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

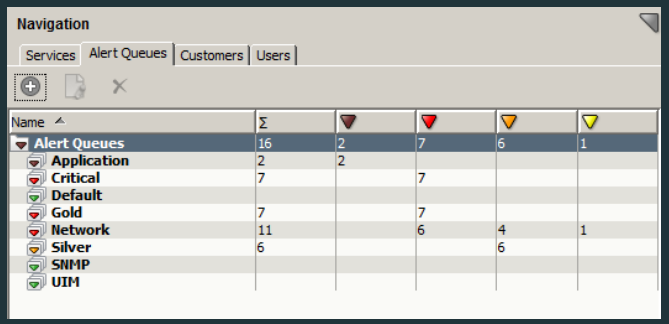
Classification: Event – Alert

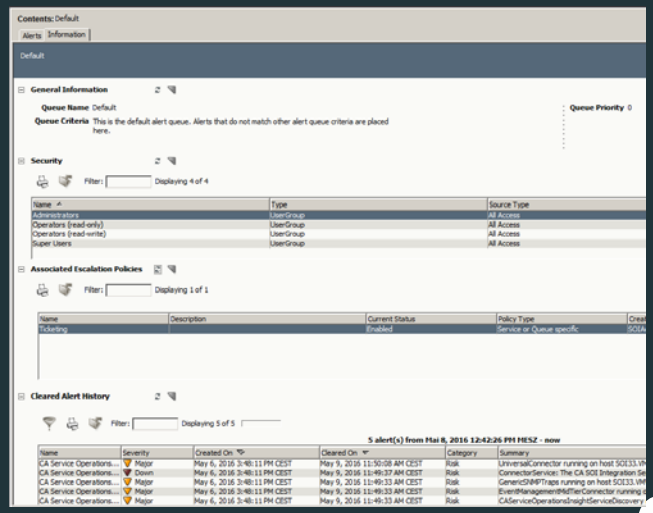
- Event
  - a software message indicating that something has happened

- 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

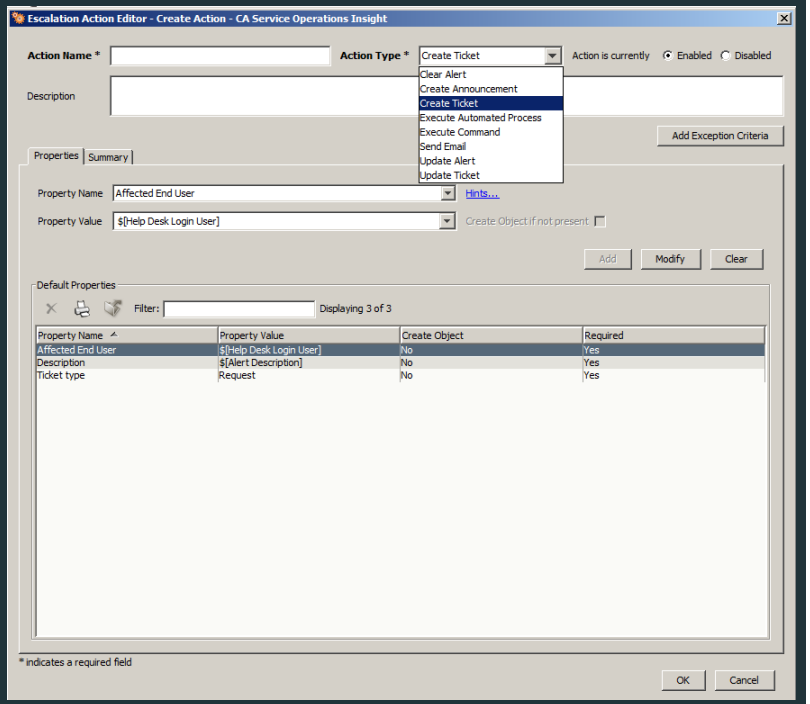




ca technologies

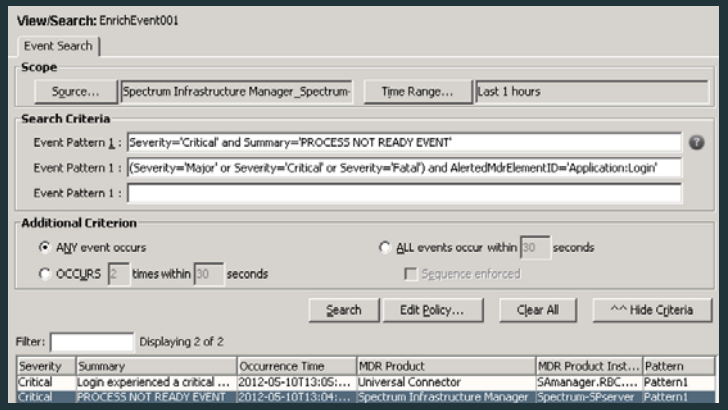
Escalation Policies

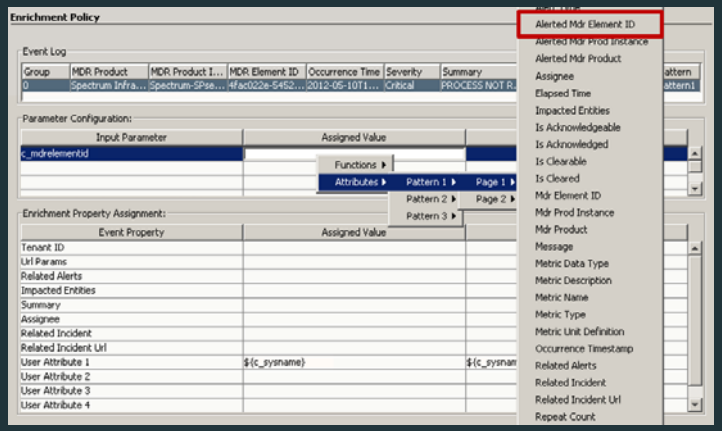
- Automated actions
  - Email
  - Ticketing
  - Process Automation
  - Execute Command
- Global, Queue and Service specific
- Schedule based
- Console Actions



Alert Management Policies

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





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\.4\.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='CluserAttribute1' format='{0}' input='temp_DeviceName' />

                <Field output='temp_Label' format='{0}' input='temp_DeviceName' />
        </Format>
</EventClass>
```


Q & A

Michael Boehm
Sen. Engineering Services Architect
Michael.Boehm@ca.com