

EM DevXchange

Manage Alerts Centrally & Automatically with CA SOI

Michael Boehm

Sen. Engineering Services Architect

12 May 2016



Agenda

1 **CLASSIFICATION: EVENT – ALERT**

2 **ALERT QUEUES**

3 **ESCALATION POLICIES**

4 **ALERT MANAGEMENT POLICIES**

5 **CONNECTOR POLICY**

6 **Q & A**

Classification: Event – Alert

- Event
 - a software message indicating that something has happened
- Alert
 - a warning that indicates an emergency situation
 - Actionable: ticket, email, Operator



Alert Queues

- Alert-centric view
- Service- and non-Service impacting
- Grouping according to criteria
- Access control
- Queue specific Escalation Policies
- History

Navigation

Services | **Alert Queues** | Customers | Users

Name	Σ	▼	▼	▼	▼
Alert Queues	16	2	7	5	1
Application	2	2			
Critical	7		7		
Default					
Gold	7		7		
Network	11		6	4	1
Silver	6			6	
SNMP					
UIM					

Contents: Default

Alerts | Information

Default

General Information

Queue Name: Default

Queue Criteria: This is the default alert queue. Alerts that do not match other alert queue criteria are placed here.

Queue Priority: 0

Security

Filter: [] Displaying 4 of 4

Name	Type	Source Type
Administrators	UserGroup	All Access
Operators (read-only)	UserGroup	All Access
Operators (read-write)	UserGroup	All Access
Super Users	UserGroup	All Access

Associated Escalation Policies

Filter: [] Displaying 1 of 1

Name	Description	Current Status	Policy Type	Created
Default		Active	Service or Queue specific	2016

Cleared Alert History

Filter: [] Displaying 5 of 5

5 alert(s) from Mail 6, 2016 12:42:26 PM HEST - now

Name	Severity	Created On	Cleared On	Category	Summary
CA Service Operations	Major	May 6, 2016 3:48:11 PM CEST	May 9, 2016 11:50:08 AM CEST	Risk	UniversalConnector running on host S0213.1P
CA Service Operations	Major	May 6, 2016 3:48:11 PM CEST	May 9, 2016 11:49:37 AM CEST	Risk	ConnectorService: The CA S02 Integration Se
CA Service Operations	Major	May 6, 2016 3:48:11 PM CEST	May 9, 2016 11:49:33 AM CEST	Risk	GenericSNMPTraps running on host S0213.1P
CA Service Operations	Major	May 6, 2016 3:48:11 PM CEST	May 9, 2016 11:49:33 AM CEST	Risk	EventManager/EventConnector running
CA Service Operations	Major	May 6, 2016 3:48:11 PM CEST	May 9, 2016 11:49:33 AM CEST	Risk	CAServiceOperations/ServiceDiscovery

Escalation Policies

- Automated actions
 - Email
 - Ticketing
 - Process Automation
 - Execute Command
- Global, Queue and Service specific
- Schedule based
- Console Actions

Escalation Action Editor - Create Action - CA Service Operations Insight

Action Name * Action Type * Action is currently ☒ Enabled ☐ Disabled

Description

Properties Summary

Property Name [Help...](#)

Property Value ☐ Create Object if not present

Default Properties

Filter: Displaying 3 of 3

Property Name	Property Value	Create Object	Required
Affected End User	{\$Help Desk Login User}	No	Yes
Description	{\$Alert Description}	No	Yes
Ticket type	Request	No	Yes

* Indicates a required field

Alert Management Policies

- Correlation of Alerts
- Policy actions
 - Filter, Exempt
 - Create new Alert
 - Enrichment, Map-only
- Connector specific
- Historical search

View/Search: EnrichEvent001

Event Search |

Scope

Source... Spectrum Infrastructure Manager_Spectrum Time Range... Last 1 hours

Search Criteria

Event Pattern 1: Severity='Critical' and Summary='PROCESS NOT READY EVENT'

Event Pattern 1: (Severity='Major' or Severity='Critical' or Severity='Fatal') and AlertedMdrElementID='Application:Login'

Event Pattern 1:

Additional Criterion

☒ ANY event occurs ☐ ALL events occur within 30 seconds

☐ OCCURS 2 times within 30 seconds ☐ Sequence enforced

Search Edit Policy... Clear All ^ Hide Criteria

Filter: Displaying 2 of 2

Severity	Summary	Occurrence Time	MDR Product	MDR Product Inst...	Pattern
Critical	Login experienced a critical ...	2012-05-10T13:05:...	Universal Connector	SAManager.RBC...	Pattern1
Critical	PROCESS NOT READY EVENT	2012-05-10T13:04:...	Spectrum Infrastructure Manager	Spectrum-SPserver	Pattern1

Enrichment Policy

Event Log

Group	MDR Product	MDR Product I...	MDR Element ID	Occurrence Time	Severity	Summary
0	Spectrum Infra...	Spectrum-SPse...	4fac022a-5452...	2012-05-10T1...	Critical	PROCESS NOT R...

Parameter Configuration:

Input Parameter	Assigned Value
c_mdrelementid	Functions Attributes Pattern 1 Page 1 Pattern 2 Page 2 Pattern 3

Enrichment Property Assignment:

Event Property	Assigned Value
Tenant ID	
Url Params	
Related Alerts	
Impacted Entities	
Summary	
Assignee	
Related Incident	
Related Incident Uri	
User Attribute 1	\$(c_sysname)
User Attribute 2	
User Attribute 3	
User Attribute 4	

Alerted Mdr Element ID

Alerted Mdr Product Instance

Alerted Mdr Product

Assignee

Elapsed Time

Impacted Entities

Is Acknowledgeable

Is Acknowledged

Is Clearable

Is Cleared

Mdr Element ID

Mdr Prod Instance

Mdr Product

Message

Metric Data Type

Metric Description

Metric Name

Metric Type

Metric Unit Definition

Occurrence Timestamp

Related alerts

Related Incident

Related Incident Uri

Repeat Count

Connector Policy

- Modification on the base
- Global changes
- CI and Alert modification
- XML coding
 - USM Schema
 - Mandatory fields
 - Syntax

```
<Catalog version='1.0' globalextends='GLOBAL'>

<EventClass name='Item' >
  <Classify>
    <Field input='snmp_enterprise' pattern='^1.3.6.1.1.4.1.1.1.2.3.4$' output='eventtype' outval='Item_demo' />
  </Classify>
</EventClass>

<EventClass name='Item_demo' extends='Item'>
  <Classify>
    <Field input='snmp_varbindvals' pattern='^Server,.*$' output='eventtype' outval='Item_demo_CS' />
    <Field input='snmp_varbindvals' pattern='^Database,.*$' output='eventtype' outval='Item_demo_DB' />
    <Field input='snmp_varbindvals' pattern='^Person,.*$' output='eventtype' outval='Item_demo_Person' />
  </Classify>
  <Format>
    <Field output='MdrProduct' format='CA.00036' input='*' />
    <Field output='MdrProdInstance' format='{0}' input='{fqdn(localhost)}' />
  </Format>
  <Write>
    <Field type='publishcache' properties='' />
  </Write>
</EventClass>

<EventClass name='Item_demo_CS' extends='Item_demo'>
  <Parse>
    <Field input='snmp_varbindvals' output='temp_DeviceName' pattern='^.*(.*?)$' />
  </Parse>
  <Format>
    <Field output='MdrElementID' format='Demo_{0}' input='temp_DeviceName' />
    <Field output='ClassName' format='ComputerSystem' input='*' />
    <Field output='SysName' format='{0}' input='temp_DeviceName' />
    <Field output='ClusterAttribute1' format='{0}' input='temp_DeviceName' />
    <Field output='temp_Label' format='{0}' input='temp_DeviceName' />
  </Format>
</EventClass>
```





Michael Boehm

Sen. Engineering Services Architect

Michael.Boehm@ca.com

