Desc: *
Service Control Manager	EvtID: 7038	Desc: *
Service Control Manager	EvtID: 7041	Desc: *

MB-CORE.EVT.W.P3.Alm

Microsoft-Windows-GroupPolicy	EvtID: 1002	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1125	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1127	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1126	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1130	Desc: *
Microsoft-Windows-GroupPolicy	EvtID: 1096	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 311	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 401	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 403	Desc: *
Microsoft-Windows-TaskScheduler	EvtID: 412	Desc: *
Server	EvtID: 2001	Desc: *
Server	EvtID: 2505	Desc: *
Service Control Manager	EvtID: 7016	Desc: *
Service Control Manager	EvtID: 7022	Desc: *
Service Control Manager	EvtID: 7023	Desc: *
Service Control Manager	EvtID: 7024	Desc: *
Service Control Manager	EvtID: 7033	Desc: *
Service Control Manager	EvtID: 7034	Desc: *
Service Control Manager	EvtID: 7038	Desc: *
Service Control Manager	EvtID: 7041	Desc: *
ntfs	EvtID: 55	Desc: *

MB-CRSH-S.EVT.S.P3.Alm

Kernel-Power	EvtID: 41	Desc: *
Microsoft-Windows-Kernel-Power	EvtID: 41	Desc: *

MB-DHCP-S.EVT.S.P2.Alm

DHCP-Server	EvtID: 1008	Desc: *

MB-DHCP-S.EVT.S.P3.Alm

DHCP-Server	EvtID: 1020	Desc: *
DHCP-Server	EvtID: 1034	Desc: *

DHCP-Server	EvtID: 1045	Desc: *
DHCP-Server	EvtID: 1046	Desc: *
DHCP-Server	EvtID: 1050	Desc: *
DHCP-Server	EvtID: 1058	Desc: *
DHCP-Server	EvtID: 1059	Desc: *
DHCP-Server	EvtID: 1063	Desc: *
DHCP-Server	EvtID: 1102	Desc: *
DHCP-Server	EvtID: 1104	Desc: *
DHCP-Server	EvtID: 1144	Desc: *
DHCP-Server	EvtID: 1001	Desc: *
DHCP-Server	EvtID: 1002	Desc: *
DHCP-Server	EvtID: 1003	Desc: *
DHCP-Server	EvtID: 1004	Desc: *
DHCP-Server	EvtID: 1005	Desc: *
DHCP-Server	EvtID: 1006	Desc: *
DHCP-Server	EvtID: 1007	Desc: *

MB-DNS.EVT.S.P2.Alm

DNS-Server-Service	EvtID: 10	Desc: *
DNS-Server-Service	EvtID: 111	Desc: *

MB-DNS.EVT.S.P3.Alm

DNS-Server-Service	EvtID: 140	Desc: *
DNS-Server-Service	EvtID: 500	Desc: *
DNS-Server-Service	EvtID: 505	Desc: *
DNS-Server-Service	EvtID: 707	Desc: *
DNS-Server-Service	EvtID: 1003	Desc: *
DNS-Server-Service	EvtID: 1501	Desc: *
DNS-Server-Service	EvtID: 3151	Desc: *
DNS-Server-Service	EvtID: 7502	Desc: *

MB-EXC-CERT.EVT.S.P3.Alm

MSExchange Web Services	EvtID: 24	Desc: *
MSExchangeTransport	EvtID: 12015	Desc: *
MSExchangeTransport	EvtID: 12017	Desc: *

MB-EXC.EVT.S.P2.Alm

MSExchangeTransport	EvtID: 15006	Desc: *
MSExchangeTransport	EvtID: 15007	Desc: *
ESE	EvtID: 445	Desc: *Information Store * The database * has reached its maximum size*
MSExchangeIS	EvtID: 1112	Desc: *The database * has reached the maximum allowed size*
MSExchangeIS	EvtID: 9689	Desc: *This database size has exceeded the size limit * will be dismounted the next

		time a database size check is performed*
MSExchangeIS	EvtID: 9690	Desc: *database size has exceeded the size limit * This database will be dismounted immediately*
MSExchangeIS	EvtID: 1003	Desc: *The disk is full. Attempting to stop the Microsoft Exchange Information Store service.*
MSExchangeIS	EvtID: 9518	Desc: *Error Current log file missing starting Storage Group*
MSExchangeIS	EvtID: 1111	Desc: *An error occurred while writing to the database log file*
MSExchangeIS	EvtID: 1113	Desc: *The log disk is full. Attempting to stop the Microsoft Exchange Information Store service*
MSExchangeIS	EvtID: 9518	Desc: *Error 0x89a starting Storage Group *
MSExchangeIS	EvtID: 9519	Desc: *Error 0x89a starting database *
MSExchangeDSAccess	EvtID: 2067	Desc: *Active Directory error occurred*
MSExchangeDSAccess	EvtID: 2102	Desc: *All Domain Controller Servers in use are not responding*
MSExchangeDSAccess	EvtID: 2103	Desc: *All Global Catalog Servers in use are not responding*
MSExchangeDSAccess	EvtID: 2104	Desc: *All the DS Servers in domain are not responding*
MSExchangeDSAccess	EvtID: 2142	Desc: *The LDAP server is unavailable*
MSExchangeDSAccess	EvtID: 4027	Desc: *The LDAP server is unavailable*

MB-EXC.EVT.S.P3.Alm

MSExchange ActiveSync	EvtID: 1040	Desc: *heartbeat intervals used by clients is less than or equal to*
MSExchangeTransport	EvtID: 15004	Desc: *
MSExchange Anti-spam Update	EvtID: 1009	Desc: *failed with error*
MSExchange Anti-spam Update	EvtID: 1012	Desc: *failed with error*
MSExchange Anti-spam Update	EvtID: 1017	Desc: *couldn&amp;#39;t successfully use the Microsoft Update agent*
MSExchangeIS	EvtID: 9688	Desc: *This database size is approaching the size limit*
MSExchangeIS	EvtID: 8528	Desc: *has exceeded the maximum mailbox size*
MSExchangeDSAccess	EvtID: 2091	Desc: *DS Server name specified in the registry * was not found in the Sites container*
MSExchangeIS	EvtID: 9581	Desc: *Virus scanner was not loaded*
MSExchangeIS	EvtID: 9565	Desc: *Invalid virus scanner configuration. Unable to start virus scanner*
MSExchangeTransport	EvtID: 4003	Desc: *domain*currently unreachable*

MB-HyperV-S.EVT.S.P2.Alm

Hyper-V-Integration	EvtID: 4010	Desc: *

Hyper-V-VMMS	EvtID: 19090	Desc: *
Hyper-V-VMMS	EvtID: 19100	Desc: *
Hyper-V-VMMS	EvtID: 16050	Desc: *
Hyper-V-VMMS	EvtID: 16060	Desc: *
Hyper-V-VMMS	EvtID: 16210	Desc: *
Hyper-V-Worker	EvtID: 3040	Desc: *

MB-HyperV-S.EVT.S.P3.Alm

Hyper-V-Config	EvtID: 4096	Desc: *
Hyper-V-SynthNic	EvtID: 12572	Desc: *
Hyper-V-SynthNic	EvtID: 12570	Desc: *
Hyper-V-SynthStor	EvtID: 12140	Desc: *
Hyper-V-SynthStor	EvtID: 12240	Desc: *
Hyper-V-SynthStor	EvtID: 12290	Desc: *
Hyper-V-VMMS	EvtID: 16310	Desc: *
Hyper-V-VMMS	EvtID: 10104	Desc: *
Hyper-V-VMMS	EvtID: 16020	Desc: *
Hyper-V-VMMS	EvtID: 16420	Desc: *
Hyper-V-VMMS	EvtID: 16400	Desc: *
Hyper-V-VMMS	EvtID: 16410	Desc: *
Hyper-V-VMMS	EvtID: 16060	Desc: *
Hyper-V-VMMS	EvtID: 12240	Desc: *
Hyper-V-VMMS	EvtID: 12290	Desc: *
Hyper-V-Worker	EvtID: 3320	Desc: *
Hyper-V-Worker	EvtID: 3030	Desc: *
Hyper-V-Worker	EvtID: 3122	Desc: *
Hyper-V-Worker	EvtID: 3080	Desc: *
Hyper-V-Worker	EvtID: 3050	Desc: *
Hyper-V-Worker	EvtID: 12140	Desc: *

MB-HyperVRepl-S.EVT.S.P3.Alm

Hyper-V-VMMS	EvtID: 19060	Desc: *The virtual machine is currently performing the following operation*
Hyper-V-VMMS	EvtID: 29012	Desc: *Could not apply the replicated changes on the Replica virtual machine*
Hyper-V-VMMS	EvtID: 29292	Desc: *The operation timed out*
Hyper-V-VMMS	EvtID: 29296	Desc: *An unexpected network error occurred*
Hyper-V-VMMS	EvtID: 32022	Desc: *
Hyper-V-VMMS	EvtID: 32026	Desc: *Hyper-V failed to generate delta for virtual machine*
Hyper-V-VMMS	EvtID: 32032	Desc: *There is not enough space on the disk*
Hyper-V-VMMS	EvtID: 32088	Desc: *replication is suspended on the Replica server*
Hyper-V-VMMS	EvtID: 32326	Desc: *requires resynchronization to get back into an operational state*
Hyper-V-VMMS	EvtID: 32346	Desc: *it is about to run out of disk space*
Hyper-V-VMMS	EvtID: 32350	Desc: *requires resynchronization because tracking went into error state*

Hyper-V-VMMS	EvtID: 32366	Desc: *failed to apply the log file onto the VHD*
Hyper-V-VMMS	EvtID: 32510	Desc: *Failed to delete the log file*
Hyper-V-VMMS	EvtID: 32546	Desc: *cannot be performed for this virtual machine while it is in its current state*
Hyper-V-VMMS	EvtID: 32572	Desc: *Hyper-V failed to resynchronize changes for virtual machine*
Hyper-V-VMMS	EvtID: 32587	Desc: *Failed to update log file time*
Hyper-V-VMMS	EvtID: 32592	Desc: *Hyper-V Replica failed to apply changes*
Hyper-V-VMMS	EvtID: 33676	Desc: *There is not enough space on the disk*
Hyper-V-VMMS	EvtID: 33680	Desc: *Replication operation for virtual machine*
Hyper-V-VMMS	EvtID: 33812	Desc: *Reference point export operation failed due to invalid data*
Hyper-V-VMMS	EvtID: 33824	Desc: *would be disabled because it has run out of required disk space*
Hyper-V-VMMS	EvtID: 20880	Desc: *Failed to delete folder*
Hyper-V-VMMS	EvtID: 32315	Desc: *Hyper-V failed to replicate changes for virtual machine*
Hyper-V-VMMS	EvtID: 33826	Desc: *about to run out of the required disk space*

MB-ICC-A.EVT.S.P3.Alm

RMM-SMARTMON	EvtID: 131	Desc: *RMSICC: On Primary Connection*
RMM-SMARTMON	EvtID: 132	Desc: *RMSICCRMSICC: On Backup Connection*
RMM-SMARTMON	EvtID: 135	Desc: *RMSICC: Primary IP not set - NOT CONFIGURED!*
RMM-SMARTMON	EvtID: 136	Desc: *RMSICC: Unsupported Platform!*

MB-IIS.EVT.S.P3.Alm

IIS-W3SVC	EvtID: 1003	Desc: *
IIS-W3SVC	EvtID: 1004	Desc: *
IIS-W3SVC	EvtID: 1007	Desc: *

MB-ITP-A.EVT.S.P2.Alm

ITP_Monitor	EvtID: 101	Desc: ITP_Supervisor Service not installed
ITP_Monitor	EvtID: 101	Desc: ITP_Supervisor Service not automatic start
ITP_Monitor	EvtID: 101	Desc: ITP_Supervisor Service not running
ITP_Monitor	EvtID: 102	Desc: ITP Service in inactive state
ITP_Monitor	EvtID: 103	Desc: ITP Process Engine in inactive state

MB-KAVL.EVT.W.P3.Alm

*	EvtID: 4660	Desc: *License has expired*
*	EvtID: 4660	Desc: *Application is not activated*

MB-KNMG-A.EVT.S.P3.Act

Kaseya Network Monitor	EvtID: 0	Desc: *Failed to perform handshake with server, no answer*

MB-LDS-S.EVT.S.P3.Alm

Cissesrv	EvtID: 24595	Desc: *drive failure notification*
Cissesrv	EvtID: 24596	Desc: *predictive failure state*
Server Administrator	EvtID: 2057	Desc: *Virtual disk degraded*
Server Administrator	EvtID: 2048	Desc: *Device failed:*
Server Administrator	EvtID: 2094	Desc: *Predictive Failure reported*
Storage Agents	EvtID: 1200	Desc: *has a new status of 3*
Storage Agents	EvtID: 1200	Desc: *has a new status of 10*
Storage Agents	EvtID: 1200	Desc: *has a new status of 11*
Storage Agents	EvtID: 1200	Desc: *has a new status of 9*
Storage Agents	EvtID: 1200	Desc: *has a new status of 13*
Storage Agents	EvtID: 1200	Desc: *has a new status of 15*
Storage Agents	EvtID: 1216	Desc: *has a new status of 3*
Storage Agents	EvtID: 1216	Desc: *has a new status of 4*

MB-LDS-S.EVT.W.P2.Alm

IAStorDataMgrSvc	EvtID: 7206	Desc: *

MB-MNT-A.EVT.S.P3.Alm

RMM-MAINTENANCE	EvtID: 102	Desc: *RMM-Maintenance: Invalid*
RMM-MAINTENANCE	EvtID: 104	Desc: *RMM-Maintenance: Task Failed:*
RMM-MAINTENANCE	EvtID: 131	Desc: *RMMVDU: Defrag failed -*
RMM-MAINTENANCE	EvtID: 108	Desc: *RMM-Maintenance: ALARM-Uptime exceeds required maximum*
RMM-MAINTENANCE	EvtID: 108	Desc: *RMM-Maintenance: WARNING-Uptime exceeds recommended maximum:*
RMM-MAINTENANCE	EvtID: 191	Desc: *RMMCKD: C*
RMM-MAINTENANCE	EvtID: 192	Desc: *RMMCKD: C*
RMM-MAINTENANCE	EvtID: 193	Desc: *RMMCKD: C*
RMM-MAINTENANCE	EvtID: 105	Desc: *RMM-Maintenance: ALARM*
RMM-MAINTENANCE	EvtID: 105	Desc: *RMM-Maintenance: WARNING*

MB-MNT-A.EVT.W.P3.Alm

RMM-MAINTENANCE	EvtID: 102	Desc: *RMM-Maintenance: Invalid*
RMM-MAINTENANCE	EvtID: 104	Desc: *RMM-Maintenance: Task Failed:*
RMM-MAINTENANCE	EvtID: 131	Desc: *RMMVDU: Defrag failed -*
RMM-MAINTENANCE	EvtID: 109	Desc: *RMM-SysTrayMon: Kixforms.dll failed to init*
RMM-MAINTENANCE	EvtID: 152	Desc: *RMMLSB: System Restore Point*
RMM-MAINTENANCE	EvtID: 108	Desc: *RMM-Maintenance: ALARM*
RMM-MAINTENANCE	EvtID: 108	Desc: *RMM-Maintenance: WARNING*

RMM-MAINTENANCE	EvtID: 191	Desc: *RMMCKD: C*
RMM-MAINTENANCE	EvtID: 192	Desc: *RMMCKD: C*
RMM-MAINTENANCE	EvtID: 193	Desc: *RMMCKD: C*
RMM-MAINTENANCE	EvtID: 151	Desc: *RMMLSB: Backup process completed with errors*
RMM-MAINTENANCE	EvtID: 901	Desc: *RMM-SysTrayMon: User Ticket Request*
RMM-MAINTENANCE	EvtID: 105	Desc: *RMM-Maintenance: ALARM*
RMM-MAINTENANCE	EvtID: 105	Desc: *RMM-Maintenance: WARNING*

MB-MNT-A.EVT.W.P3.Chk

RMM-MAINTENANCE	EvtID: 100	Desc: *RMM-Maintenance: Complete - NITE*

MB-MNT-RUNNOW-A.EVT.W.P4.Req

RMM-MAINTENANCE	EvtID: 108	Desc: *RMM-Maintenance: User requests immediate execution*

MB-MNT-SUSP_ALM-A.EVT.S.P4.Req

RMM-Maintenance	EvtID: 901	Desc: *

MB-NTS.EVT.S.P3.Alm

Microsoft-Windows-Time-Service	EvtID: 1	Desc: *
Microsoft-Windows-Time-Service	EvtID: 4	Desc: *
Microsoft-Windows-Time-Service	EvtID: 11	Desc: *
Microsoft-Windows-Time-Service	EvtID: 12	Desc: *
Microsoft-Windows-Time-Service	EvtID: 15	Desc: *
Microsoft-Windows-Time-Service	EvtID: 21	Desc: *
Microsoft-Windows-Time-Service	EvtID: 28	Desc: *
Microsoft-Windows-Time-Service	EvtID: 30	Desc: *
Microsoft-Windows-Time-Service	EvtID: 31	Desc: *
Microsoft-Windows-Time-Service	EvtID: 32	Desc: *
Microsoft-Windows-Time-Service	EvtID: 34	Desc: *
Microsoft-Windows-Time-Service	EvtID: 36	Desc: *
Microsoft-Windows-Time-Service	EvtID: 39	Desc: *
Microsoft-Windows-Time-Service	EvtID: 41	Desc: *
Microsoft-Windows-Time-Service	EvtID: 42	Desc: *
Microsoft-Windows-Time-Service	EvtID: 44	Desc: *
Microsoft-Windows-Time-Service	EvtID: 45	Desc: *
Microsoft-Windows-Time-Service	EvtID: 46	Desc: *
Microsoft-Windows-Time-Service	EvtID: 50	Desc: *
Microsoft-Windows-Time-Service	EvtID: 54	Desc: *
Microsoft-Windows-Time-Service	EvtID: 130	Desc: *
Microsoft-Windows-Time-Service	EvtID: 131	Desc: *
Microsoft-Windows-Time-Service	EvtID: 141	Desc: *
Microsoft-Windows-Time-Service	EvtID: 142	Desc: *
Microsoft-Windows-Time-Service	EvtID: 144	Desc: *

MB-PSP.EVT.S.P2.Alm

Microsoft-Windows-PrintSpooler	EvtID: 363	Desc: *

MB-PSP.EVT.S.P3.Alm

Microsoft-Windows-PrintSpooler	EvtID: 99	Desc: *
Microsoft-Windows-PrintSpooler	EvtID: 315	Desc: *
Microsoft-Windows-PrintSpooler	EvtID: 319	Desc: *
Microsoft-Windows-PrintSpooler	EvtID: 361	Desc: *

MB-RDCM.EVT.S.P3.Alm

Microsoft-Windows-TerminalServices-RemoteConnectionManager	EvtID: 1149	Desc: *

MB-RDGW.EVT.S.P3.Alm

Microsoft-Windows-TerminalServices-Gateway	EvtID: 203	Desc: *

MB-RDLC.EVT.S.P3.Alm

Microsoft-Windows-TerminalServices-Licensing	EvtID: 12	Desc: *
Microsoft-Windows-TerminalServices-Licensing	EvtID: 22	Desc: *
Microsoft-Windows-TerminalServices-Licensing	EvtID: 36	Desc: *

MB-SM-A.EVT.S.P3.Alm

RMM-SMARTMON	EvtID: 161	Desc: *RMSDCC: Disk Capacity Trending Alarm for*
RMM-SMARTMON	EvtID: 162	Desc: *RMSDCC*
RMM-SMARTMON	EvtID: 181	Desc: *RMSNTP: Warning - Domain Time*
RMM-SMARTMON	EvtID: 181	Desc: *RMSNTP: Alert - Domain Time*
RMM-SMARTMON	EvtID: 182	Desc: *RMSNTP:*
RMM-SMARTMON	EvtID: 183	Desc: *RMSNTP: Alert - NTPDATE.EXE is not present*
RMM-SMARTMON	EvtID: 169	Desc: *RMSDCC: Invalid custom parameter*
RMM-SMARTMON	EvtID: 165	Desc: *RMSDCC: Disk Monitors suspended*
RMM-SMARTMON	EvtID: 163	Desc: *RMSDCC: Disk Capacity CRITICAL Alarm*
RMM-SMARTMON	EvtID: 184	Desc: *RMSNTP: Alert - Multiple NTP Time Resync actions*
RMM-SMARTMON	EvtID: 121	Desc: *RMSSBM: The system has booted into Safe Mode*
RMM-SMARTMON	EvtID: 126	Desc: *RMSSBM: The system has booted during business hours*
RMM-SMARTMON	EvtID: 129	Desc: *RMSSBM: Unable to calculate uptime*
RMM-SMARTMON	EvtID: 187	Desc: *RMSNTP: Alert - W32Time service is missing*

RMM-SMARTMON	EvtID: 122	Desc: *RMSSBM: The system has booted into Directory Services Restore Mode*
RMM-SMARTMON	EvtID: 123	Desc: *RMSSBM: The system has Safe Mode Boot enabled*
RMM-SMARTMON	EvtID: 171	Desc: *RMSUSC:*
RMM-SMARTMON	EvtID: 172	Desc: *RMSUSC:*
RMM-SMARTMON	EvtID: 173	Desc: *RMSUSC:*

MB-SM-A.EVT.W.P3.Alm

RMM-SMARTMON	EvtID: 111	Desc: *RMSSSC: Antivirus - Product not detected!*
RMM-SMARTMON	EvtID: 112	Desc: *RMSSSC: Antivirus - Outdated -*
RMM-SMARTMON	EvtID: 113	Desc: *RMSSSC: Antivirus - Not running -*
RMM-SMARTMON	EvtID: 114	Desc: *RMSSSC: Antivirus - Multiple products are running*
RMM-SMARTMON	EvtID: 115	Desc: *RMSSSC: Antivirus - Protection is suspended*
RMM-SMARTMON	EvtID: 161	Desc: *RMSDCC: Disk Capacity Trending Alarm for*
RMM-SMARTMON	EvtID: 162	Desc: *RMSDCC: Disk Capacity*
RMM-SMARTMON	EvtID: 181	Desc: *RMSNTP:*
RMM-SMARTMON	EvtID: 182	Desc: *RMSNTP:*
RMM-SMARTMON	EvtID: 183	Desc: *RMSNTP: Alert - NTPDATE.EXE is not present*
RMM-SMARTMON	EvtID: 169	Desc: *RMSDCC: Invalid custom parameter*
RMM-SMARTMON	EvtID: 116	Desc: *RMSSSC: Antivirus - Preferred Product not installed*
RMM-SMARTMON	EvtID: 163	Desc: *RMSDCC: Disk Capacity CRITICAL Alarm*
RMM-SMARTMON	EvtID: 187	Desc: *RMSNTP: Alert - W32Time service is missing*
RMM-SMARTMON	EvtID: 171	Desc: *RMSUSC:*
RMM-SMARTMON	EvtID: 172	Desc: *RMSUSC:*
RMM-SMARTMON	EvtID: 173	Desc: *RMSUSC:*

MB-SM-A.EVT.X.P5.Log

RMM-SMARTMON	EvtID: 110	Desc: *RMSSSC: STATUS:*
RMM-SMARTMON	EvtID: 160	Desc: *RMSDCC: STATUS:*
RMM-SMARTMON	EvtID: 180	Desc: *RMSNTP: STATUS:*
RMM-SMARTMON	EvtID: 190	Desc: *RMMCKD: STATUS:*

MB-SM-TIME-A.EVT.S.P3.Act

RMM-SMARTMON	EvtID: 185	Desc: *RMSNTP: Warning - PDCe is not using NTP*
RMM-SMARTMON	EvtID: 186	Desc: *RMSNTP: Warning - Member server is not using NT5DS*

MB-SQL.EVT.S.P3.Alm

MSSQL*	EvtID: 3041	Desc: *
SQLAgent*	EvtID: 208	Desc: *
SQLSERVERAGENT*	EvtID: 208	Desc: *
SQLISPackage*	EvtID: 12291	Desc: *failed*

MB-Veeam-BR-X.EVT.S.P3.Alm

Veeam*	EvtID: 150	Desc: *
Veeam*	EvtID: 194	Desc: *
Veeam*	EvtID: 250	Desc: *
Veeam*	EvtID: 251	Desc: *
Veeam*	EvtID: 290	Desc: *
Veeam*	EvtID: 350	Desc: *
Veeam*	EvtID: 360	Desc: *
Veeam*	EvtID: 390	Desc: *
Veeam*	EvtID: 490	Desc: *
Veeam*	EvtID: 590	Desc: *
Veeam*	EvtID: 592	Desc: *
Veeam*	EvtID: 24030	Desc: *
Veeam*	EvtID: 24020	Desc: *
Veeam*	EvtID: 24040	Desc: *
Veeam*	EvtID: 24050	Desc: *
Veeam*	EvtID: 190	Desc: *

MB-Veeam-Success-X.EVT.S.P3.Alm

Veeam*	EvtID: 190	Desc: *success*

MB-WAE-A.EVT.X.P3.Alm

These monitors are specific to RMM Suite licensing and represent a failure to obtain a software license. Should these alarms be reported, confirm that the RMM Suite folders as well as the ability to generate checksums have been whitelisted / permitted by AV software.

RMM-AUTH	EvtID: 401	Desc: *
RMM-AUTH	EvtID: 402	Desc: *
RMM-AUTH	EvtID: 403	Desc: *
RMM-AUTH	EvtID: 404	Desc: *
RMM-AUTH	EvtID: 412	Desc: *
RMM-AUTH	EvtID: 405	Desc: *
RMM-AUTH	EvtID: 406	Desc: *

Creating a Custom Monitor Set

Creating a custom monitor set is as easy as defining the Services or Event Log IDs that you want to alert on and assigning a name to your monitor set that follows our MonSetID naming standard. Using the RMM Suite methods to detect when the monitor should be applied and applying it automatically isn't difficult, but does take a little bit of planning and effort. The best way to understand this is through an end to end example.

Determine What to Monitor

The first step is to determine what should be monitored. In our example, we want to monitor a custom application called Gizmo Processing. The application has one service - GizmoManager - and writes several event log events, but only two require an alarm. Both of these events have an Event Source of "GizmoMgrSvc". One event we want to monitor has an Event ID of 112, and the other has an Event ID of 119. According to the application documentation, Event ID 112 can produce both Warning and Error events, but we only want the Error event, which displays a message "Failed to deliver message:", followed by the message ID.

Create the Monitor Sets

We'll create the Service Monitor set first. Add the GizmoManager service to the monitor set, then save it with the name "**Gizmo.SVC.S.P3.Act**". The first part is the Unique Name, which can simply be "Gizmo". The next part is "SVC", which indicates a Service class monitor. The "S" indicates this monitor applies to servers, and is followed by the priority of this alarm. You can set any priority you wish, from 4 (Low) to 1 (Critical). Anything lower than 3 (higher priority) will be eligible to generate an after-hours page, so assign the priorities appropriately.

Next, create the Event Log monitor set. Define the Event Source, Event ID, and for Event 112, specify the common part of the Description text "Failed to deliver message" so that only the error and not the warning message triggers the alarm. Performing sufficient qualifying of the alert data will go a long way in minimizing the false alarms in your environment.

At this point, you could stop and manually apply these two monitor sets to the servers that run the Gizmo application, but that's not "the RMM Suite way".

Update the Audit to Locate the App

When the Daily Audit runs, it can find services and applications and associate them with "tags". These tags are written to the System Roles custom field and will be used to control the automatic deployment of the monitor sets. Creating a custom discovery and tagging action requires updating the Audit.ini file using the web management interface.

Service Roles

The easiest way to create a tag is be locating the Windows Service. Since the Gismo Processing application has a GizmoManager service, we'll leverage this to create our tag. Simply locate the SERVICE ROLES section and add an entry as shown below:

```
GizmoManager=GZMO
```

This represents the Service Name and the assigned TAG value. TAGs can be 3-4 characters long and *must* be unique. Any time you create a new service or application mapping entry, you should scan the configuration to ensure that your new tag is unique. This is all you need to do - the RMM Suite audit tool will locate the service and add the tag to the System Roles field automatically.

Define the Automation

The automation will vary from RMM platform to platform. The method is similar in all cases - you use a filter to select the computers that have the Tags assigned by the daily audit and then use a policy to apply the monitor sets that were created. The process for each supported RMM platform will be reviewed here.

Kaseya VSA

Create a View/Filter

For VSA platforms, you need to create a View that will fire when the tag is found in the System Roles field. Our views are just a bit more complex than that, though.

1. Create a new Policy Control view - we recommend using a "YAPC" prefix on these views - "Y" simply to group these views together and the end of the list, and "APC" for "Automatic Policy Control". Since this is for Gizmo application monitoring, we'll call the view "**YAPC-Gizmo Monitoring**".
    a. Select the option for "Agents that are NOT suspended"
    b. Select the option for "All Windows Operating Systems"
2. Click the Advanced Properties button and add the following entries:
    a. In Operating System, enter "*Server*" to only select Server platforms. This part is optional and should NOT be done if the service can run on workstations.
    b. In the Policy Control field, enter "NOT *GZMO*. This is the field that *turns off* the monitoring.
    c. In the System Roles field, enter "*GZMO*". This is the field that turns the monitoring on.
    In steps b and c, replace "GZMO" with the tag ID for your custom monitor!
    d. Apply the advanced settings and Save the view.
3. Use the view and verify that the computers that were identified by the Daily Audit as having the custom application are displayed. You may need to manually initiate the Daily Tasks to force the audit to run with the latest configuration updates.

Create a System Policy

The Policy is how Kaseya uses the View to define which monitor sets to apply.

1. Create a new Policy in the **Custom Monitoring (Auto-Pilot)** folder. Define an appropriate name that identifies this as a monitoring policy for your application, such as **Gizmo Processing Monitors**.
2. Add the view you created earlier - this defines when this policy will be applied.
3. Define the Service and Event Log monitors you created

Administration

Most of the process of monitoring is automated within the RMM Suite, by detecting components through the Daily Audit, defining Tags, and using the tags to apply the monitors. There are cases where the automation should be disabled if the discovered components don't need to be monitored.

Fortunately, the process to disable a monitor is simply to identify the tag that is applying the monitor set and then assign that same tag to the Policy Control field. In the RMM Suite, the System Roles field defines what was discovered and should be monitored, and the Policy Control field is used to disable that automation. In short - the rule is "Apply a monitor set associated with a specific tag unless that tag is also defined in the Policy Control field."

There are times where this control may not be "fine-grained" enough. You might want to monitor *some but not all* of the items in the default monitor set. In this case, you will need to duplicate and customize the standard monitor set and policy with a unique tag (simply use an "X" prefix on the standard tag). Update the Audit.ini file to use your modified tag and deploy that custom configuration to the customer or machine where the custom monitoring is needed.

Service Monitor "False" Alarms

It has been a common practice to simply set an unneeded service to "disabled". When this happens, the ticketing system will receive alerts that the service has "failed". This is, in fact, an accurate alarm! The service has failed because the technician has disabled it.

Many service monitors are applied based on the Role and Feature detection process. If a Role or Feature is installed, the system *expects all services associated with the role to be operational.* If you no longer need a role or feature on a server and wish to disable monitoring, you must remove the role or feature from the Operating System. Disabling the service is not enough to stop monitoring the detected role.

If the server is in the process of reconfiguration or decommissioning, you should disable all monitoring or apply specific blocker tags to prevent the monitoring from applying until the Role or Feature is removed or the server fully decommissioned.

Appendix I: Testing Monitors

The RMM Suite includes a tool that can generate test alarms in the Windows Event Log. The RMUATST command accepts a single argument that defines the alarm to test. A full list of supported alarms can be displayed by using the --L parameter.

The RMUATST.INI file lists the ID, description, and parameters for each supported alarm, This file can be customized to allow testing of custom event log monitors. The format for the alarm record is

ID_NAME=Category: Description;*T*,*E*,*S*,*X*

T = Type - 1=Error, 2=Warning
E = Event ID
S = Event Source
X = Text Message to write