Understanding Accelops Backend

Author: Kai

Thanks List

- Get Great Suggestion From
  - Bin (GUI Developer)
  - Yu (Backend Developer)
  - Lin (App Server Developer)

Content

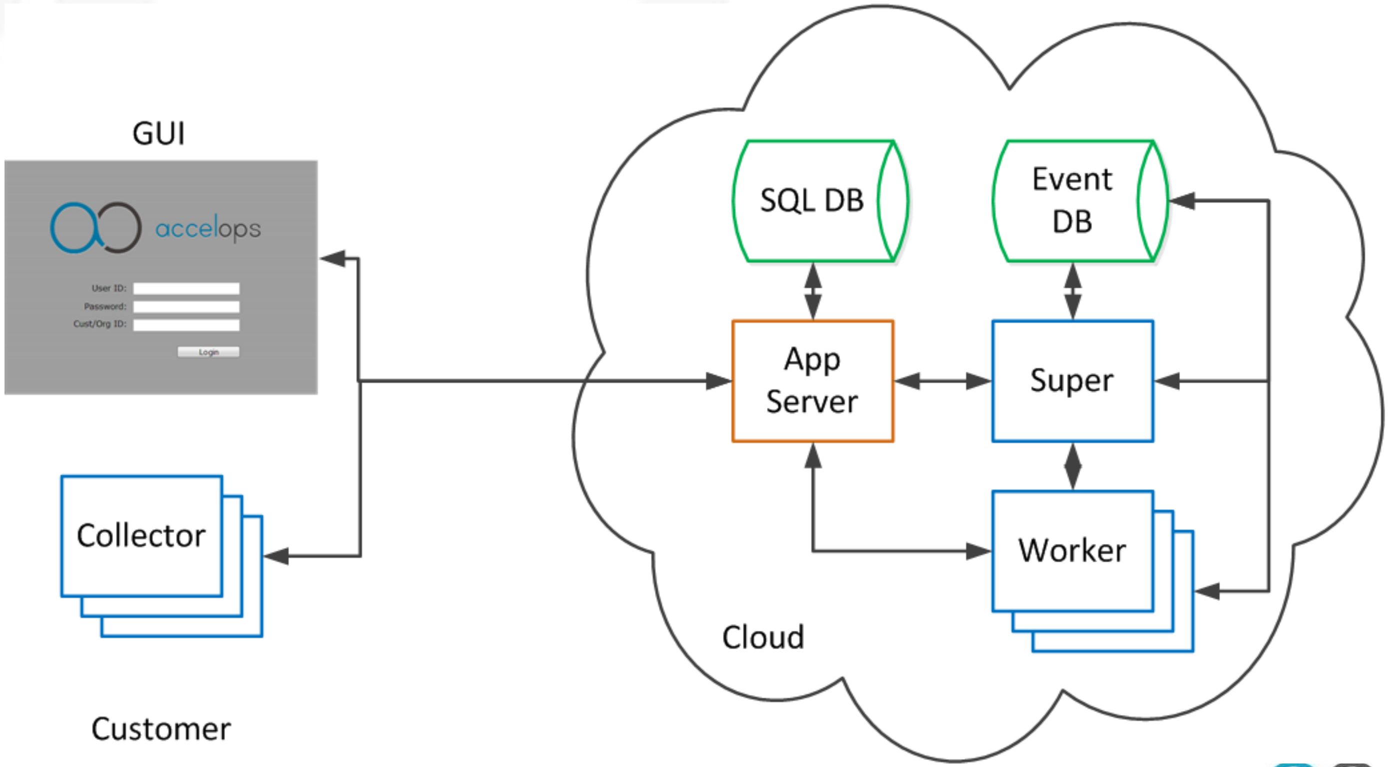
- Outline
- System Structure
- Device Monitor
- Life of Event
- App Server and Backend Communication(A&B C)
- Data Analysis

Outline

- What does Accelops do?
  - Market
    - PAM, SIEM
  - License
    - EPS, Device Number
  - GUI
    - Dashboard, Analytics, Incidents, CMDB, Admin

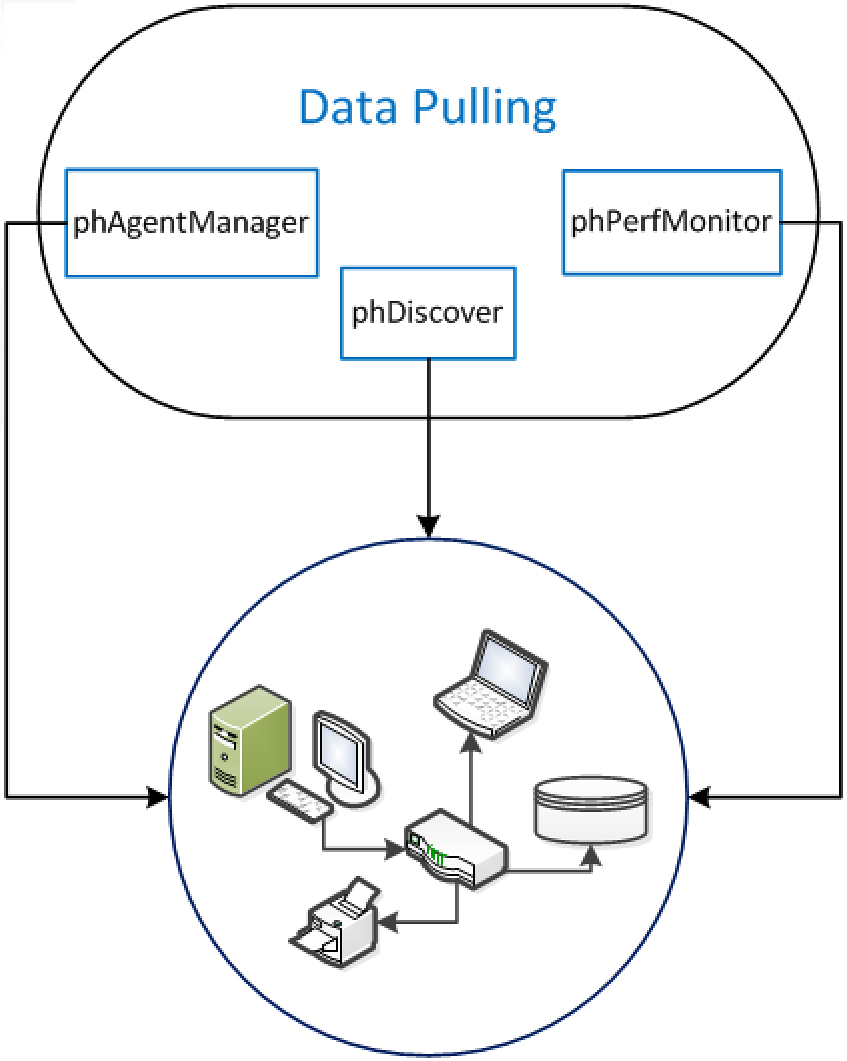
Outline

- AO Backend is about
  - Data Pulling
  - Data Storing
  - Data Analyzing



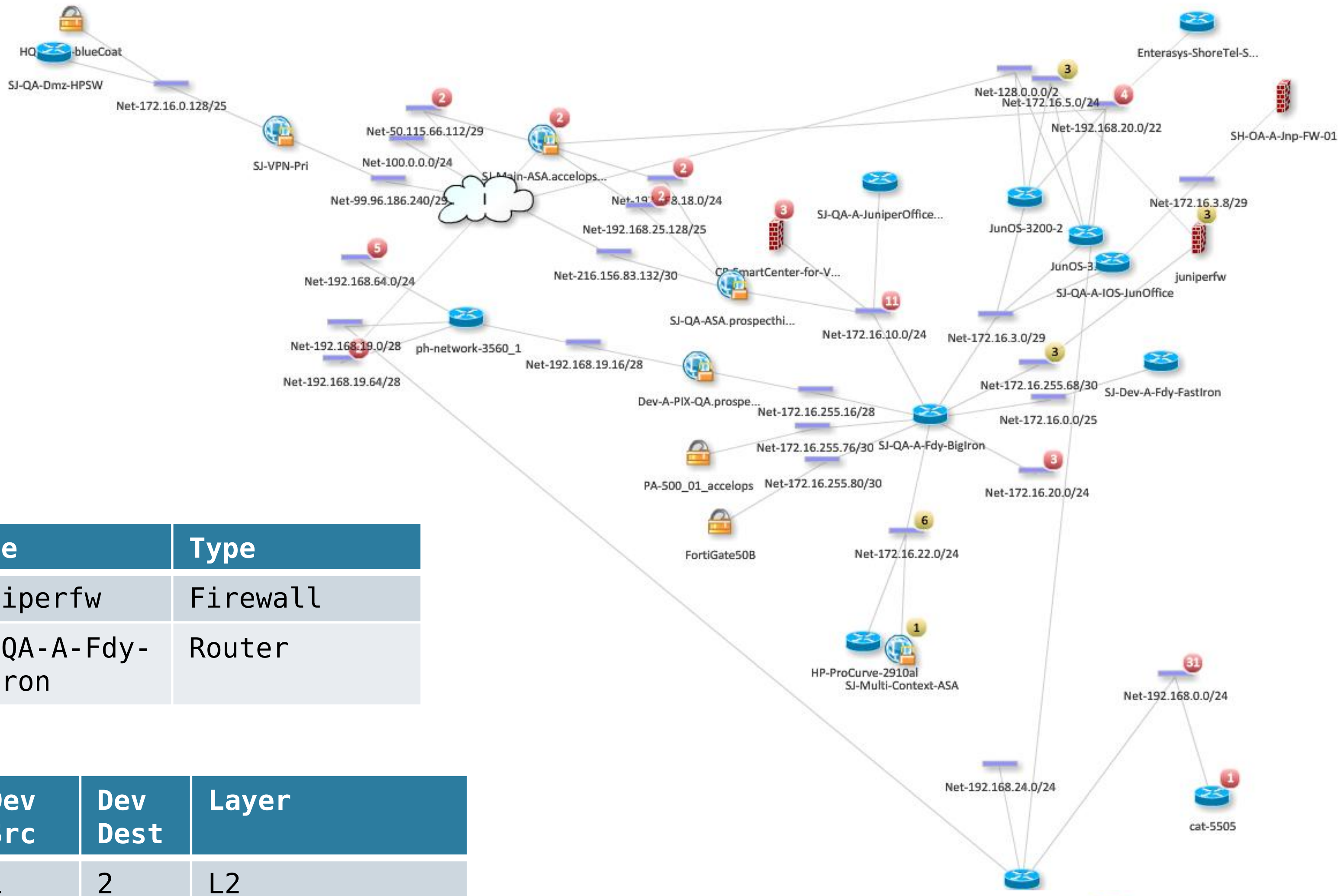
Outline – Data Pulling

- Through protocols:
  - SNMP, WMI, SSH, HTTP
- Also receive event from target device
- Transfer data to:
  - File (SVN Server)
  - XML (SQL DB)
  - Event (Event DB)



Outline – Data Type

- Relational Data – SQL DB

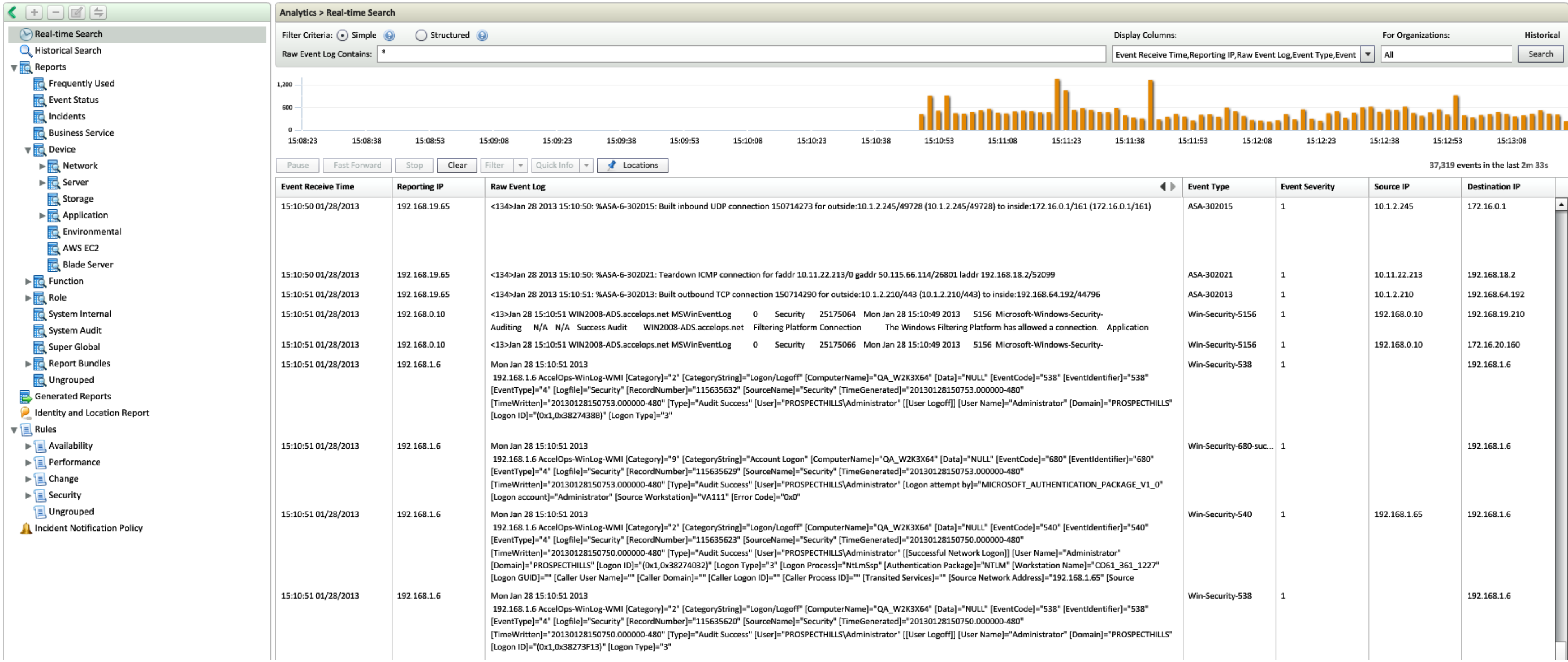


ID	Name	Type
1	juniperfw	Firewall
2	SJ-QA-A-Fdy-Bigron	Router

ID	Dev Src	Dev Dest	Layer
1	1	2	L2

Outline – Data Type

- Time-based Non-Relational Data – Event DB



Filter Criteria: ● Simple ○ Structured

Raw Event Log Contains: *

Display Columns: Event Receive Time,Reporting IP,Raw Event Log,Event Type,Event

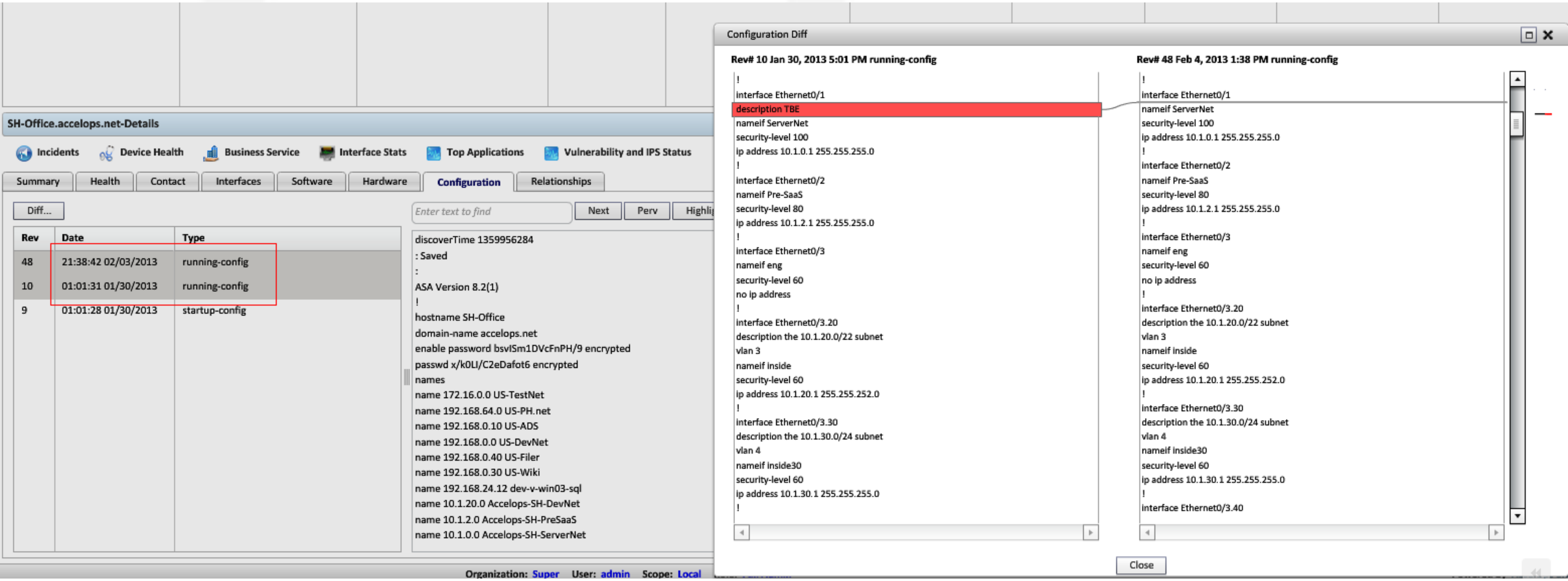
For Organizations: All

37,319 events in the last 2m 33s

Event Receive Time	Reporting IP	Raw Event Log	Event Type	Event Severity	Source IP	Destination IP
15:10:50 01/28/2013	192.168.19.65	<134>Jan 28 2013 15:10:50: %ASA-6-302015: Built inbound UDP connection 150714273 for outside:10.1.2.245/49728 (10.1.2.245/49728) to inside:172.16.0.1/161 (172.16.0.1/161)	ASA-302015	1	10.1.2.245	172.16.0.1
15:10:50 01/28/2013	192.168.19.65	<134>Jan 28 2013 15:10:50: %ASA-6-302021: Teardown ICMP connection for faddr 10.11.22.213/0 gaddr 50.115.66.114/26801 laddr 192.168.18.2/52099	ASA-302021	1	10.11.22.213	192.168.18.2
15:10:51 01/28/2013	192.168.19.65	<134>Jan 28 2013 15:10:51: %ASA-6-302013: Built outbound TCP connection 150714290 for outside:10.1.2.210/443 (10.1.2.210/443) to inside:192.168.64.192/44796	ASA-302013	1	10.1.2.210	192.168.64.192
15:10:51 01/28/2013	192.168.0.10	<13>Jan 28 15:10:51 WIN2008-ADS.accelops.net MSWinEventLog 0 Security 25175064 Mon Jan 28 15:10:49 2013 5156 Microsoft-Windows-Security-Auditing N/A N/A Success Audit WIN2008-ADS.accelops.net Filtering Platform Connection The Windows Filtering Platform has allowed a connection. Application	Win-Security-5156	1	192.168.0.10	192.168.19.210
15:10:51 01/28/2013	192.168.0.10	<13>Jan 28 15:10:51 WIN2008-ADS.accelops.net MSWinEventLog 0 Security 25175066 Mon Jan 28 15:10:49 2013 5156 Microsoft-Windows-Security-	Win-Security-5156	1	192.168.0.10	172.16.20.160
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="2" [CategoryString]="Logon/Logoff" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="538" [EventIdentifier]="538" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635632" [SourceName]="Security" [TimeGenerated]="20130128150753.000000-480" [TimeWritten]="20130128150753.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [[User Logoff]] [User Name]="Administrator" [Domain]="PROSPECTHILLS" [Logon ID]="(0x1,0x3827438B)" [Logon Type]="3"	Win-Security-538	1		192.168.1.6
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="9" [CategoryString]="Account Logon" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="680" [EventIdentifier]="680" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635629" [SourceName]="Security" [TimeGenerated]="20130128150753.000000-480" [TimeWritten]="20130128150753.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [Logon attempt by]="MICROSOFT_AUTHENTICATION_PACKAGE_V1_0" [Logon account]="Administrator" [Source Workstation]="VA111" [Error Code]="0x0"	Win-Security-680-suc...	1		192.168.1.6
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="2" [CategoryString]="Logon/Logoff" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="540" [EventIdentifier]="540" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635623" [SourceName]="Security" [TimeGenerated]="20130128150750.000000-480" [TimeWritten]="20130128150750.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [[Successful Network Logon]] [User Name]="Administrator" [Domain]="PROSPECTHILLS" [Logon ID]="(0x1,0x38274032)" [Logon Type]="3" [Logon Process]="NtLmSsp" [Authentication Package]="NTLM" [Workstation Name]="CO61_361_1227" [Logon GUID]="" [Caller User Name]="" [Caller Domain]="" [Caller Logon ID]="" [Caller Process ID]="" [Transited Services]="" [Source Network Address]="192.168.1.65" [Source	Win-Security-540	1	192.168.1.65	192.168.1.6
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="2" [CategoryString]="Logon/Logoff" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="538" [EventIdentifier]="538" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635620" [SourceName]="Security" [TimeGenerated]="20130128150750.000000-480" [TimeWritten]="20130128150750.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [[User Logoff]] [User Name]="Administrator" [Domain]="PROSPECTHILLS" [Logon ID]="(0x1,0x38273F13)" [Logon Type]="3"	Win-Security-538	1		192.168.1.6

Outline – Data Type

- Version Based Data – SVN



Rev	Date	Type
48	21:38:42 02/03/2013	running-config
10	01:01:31 01/30/2013	running-config
9	01:01:28 01/30/2013	startup-config

```
discoverTime 1359956284
: Saved
:
ASA Version 8.2(1)
!
hostname SH-Office
domain-name accelops.net
enable password bsvISm1DVcFnPH/9 encrypted
passwd x/k0LI/C2eDafot6 encrypted
names
name 172.16.0.0 US-TestNet
name 192.168.64.0 US-PH.net
name 192.168.0.10 US-ADS
name 192.168.0.0 US-DevNet
name 192.168.0.40 US-Filer
name 192.168.0.30 US-Wiki
name 192.168.24.12 dev-v-win03-sql
name 10.1.20.0 Accelops-SH-DevNet
name 10.1.2.0 Accelops-SH-PreSaaS
name 10.1.0.0 Accelops-SH-ServerNet
```

Rev# 10 Jan 30, 2013 5:01 PM running-config

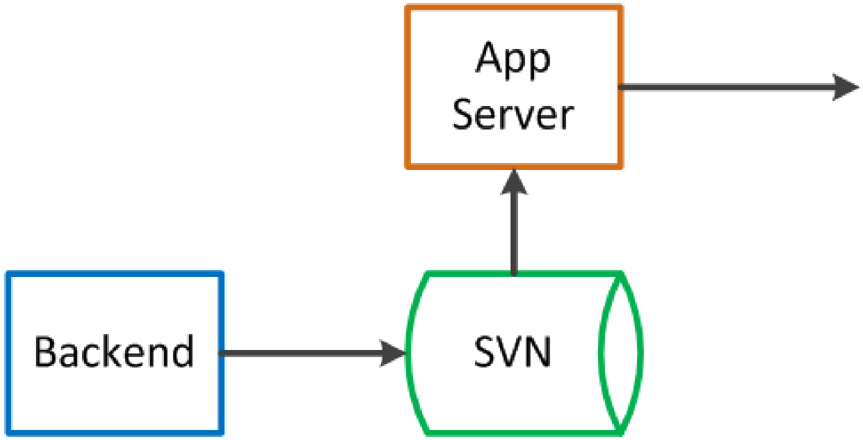
```
!
interface Ethernet0/1
description TBE
nameif ServerNet
security-level 100
ip address 10.1.0.1 255.255.255.0
!
interface Ethernet0/2
nameif Pre-SaaS
security-level 80
ip address 10.1.2.1 255.255.255.0
!
interface Ethernet0/3
nameif eng
security-level 60
no ip address
!
interface Ethernet0/3.20
description the 10.1.20.0/22 subnet
vlan 3
nameif inside
security-level 60
ip address 10.1.20.1 255.255.252.0
!
interface Ethernet0/3.30
description the 10.1.30.0/24 subnet
vlan 4
nameif inside30
security-level 60
ip address 10.1.30.1 255.255.255.0
!
```

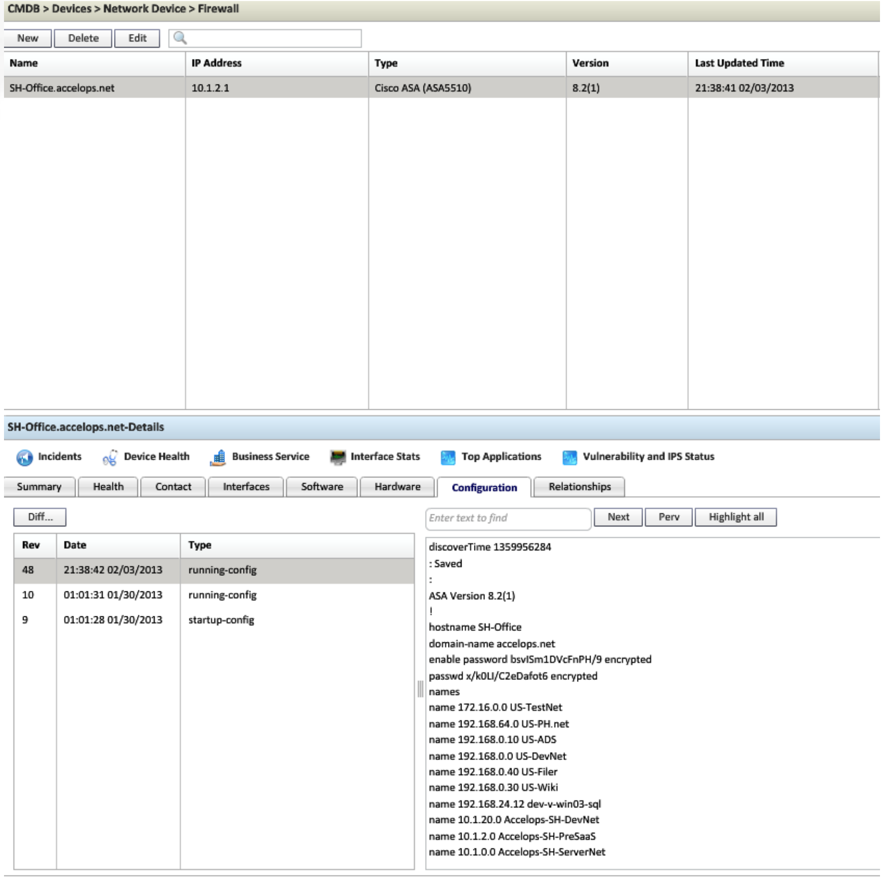
Rev# 48 Feb 4, 2013 1:38 PM running-config

```
!
interface Ethernet0/1
nameif ServerNet
security-level 100
ip address 10.1.0.1 255.255.255.0
!
interface Ethernet0/2
nameif Pre-SaaS
security-level 80
ip address 10.1.2.1 255.255.255.0
!
interface Ethernet0/3
nameif eng
security-level 60
no ip address
!
interface Ethernet0/3.20
description the 10.1.20.0/22 subnet
vlan 3
nameif inside
security-level 60
ip address 10.1.20.1 255.255.252.0
!
interface Ethernet0/3.30
description the 10.1.30.0/24 subnet
vlan 4
nameif inside30
security-level 60
ip address 10.1.30.1 255.255.255.0
!
interface Ethernet0/3.40
```

Outline – SVN

- Data Storing and Analyzing – SVN
  - Backend update SVN
  - GUI show SVN data from App Server
    - Install Software
    - Running Configure
    - Startup Configure





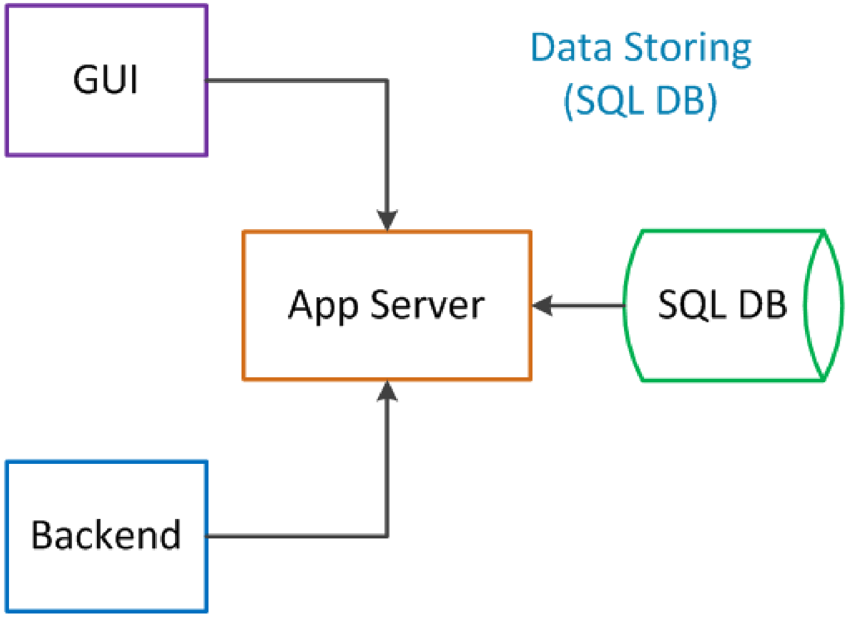
Name	IP Address	Type	Version	Last Updated Time
SH-Office.accelops.net	10.1.2.1	Cisco ASA (ASA5510)	8.2(1)	21:38:41 02/03/2013

Rev	Date	Type
48	21:38:42 02/03/2013	running-config
10	01:01:31 01/30/2013	running-config
9	01:01:28 01/30/2013	startup-config

```
discoverTime 1359956284
: Saved
:
ASA Version 8.2(1)
!
hostname SH-Office
domain-name accelops.net
enable password bsvlSm1DVcFnPH/9 encrypted
passwd x/k0LI/C2eDafot6 encrypted
names
name 172.16.0.0 US-TestNet
name 192.168.64.0 US-PH.net
name 192.168.0.10 US-ADS
name 192.168.0.0 US-DevNet
name 192.168.0.40 US-Filer
name 192.168.0.30 US-Wiki
name 192.168.24.12 dev-v-win03-sql
name 10.1.20.0 Accelops-SH-DevNet
name 10.1.2.0 Accelops-SH-PreSaaS
name 10.1.0.0 Accelops-SH-ServerNet
```

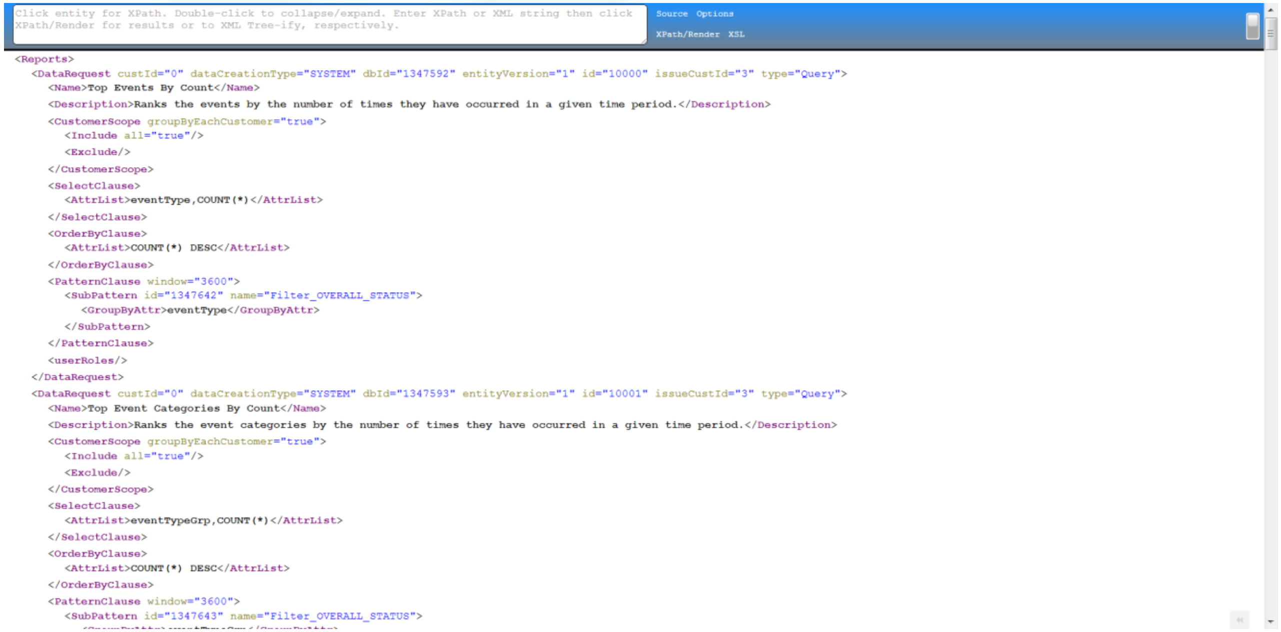
Outline – SQL DB

- Data Storing and Analyzing – SQL DB
  - App Server protect SQL DB
  - REST API (Backend to App Server)



Outline – Rest API

- REST API – Important way for debugging
  - Decouple Backend and App Server
  - Easy to get (browser or curl)
  - Human Readable
  - Cache



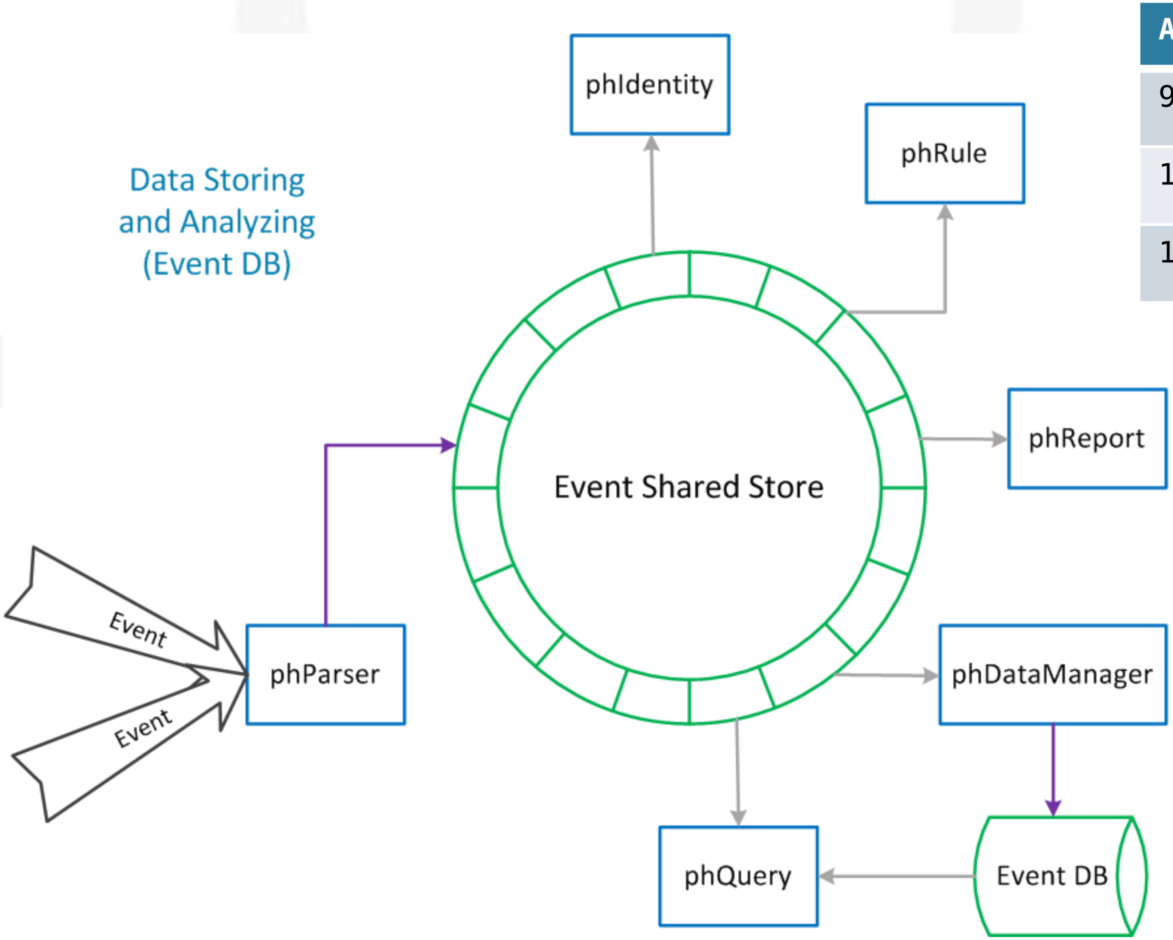
Click entity for XPath. Double-click to collapse/expand. Enter XPath or XML string then click XPath/Render for results or to XML Tree-ify, respectively.
Source
Options
XPath/Render
XSL

```
<Reports>
  <DataRequest custId="0" dataCreationType="SYSTEM" dbId="1347592" entityVersion="1" id="10000" issueCustId="3" type="Query">
    <Name>Top Events By Count</Name>
    <Description>Ranks the events by the number of times they have occurred in a given time period.</Description>
    <CustomerScope groupByEachCustomer="true">
      <Include all="true"/>
      <Exclude/>
    </CustomerScope>
    <SelectClause>
      <AttrList>eventType,COUNT(*)</AttrList>
    </SelectClause>
    <OrderByClause>
      <AttrList>COUNT(*) DESC</AttrList>
    </OrderByClause>
    <PatternClause window="3600">
      <SubPattern id="1347642" name="Filter_OVERALL_STATUS">
        <GroupByAttr>eventType</GroupByAttr>
      </SubPattern>
    </PatternClause>
    <userRoles/>
  </DataRequest>
  <DataRequest custId="0" dataCreationType="SYSTEM" dbId="1347593" entityVersion="1" id="10001" issueCustId="3" type="Query">
    <Name>Top Event Categories By Count</Name>
    <Description>Ranks the event categories by the number of times they have occurred in a given time period.</Description>
    <CustomerScope groupByEachCustomer="true">
      <Include all="true"/>
      <Exclude/>
    </CustomerScope>
    <SelectClause>
      <AttrList>eventTypeGrp,COUNT(*)</AttrList>
    </SelectClause>
    <OrderByClause>
      <AttrList>COUNT(*) DESC</AttrList>
    </OrderByClause>
    <PatternClause window="3600">
      <SubPattern id="1347643" name="Filter_OVERALL_STATUS">
```

File:/opt/phoenix/cache

Outline – Event DB

- Data Storing and Analyzing – Event DB



Attr	Name	Type
9	reptDevIpAddr	IP
1006	hostName	String
1053	inIntfUtil	Double

Attr	Value
9	192.16.20.116
1006	devAOTest
1053	88.13%

Rest API: https://192.168.20.116/phoenix/rest/config/eventAttributeType

System Structure – Selling Model

- Beginning
  - VA
  - SaaS
- Now
  - VA
  - VA with collector
  - AOSP
  - Amazon EC2

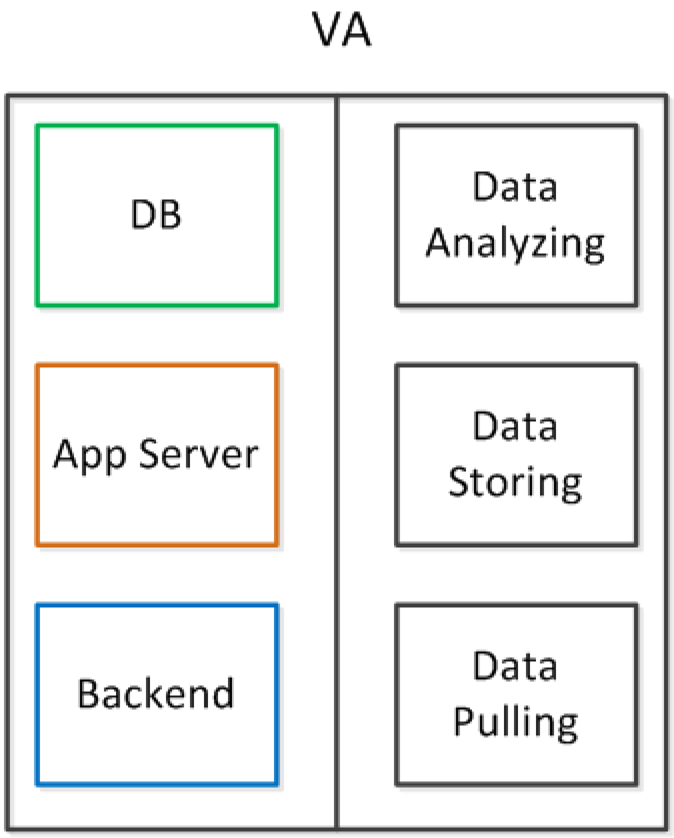
System structure is dependent on how we sell

System Structure – VA

- What IT management tool should like for enterprise at one location
  - Software Install
  - GUI
- Challenge
  - QA need to test different OS – Virtual Machine
  - Access tool from different devices – B/S architecture

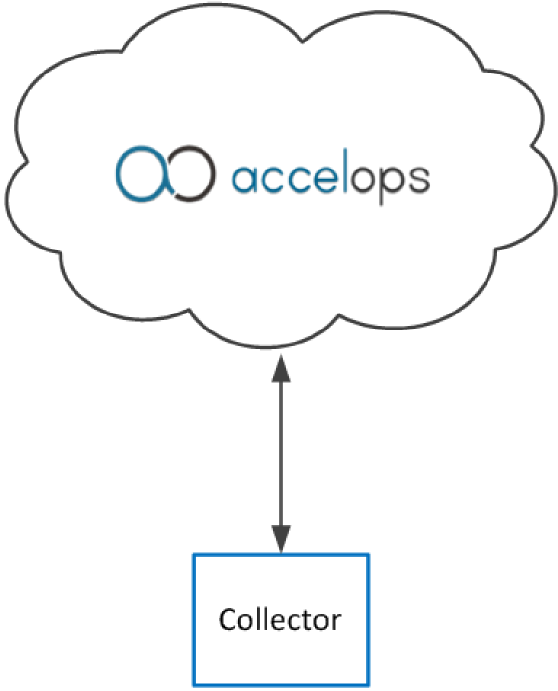
System Structure – VA

- VA – Virtual Application
  - All in One
  - Internal data center
  - Simplified deploy
  - Single customer

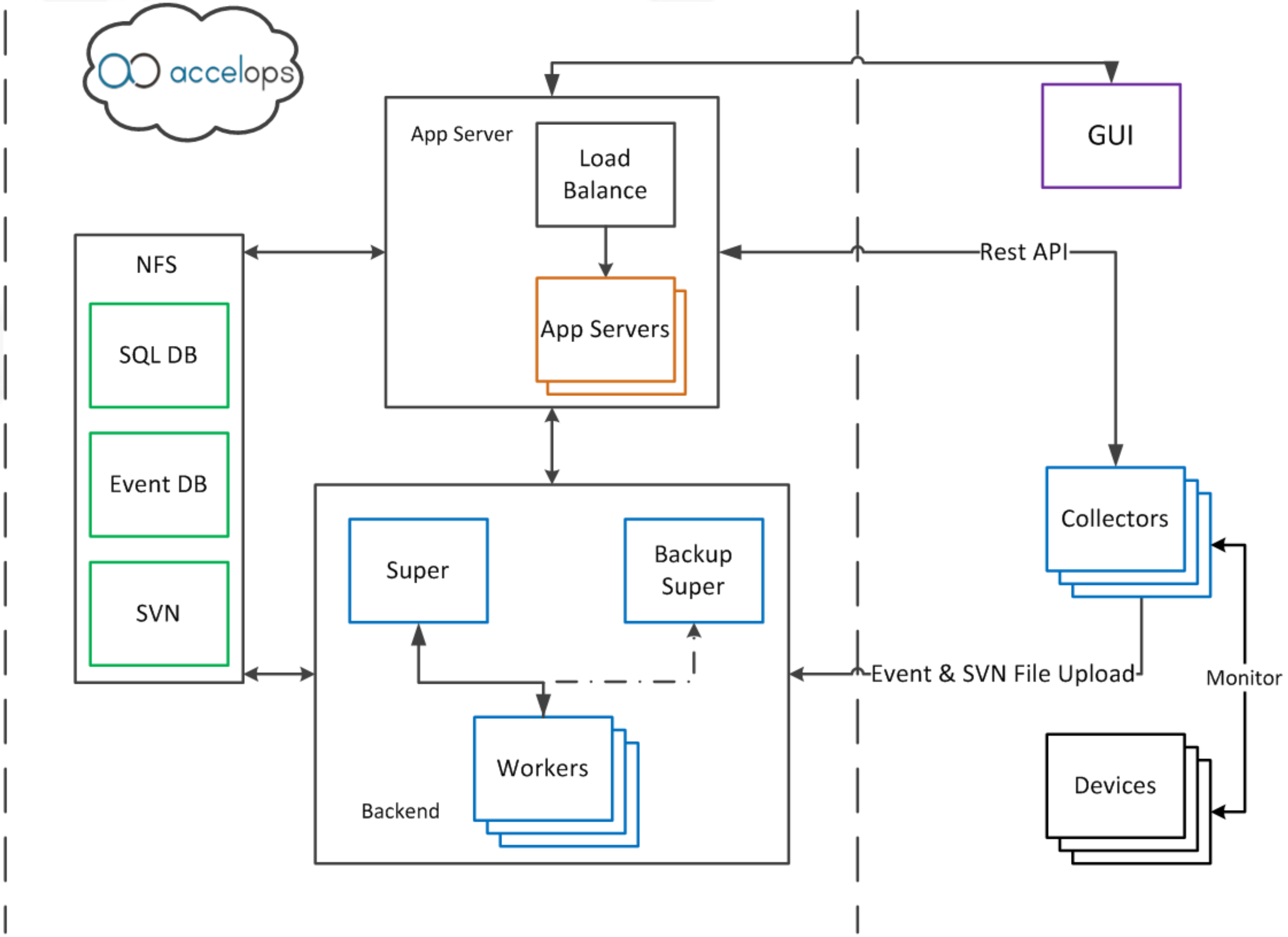


System Structure – Saas

- Saas – Software as a service
  - Customized Resource
  - Light collector
  - Logon to our service and monitoring
- Challenge
  - Scalability – Distributed System
  - Multiple Customer
  - Monitoring Service 7x24



System Structure – SaaS



System Structure – Processes on SaaS

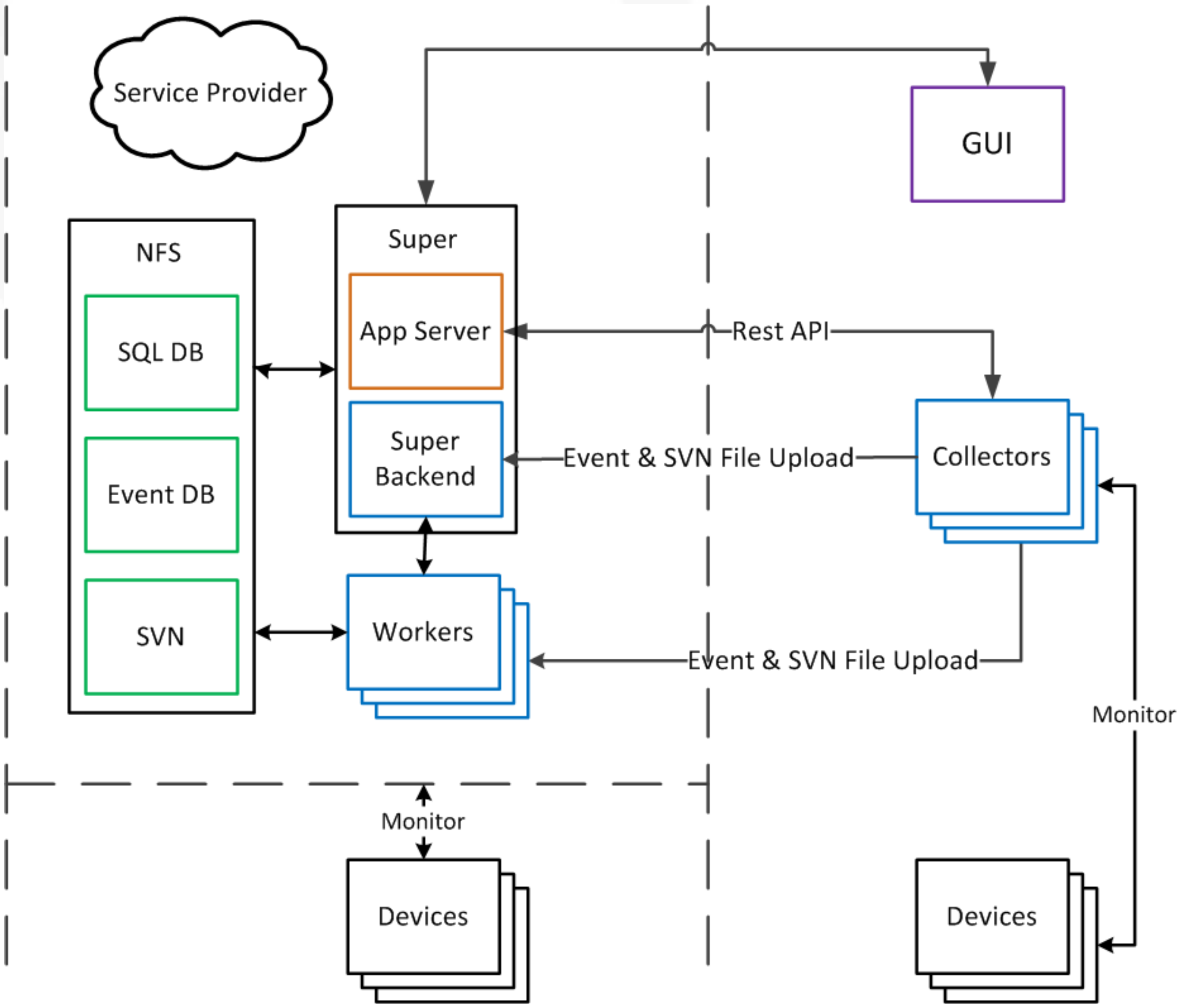
Process	Function	Sp	Wk	Co
phMonitor	Monitoring other processes	√	√	√
(P) phDiscover	Pulling basic data from target			√
(P) phPerfMonitor	Execute performance job			√
(P) phAgentManager	Execute event pulling job			√
(P) phCheckpoint	Execute checkpoint monitoring			√
(S) phParser	Parsing event to shared store (SS)	√	√	√
(S) phEventPackage	Uploading event/svn file to super/worker			√
(S) phDataManager	Save event from SS to Event DB	√	√	
(A) phRuleMaster	Decide if rule fire	√		
(A) phRuleWorker	Aggregating data for rule	√	√	
(A) phQueryMaster	Merge data from queryWorker	√		
(A) phQueryWorker	Execute query task	√	√	
(A) phReportMaster	Merge data from reportWorker	√		
(A) phReportWorker	Aggregating data for report	√	√	
(A) phIpIdentityMaster	Merge IP Identity info	√		
(A) phIpIdentityWorker	Collecting IP Identity info	√	√	
(S) Apache	Receive event/svn file from collector	√	√	

System Structure

- Saas to AOSP(Service Provider)
  - What is SP?
  - Why SP?
- Challenge
  - Multiple Customer
  - Large Scale of Data
  - Complex Customer Environment

Nightmare of CustId Starts Here

System Structure – AOSP

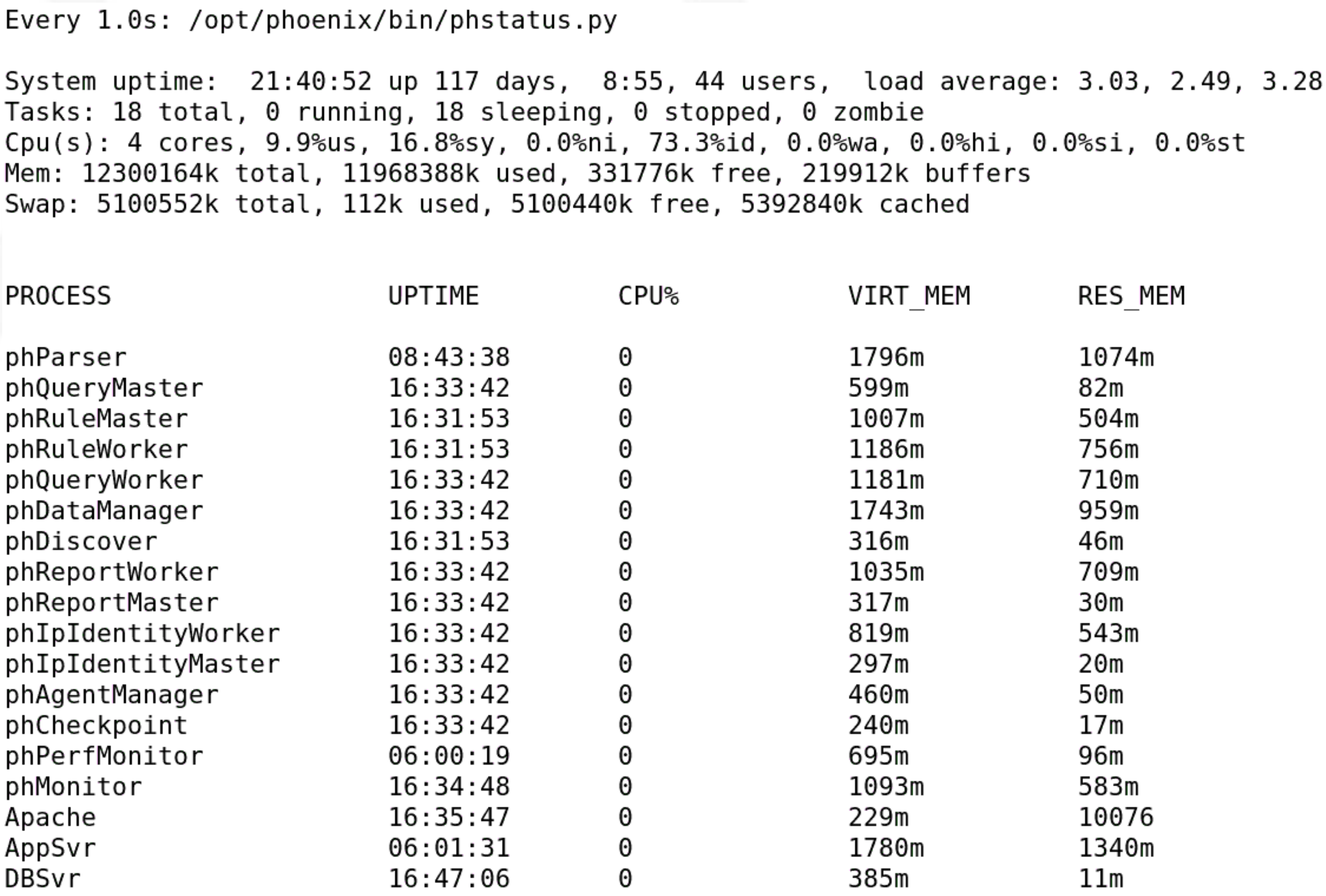


System Structure – Processes on AOSP

Process	Function	Sp	Wk	Co
phMonitor	Monitoring other processes	√	√	√
(P) phDiscover	Pulling basic data from target	√		√
(P) phPerfMonitor	Execute performance job	√	√	√
(P) phAgentManager	Execute event pulling job	√	√	√
(P) phCheckpoint	Execute checkpoint monitoring	√	√	√
(S) phParser	Parsing event to shared store (SS)	√	√	√
(S) phEventPackage	Uploading event/svn file to super/worker			√
(S) phDataManager	Save event from SS to Event DB	√	√	
(A) phRuleMaster	Decide if rule fire	√		
(A) phRuleWorker	Aggregating data for rule	√	√	
(A) phQueryMaster	Merge data from queryWorker	√		
(A) phQueryWorker	Execute query task	√	√	
(A) phReportMaster	Merge data from reportWorker	√		
(A) phReportWorker	Aggregating data for report	√	√	
(A) phIpIdentityMaster	Merge IP Identity info	√		
(A) phIpIdentityWorker	Collecting IP Identity info	√	√	
(S) Apache	Receive event/svn file from collector	√	√	

System Structure – Processes on SaaS

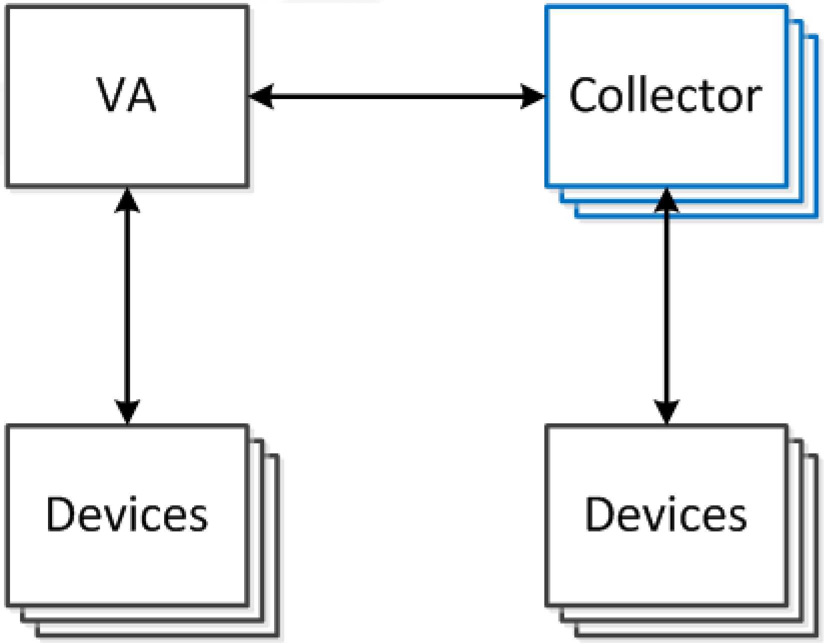
- phstatus



```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  21:40:52 up 117 days,  8:55, 44 users,  load average: 3.03, 2.49, 3.28
Tasks: 18 total, 0 running, 18 sleeping, 0 stopped, 0 zombie
Cpu(s): 4 cores, 9.9%us, 16.8%sy, 0.0%ni, 73.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 12300164k total, 11968388k used, 331776k free, 219912k buffers
Swap: 5100552k total, 112k used, 5100440k free, 5392840k cached


PROCESS                  UPTIME         CPU%           VIRT_MEM       RES_MEM

phParser                 08:43:38       0              1796m          1074m
phQueryMaster            16:33:42       0              599m           82m
phRuleMaster             16:31:53       0              1007m          504m
phRuleWorker             16:31:53       0              1186m          756m
phQueryWorker            16:33:42       0              1181m          710m
phDataManager            16:33:42       0              1743m          959m
phDiscover               16:31:53       0              316m           46m
phReportWorker           16:33:42       0              1035m          709m
phReportMaster           16:33:42       0              317m           30m
phIpIdentityWorker       16:33:42       0              819m           543m
phIpIdentityMaster       16:33:42       0              297m           20m
phAgentManager           16:33:42       0              460m           50m
phCheckpoint             16:33:42       0              240m           17m
phPerfMonitor            06:00:19       0              695m           96m
phMonitor                16:34:48       0              1093m          583m
Apache                   16:35:47       0              229m           10076
AppSvr                   06:01:31       0              1780m          1340m
DBSvr                    16:47:06       0              385m           11m
```

System Structure – VA with Collector

- Solution for enterprise with multiple location
  - One customer only
  - Multiple internal networks



Device Monitor

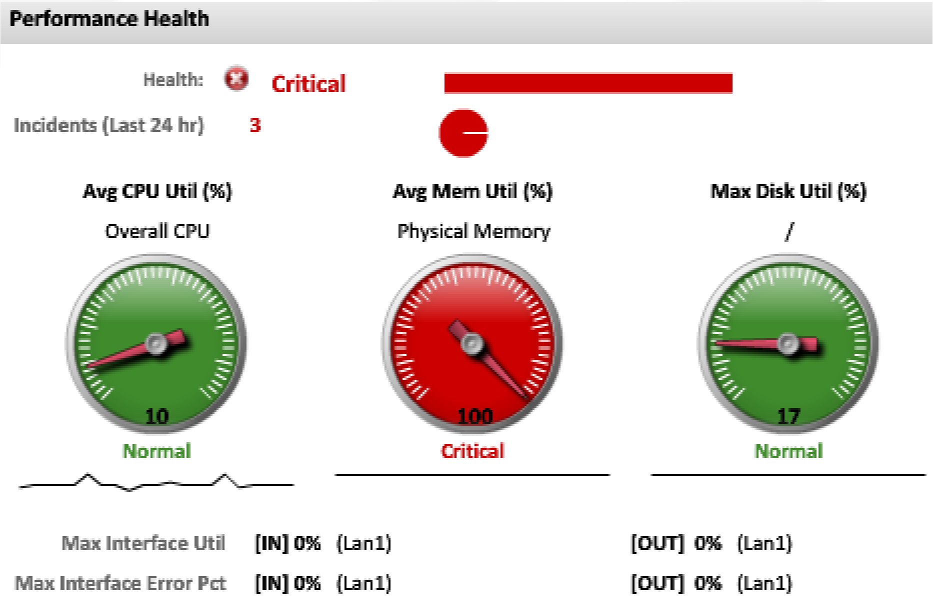
- Answering
  - What is it? (Discover – SQL DB)
  - What the status of it? (Performance Monitoring, STM – Event DB, SVN Server)
  - What is it telling us? (Event Pulling – Event DB)
- Basic Idea
  - No agent on target
  - Stable info and rapidly changed info
  - Device based

Device Monitor

- Stable Info (SQL DB)
  - Hostname
  - Hardware
  - Relationship
  - Network connectivity
- Rapidly Changed Info (Event DB)
  - Uptime
  - Availability
  - CPU, MEM, INTF Utility
  - Processes Utility

Device Monitor

- Device Monitor
  - Has IP Address
  - Application is installed in device
  - Device relationship is on topology
  - Incident with target IP



Performance Health

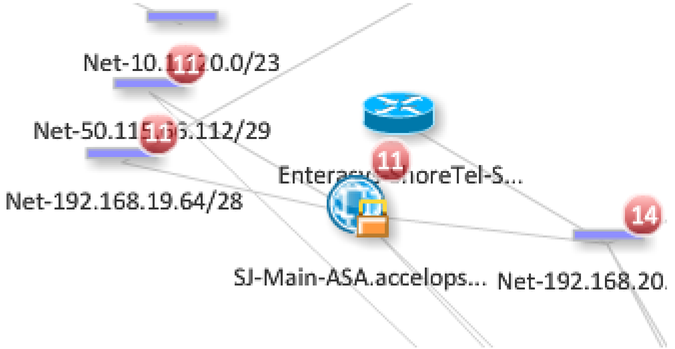
Health: Critical

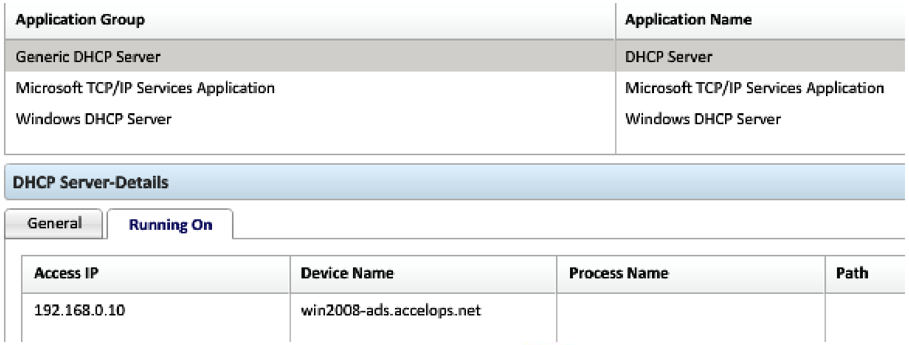
Incidents (Last 24 hr) 3

Avg CPU Util (%)	Avg Mem Util (%)	Max Disk Util (%)
Overall CPU	Physical Memory	/
10	100	17
Normal	Critical	Normal

Max Interface Util [IN] 0% (Lan1) [OUT] 0% (Lan1)

Max Interface Error Pct [IN] 0% (Lan1) [OUT] 0% (Lan1)





Application Group	Application Name
Generic DHCP Server	DHCP Server
Microsoft TCP/IP Services Application	Microsoft TCP/IP Services Application
Windows DHCP Server	Windows DHCP Server

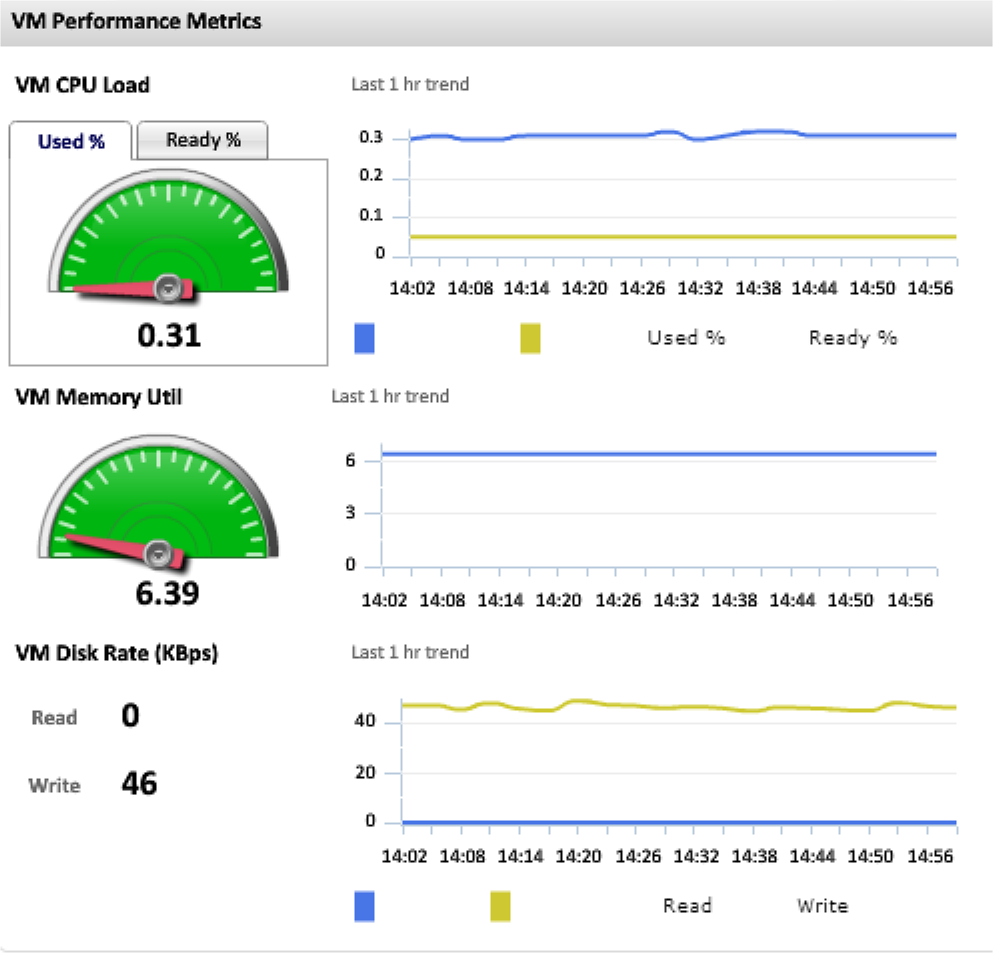
DHCP Server-Details

General | Running On

Access IP	Device Name	Process Name	Path
192.168.0.10	win2008-ads.accelops.net		

Device Monitor

- Service Monitoring
  - VM monitoring



VM Performance Metrics

VM CPU Load

Used % | Ready %

0.31

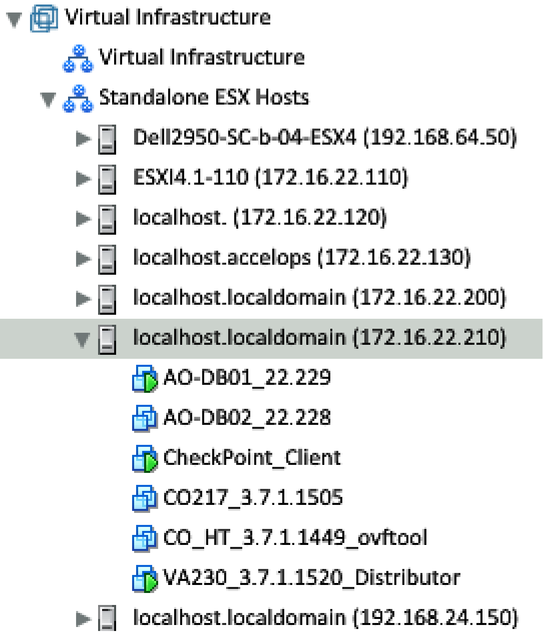
VM Memory Util

6.39

VM Disk Rate (KBps)

Read 0

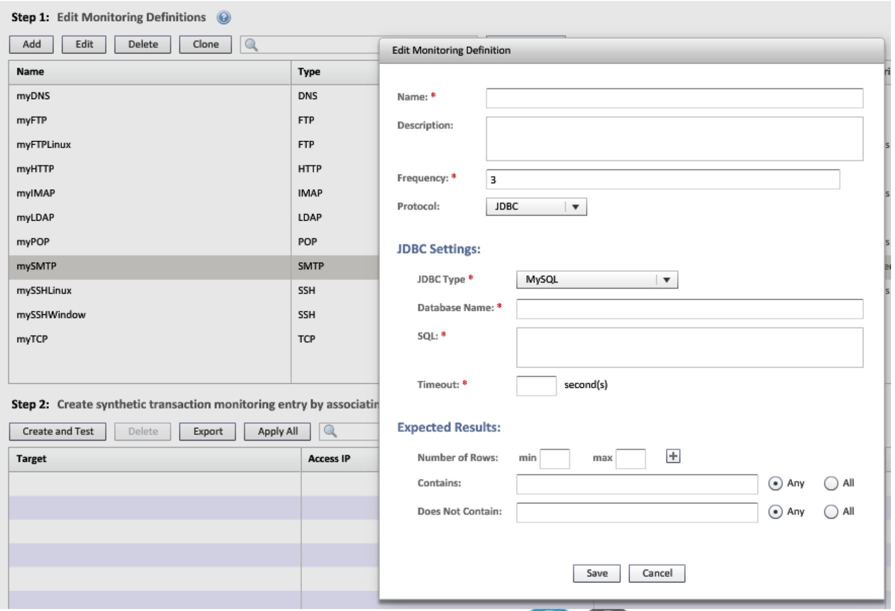
Write 46



- ▼ Virtual Infrastructure
  - Virtual Infrastructure
  - ▼ Standalone ESX Hosts
    - ▶ Dell2950-SC-b-04-ESX4 (192.168.64.50)
    - ▶ ESXI4.1-110 (172.16.22.110)
    - ▶ localhost. (172.16.22.120)
    - ▶ localhost.accelops (172.16.22.130)
    - ▶ localhost.localdomain (172.16.22.200)
    - ▼ localhost.localdomain (172.16.22.210)
      - AO-DB01_22.229
      - AO-DB02_22.228
      - CheckPoint_Client
      - CO217_3.7.1.1505
      - CO_HT_3.7.1.1449_ovftool
      - VA230_3.7.1.1520_Distributor
    - ▶ localhost.localdomain (192.168.24.150)

Device Monitor

- Service Monitoring
  - Application only monitoring
    - LDAP
    - Nessus
    - Checkpoint
  - URL based monitoring
    - Qualys
    - Customer Https



Step 1: Edit Monitoring Definitions

Name	Type
myDNS	DNS
myFTP	FTP
myFTPLinux	FTP
myHTTP	HTTP
myIMAP	IMAP
myLDAP	LDAP
myPOP	POP
mySMTP	SMTP
mySSHLinux	SSH
mySSHWindow	SSH
myTCP	TCP

Step 2: Create synthetic transaction monitoring entry by associatin

Target	Access IP

Edit Monitoring Definition

Name: *
Description:
Frequency: * 3
Protocol: JDBC

JDBC Settings:

JDBC Type * MySQL
Database Name: *
SQL: *
Timeout: * second(s)

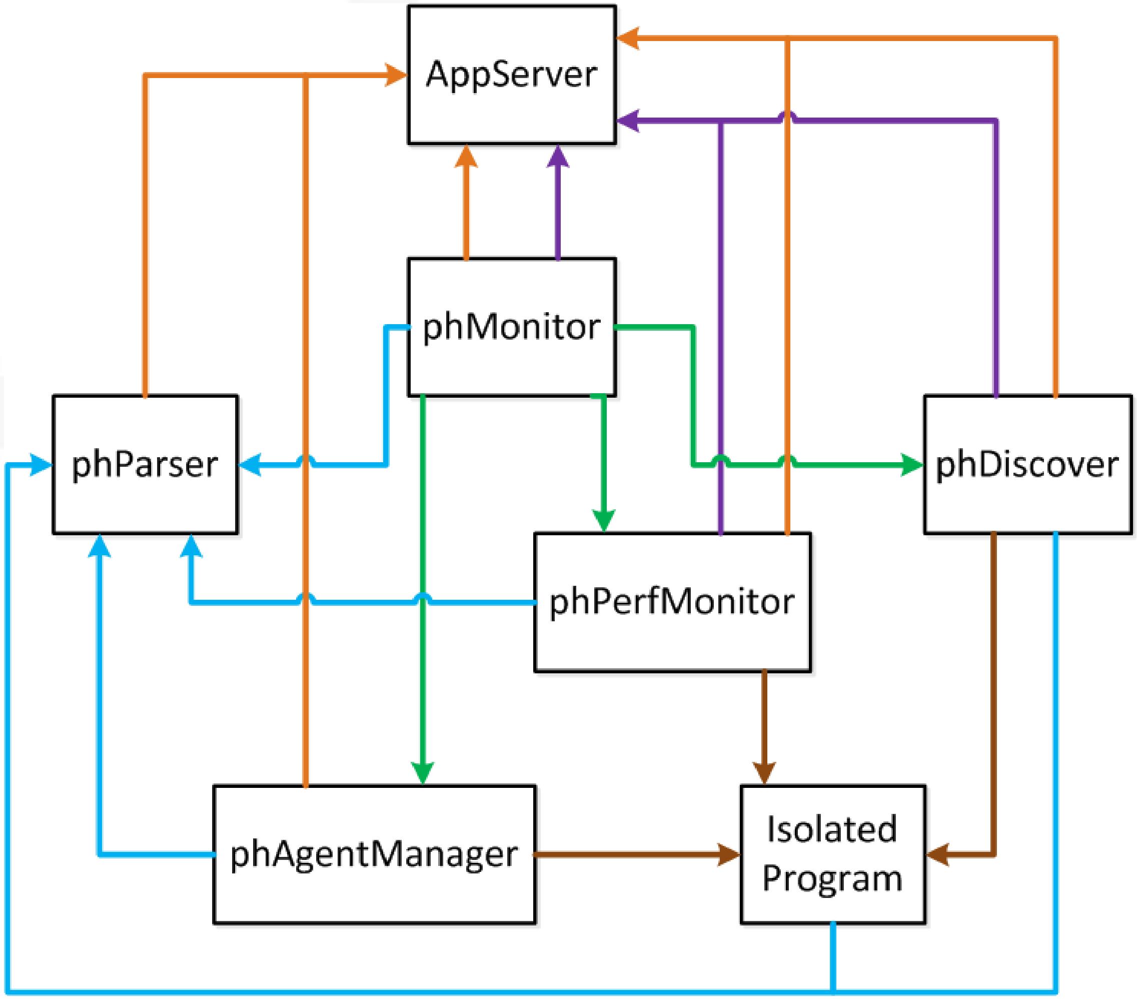
Expected Results:

Number of Rows: min max
Contains: ● Any ○ All
Does Not Contain: ● Any ○ All

Device Monitor

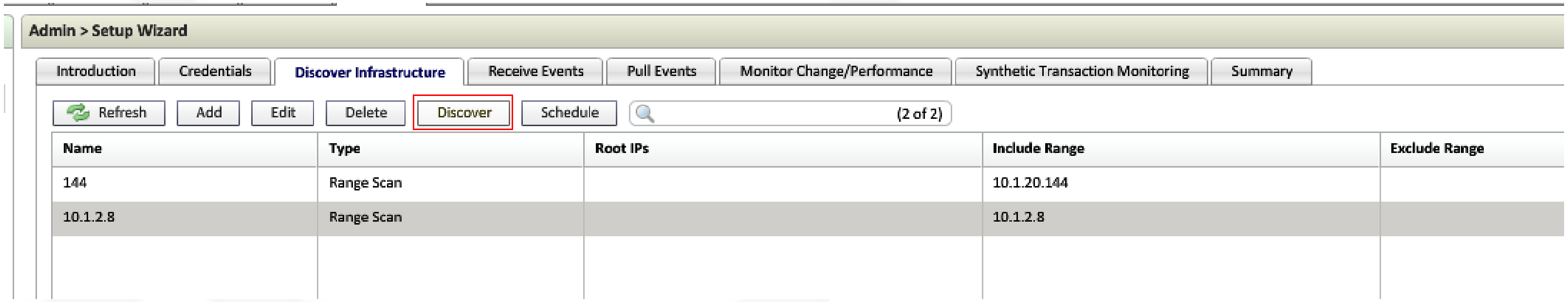
- Go Through A Discover and Monitor Case

- Http Get
- Http Post
- Socket
- LOG
- Pipe



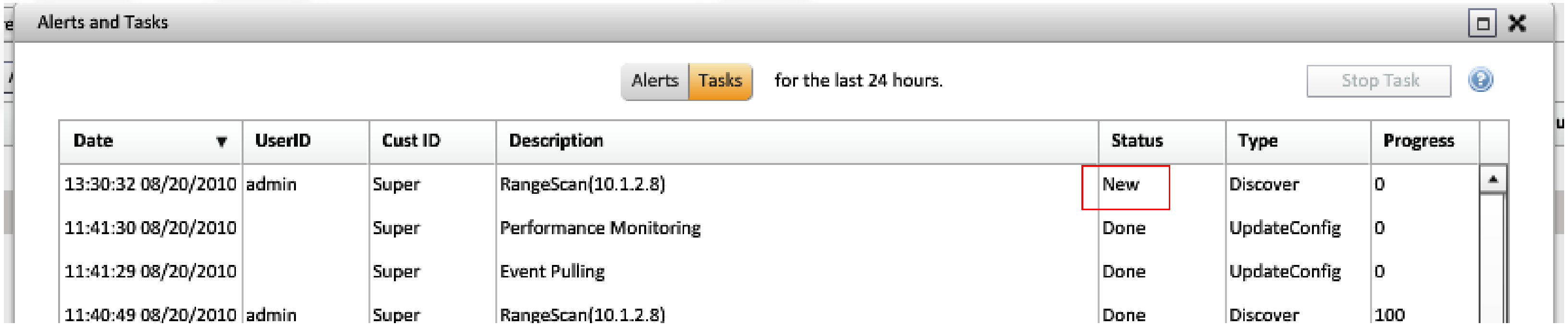
Device Monitor – Discover

- Customer click discover on GUI



Admin > Setup Wizard

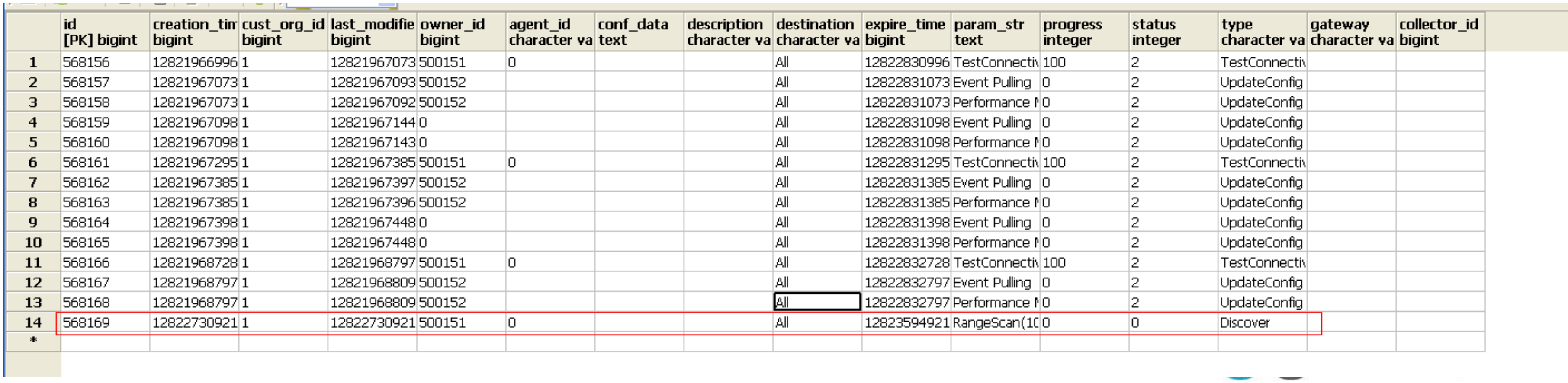
Name	Type	Root IPs	Include Range	Exclude Range
144	Range Scan		10.1.20.144	
10.1.2.8	Range Scan		10.1.2.8	



Alerts and Tasks

for the last 24 hours.

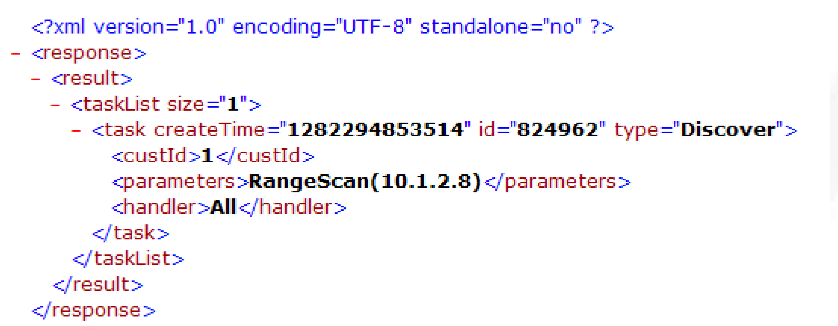
Date	UserID	Cust ID	Description	Status	Type	Progress
13:30:32 08/20/2010	admin	Super	RangeScan(10.1.2.8)	New	Discover	0
11:41:30 08/20/2010		Super	Performance Monitoring	Done	UpdateConfig	0
11:41:29 08/20/2010		Super	Event Pulling	Done	UpdateConfig	0
11:40:49 08/20/2010	admin	Super	RangeScan(10.1.2.8)	Done	Discover	100



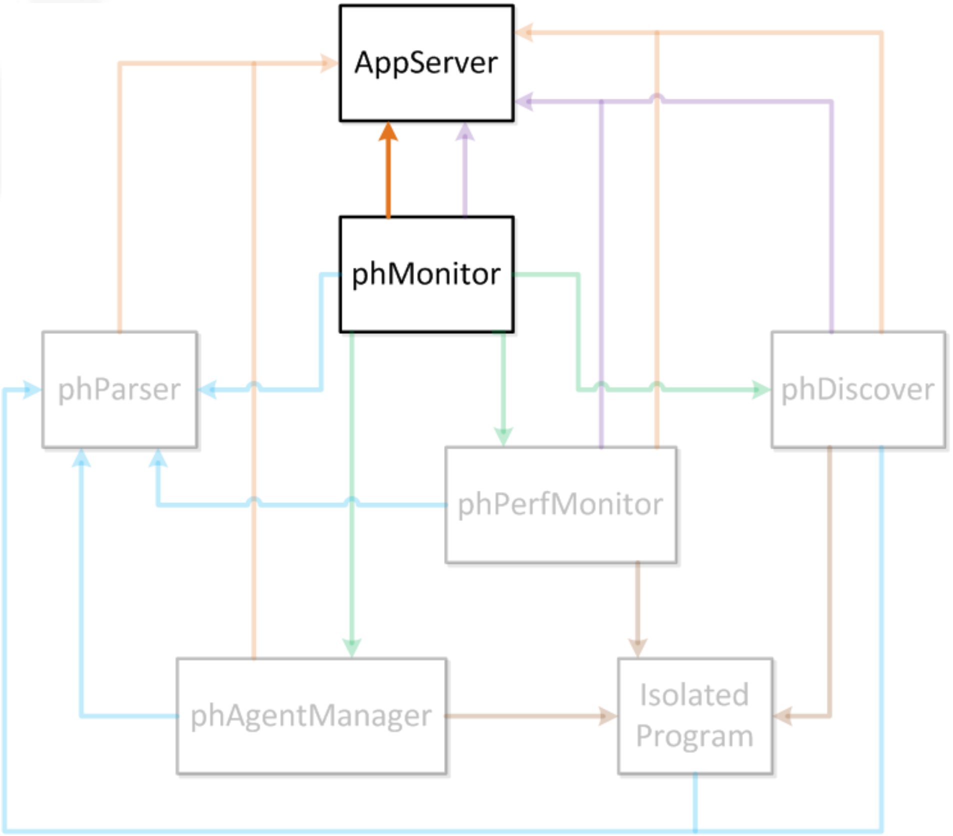
	id [PK] bigint	creation_tim bigint	cust_org_id bigint	last_modifie bigint	owner_id bigint	agent_id character va	conf_data text	description character va	destination character va	expire_time bigint	param_str text	progress integer	status integer	type character va	gateway character va	collector_id bigint
1	568156	12821966996	1	12821967073	500151	0			All	12822830996	TestConnecti	100	2	TestConnecti		
2	568157	12821967073	1	12821967093	500152				All	12822831073	Event Pulling	0	2	UpdateConfig		
3	568158	12821967073	1	12821967092	500152				All	12822831073	Performance M	0	2	UpdateConfig		
4	568159	12821967098	1	12821967144	0				All	12822831098	Event Pulling	0	2	UpdateConfig		
5	568160	12821967098	1	12821967143	0				All	12822831098	Performance M	0	2	UpdateConfig		
6	568161	12821967295	1	12821967385	500151	0			All	12822831295	TestConnecti	100	2	TestConnecti		
7	568162	12821967385	1	12821967397	500152				All	12822831385	Event Pulling	0	2	UpdateConfig		
8	568163	12821967385	1	12821967396	500152				All	12822831385	Performance M	0	2	UpdateConfig		
9	568164	12821967398	1	12821967448	0				All	12822831398	Event Pulling	0	2	UpdateConfig		
10	568165	12821967398	1	12821967448	0				All	12822831398	Performance M	0	2	UpdateConfig		
11	568166	12821968728	1	12821968797	500151	0			All	12822832728	TestConnecti	100	2	TestConnecti		
12	568167	12821968797	1	12821968809	500152				All	12822832797	Event Pulling	0	2	UpdateConfig		
13	568168	12821968797	1	12821968809	500152				All	12822832797	Performance M	0	2	UpdateConfig		
14	568169	12822730921	1	12822730921	500151	0			All	12823594921	RangeScan(10	0	0	Discover		
*																

Device Monitor – Discover

- phMonitor periodically asking for new task from App Server(Http Get)



```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <response>
  - <result>
    - <taskList size="1">
      - <task createTime="1282294853514" id="824962" type="Discover">
          <custId>1</custId>
          <parameters>RangeScan(10.1.2.8)</parameters>
          <handler>All</handler>
        </task>
      </taskList>
    </result>
  </response>
```

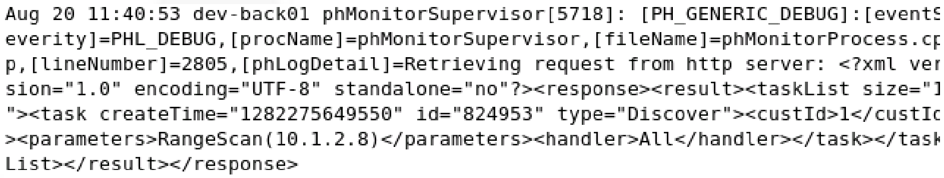


Why not send out task by App Server?

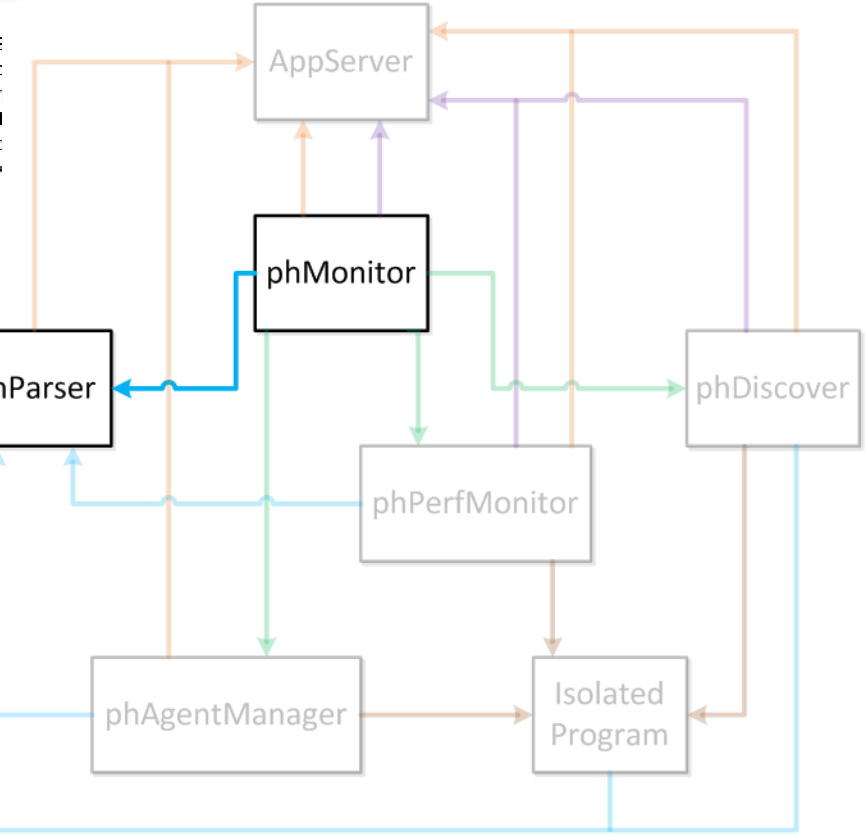
Rest API: https://192.168.20.116/phoenix/rest/sync/task?custId=1&agentId=1

Device Monitor – Discover

- phMonitor logged task list to phParser (LOG)



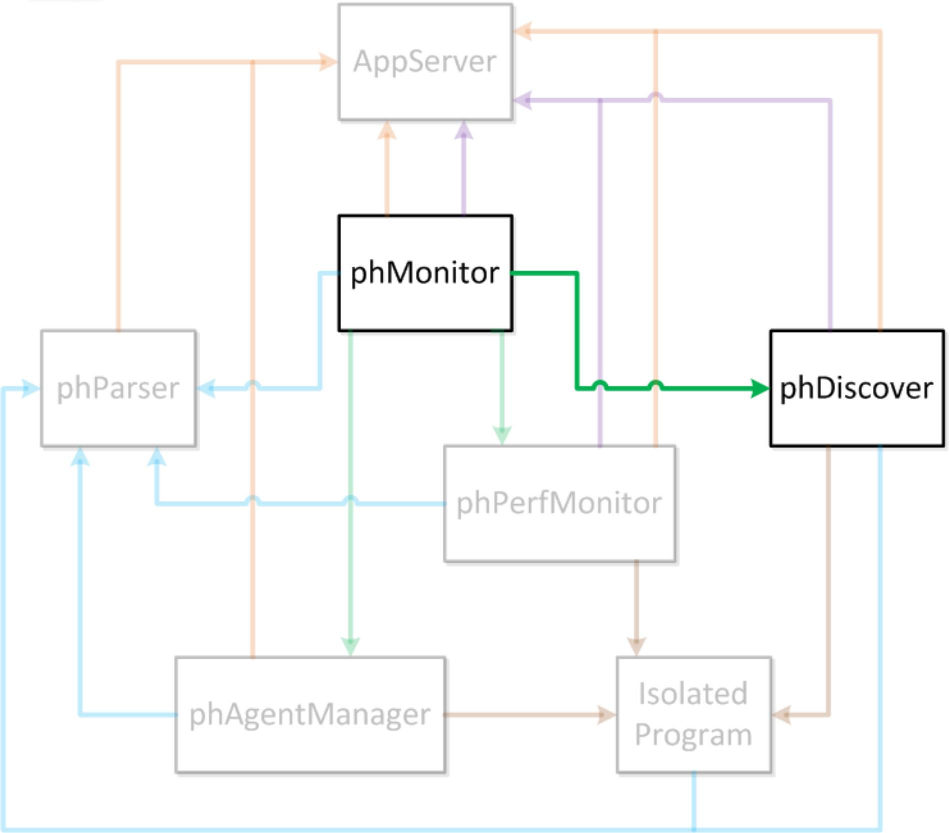
```
Aug 20 11:40:53 dev-back01 phMonitorSupervisor[5718]: [PH_GENERIC_DEBUG]:[eventS
everity]=PHL_DEBUG,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cp
p,[lineNumber]=2805,[phLogDetail]=Retrieving request from http server: <?xml ver
sion="1.0" encoding="UTF-8" standalone="no"?><response><result><taskList size="1
"><task createTime="1282275649550" id="824953" type="Discover"><custId>1</custId
><parameters>RangeScan(10.1.2.8)</parameters><handler>All</handler></task></task
List></result></response>
```



Device Monitor – Discover

- phMonitor send task to phDiscover (Socket)
  - Command Port
  - Command Id
  - Callback

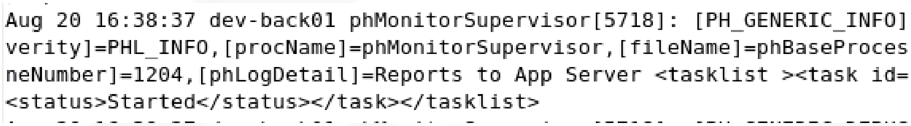
Process	Port
phMonitor	7900
phDiscover	7928
phPerfMonitor	7942
phParser	7914
phAgentManager	7926
phQueryMaster	7918



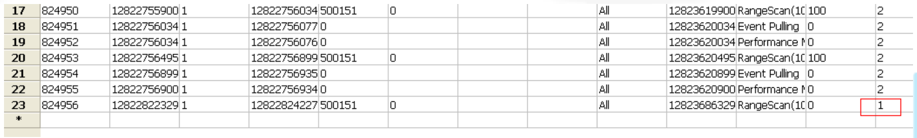
File:/opt/phoenix/config/phoenix_config.txt

Device Monitor – Discover

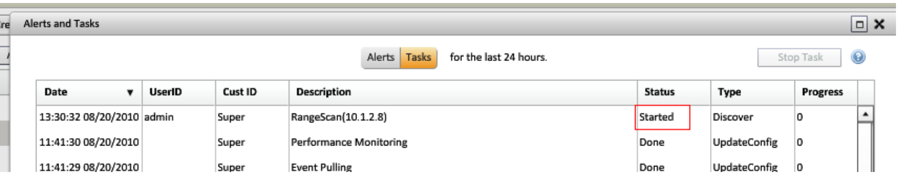
- phMonitor update task status
  - To App Server (Http Post)
  - To phParser (LOG)



```
Aug 20 16:38:37 dev-back01 phMonitorSupervisor[5718]: [PH_GENERIC_INFO]:[eventSe
verity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phBaseProcess.cpp,[li
neNumber]=1204,[phLogDetail]=Reports to App Server <tasklist ><task id='824959'>
<status>Started</status></task></tasklist>
```

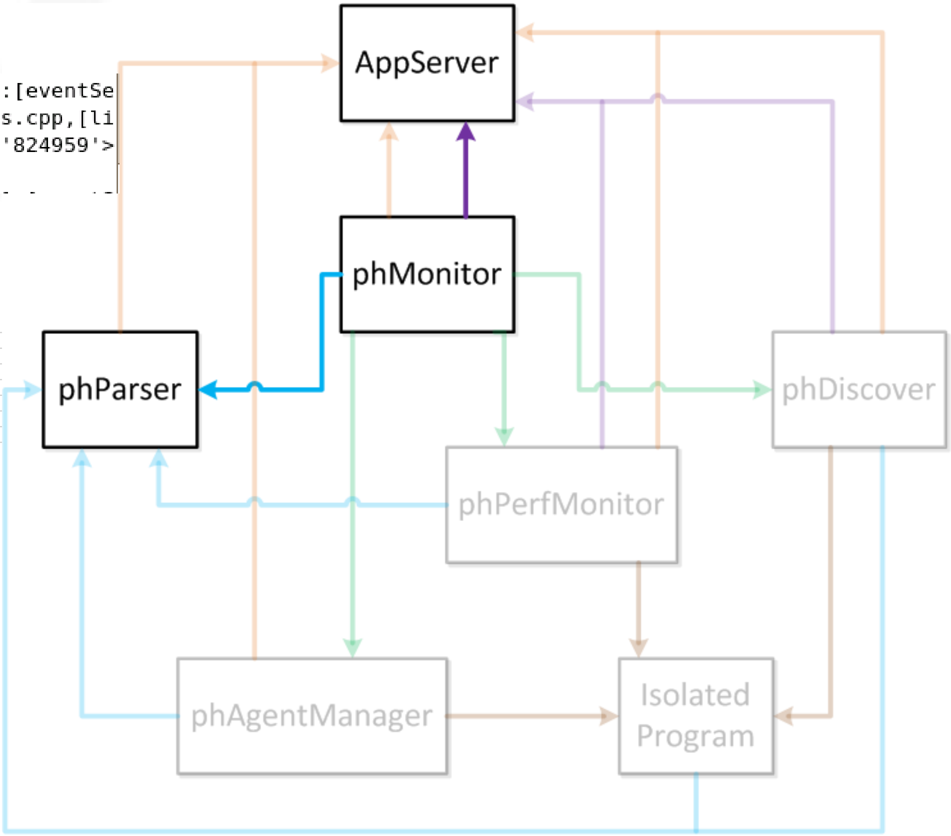


17	824950	12822755900	1	12822756034	500151	0			All	12823619900	RangeScan(1(	100	2
18	824951	12822756034	1	12822756077	0				All	12823620034	Event Pulling	0	2
19	824952	12822756034	1	12822756076	0				All	12823620034	Performance I	0	2
20	824953	12822756495	1	12822756899	500151	0			All	12823620495	RangeScan(1(	100	2
21	824954	12822756899	1	12822756935	0				All	12823620899	Event Pulling	0	2
22	824955	12822756900	1	12822756934	0				All	12823620900	Performance I	0	2
23	824956	12822822329	1	12822824227	500151	0			All	12823686329	RangeScan(1(	0	1
*													



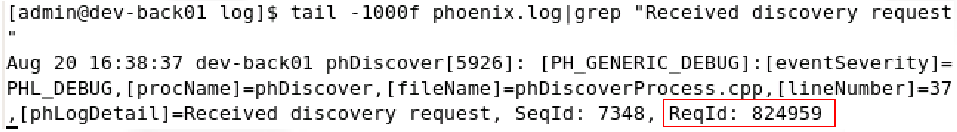
for the last 24 hours.

Date ▼	UserID	Cust ID	Description	Status	Type	Progress
13:30:32 08/20/2010	admin	Super	RangeScan(10.1.2.8)	Started	Discover	0
11:41:30 08/20/2010		Super	Performance Monitoring	Done	UpdateConfig	0
11:41:29 08/20/2010		Super	Event Pulling	Done	UpdateConfig	0



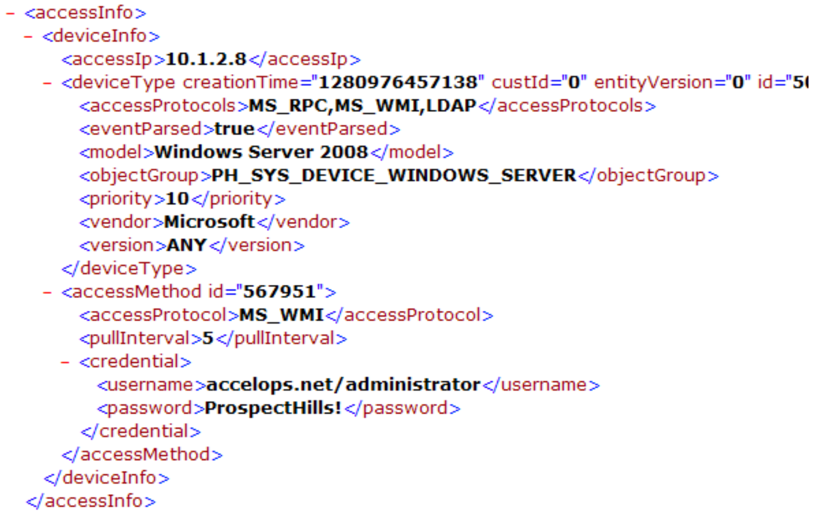
Device Monitor – Discover

- phDiscover log received task to phParser(LOG)

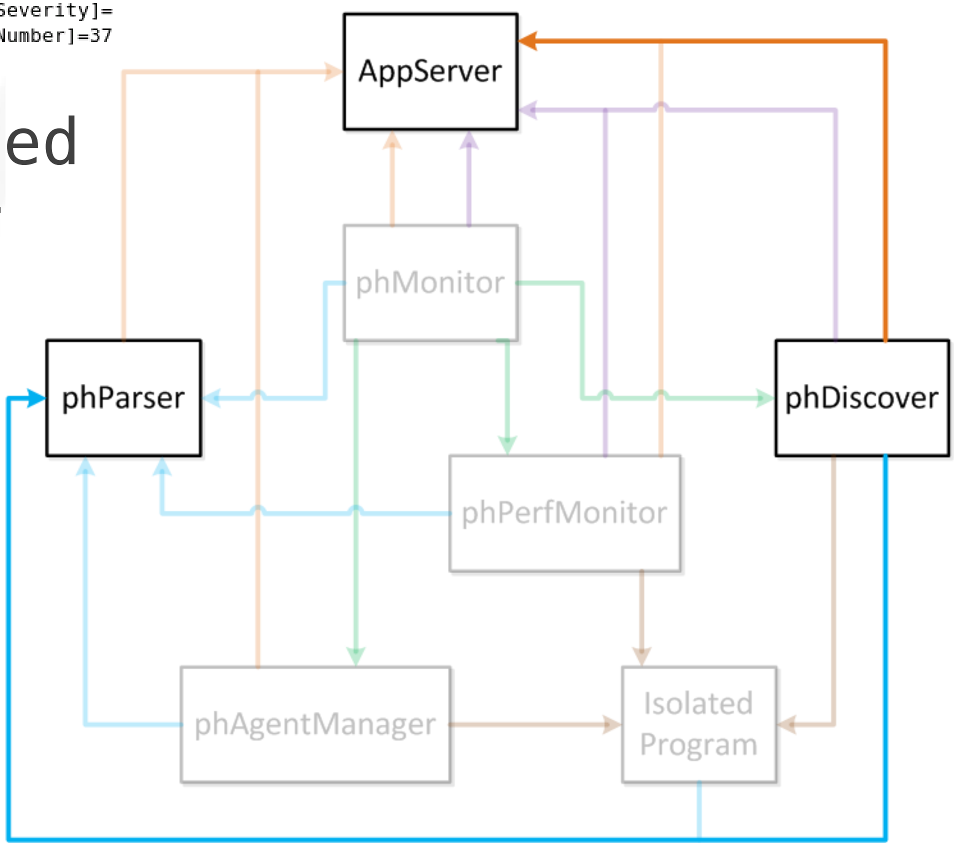


```
[admin@dev-back01 log]$ tail -1000f phoenix.log|grep "Received discovery request
"
Aug 20 16:38:37 dev-back01 phDiscover[5926]: [PH_GENERIC_DEBUG]:[eventSeverity]=
PHL_DEBUG,[procName]=phDiscover,[fileName]=phDiscoverProcess.cpp,[lineNumber]=37
,[phLogDetail]=Received discovery request, SeqId: 7348, ReqId: 824959
```

- phDiscover get related info from App Server (Http Get)



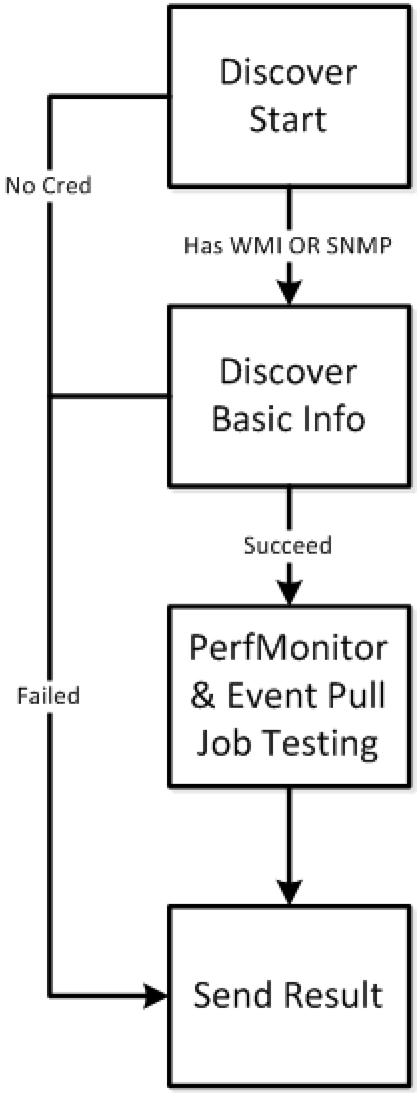
```
- <accessInfo>
  - <deviceInfo>
      <accessIp>10.1.2.8</accessIp>
    - <deviceType creationTime="1280976457138" custId="0" entityVersion="0" id="5
        <accessProtocols>MS_RPC,MS_WMI,LDAP</accessProtocols>
        <eventParsed>true</eventParsed>
        <model>Windows Server 2008</model>
        <objectGroup>PH_SYS_DEVICE_WINDOWS_SERVER</objectGroup>
        <priority>10</priority>
        <vendor>Microsoft</vendor>
        <version>ANY</version>
      </deviceType>
    - <accessMethod id="567951">
        <accessProtocol>MS_WMI</accessProtocol>
        <pullInterval>5</pullInterval>
      - <credential>
          <username>accelops.net/administrator</username>
          <password>ProspectHills!</password>
        </credential>
      </accessMethod>
    </deviceInfo>
  </accessInfo>
```



Rest API: https://192.168.20.116/phoenix/rest/deviceInfo/discovery
?taskId=565361&custId=1&agentId=1

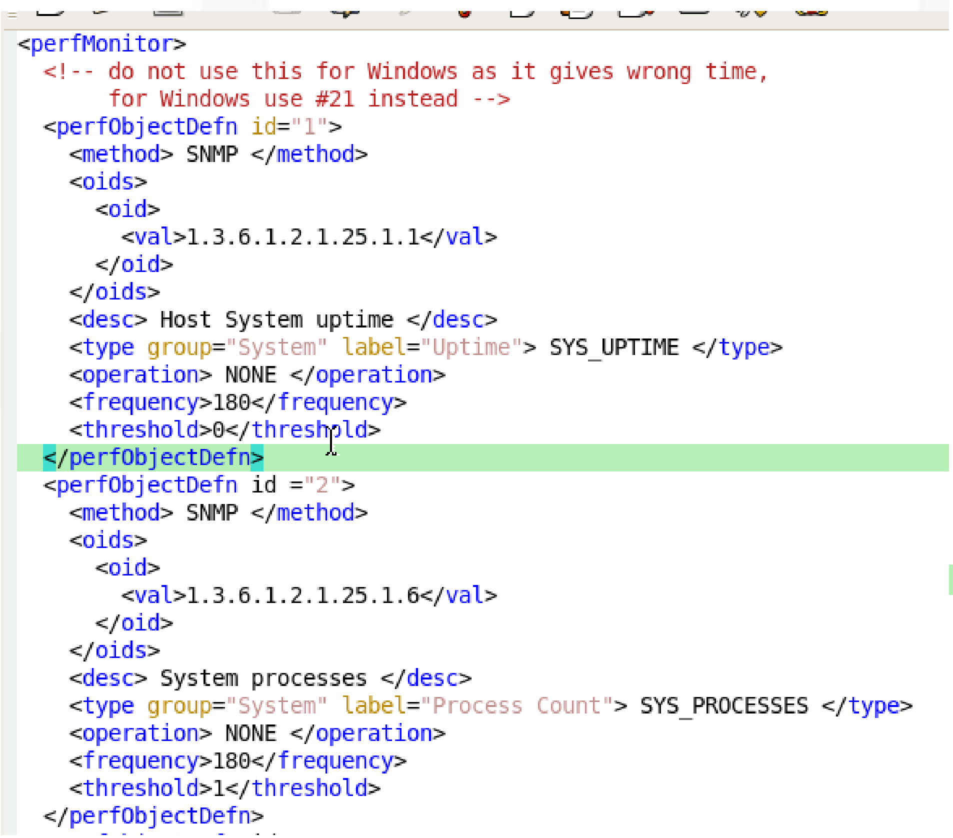
Device Monitor – Discover

- Work Flow of Discover
  - Typical
    - SNMP (snmpwalk)
    - WMI (wmic)
  - Exceptions
    - LDAP
    - PING
    - CHECKPOINT
    - AWS
    - UCS
    - ……

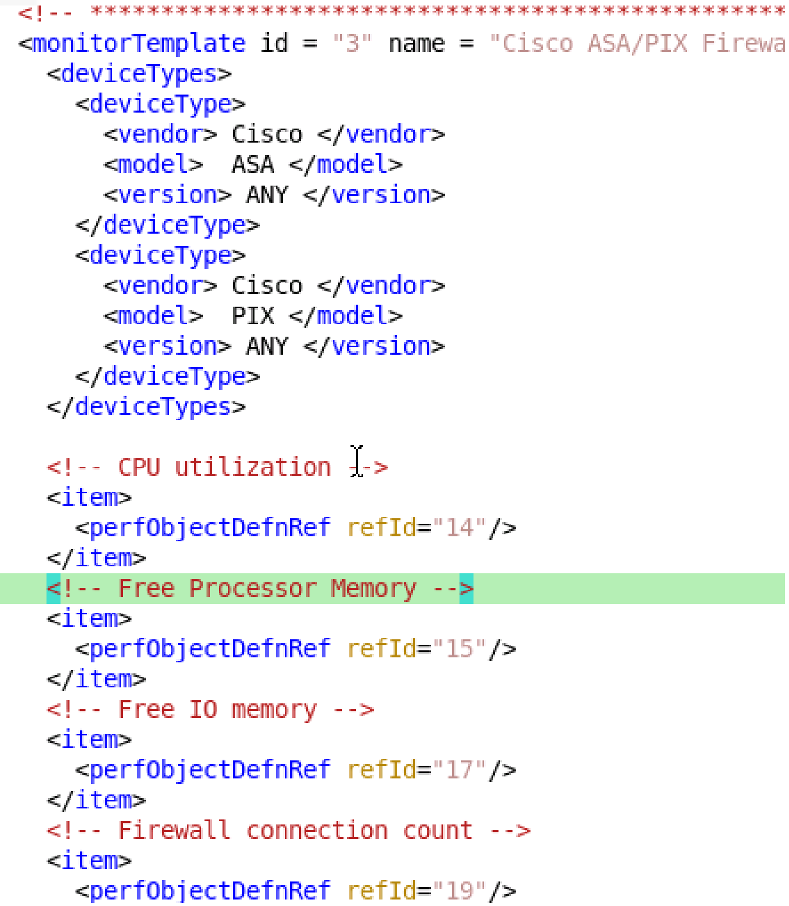


Device Monitor – Discover

- Predefined Performance Job



```
<perfMonitor>
  <!-- do not use this for Windows as it gives wrong time,
       for Windows use #21 instead -->
  <perfObjectDefn id="1">
    <method> SNMP </method>
    <oids>
      <oid>
        <val>1.3.6.1.2.1.25.1.1</val>
      </oid>
    </oids>
    <desc> Host System uptime </desc>
    <type group="System" label="Uptime"> SYS_UPTIME </type>
    <operation> NONE </operation>
    <frequency>180</frequency>
    <threshold>0</threshold>
  </perfObjectDefn>
  <perfObjectDefn id ="2">
    <method> SNMP </method>
    <oids>
      <oid>
        <val>1.3.6.1.2.1.25.1.6</val>
      </oid>
    </oids>
    <desc> System processes </desc>
    <type group="System" label="Process Count"> SYS_PROCESSES </type>
    <operation> NONE </operation>
    <frequency>180</frequency>
    <threshold>1</threshold>
  </perfObjectDefn>
```



```
<!-- *************************************************
<monitorTemplate id = "3" name = "Cisco ASA/PIX Firewa
  <deviceTypes>
    <deviceType>
      <vendor> Cisco </vendor>
      <model>  ASA </model>
      <version> ANY </version>
    </deviceType>
    <deviceType>
      <vendor> Cisco </vendor>
      <model>  PIX </model>
      <version> ANY </version>
    </deviceType>
  </deviceTypes>

  <!-- CPU utilization -->
  <item>
    <perfObjectDefnRef refId="14"/>
  </item>
  <!-- Free Processor Memory -->
  <item>
    <perfObjectDefnRef refId="15"/>
  </item>
  <!-- Free IO memory -->
  <item>
    <perfObjectDefnRef refId="17"/>
  </item>
  <!-- Firewall connection count -->
  <item>
    <perfObjectDefnRef refId="19"/>
```

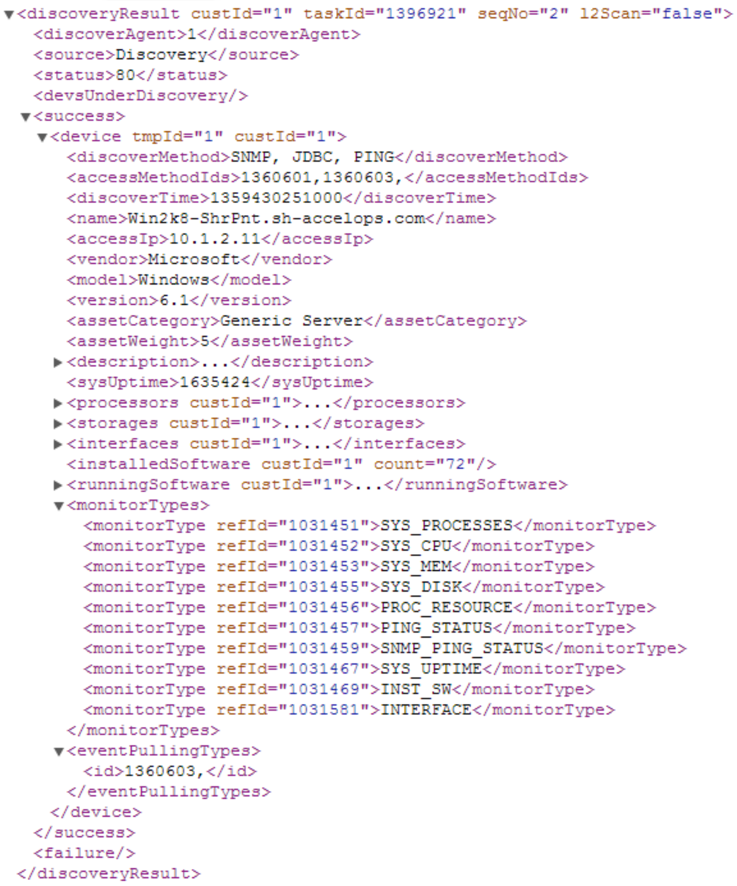
File:/opt/phoenix/data-definition/PerfMonitorTemplate.xml

Device Monitor – Discover

- Predefined Event Pulling Job
  - Type
    - Cisco SDEE
    - JDBC
    - Checkpoint
    - Nessus
    - ……
  - Difference with Performance Job
    - SIEM and PAM
    - Predefine Matrix and Unknown Scale Data

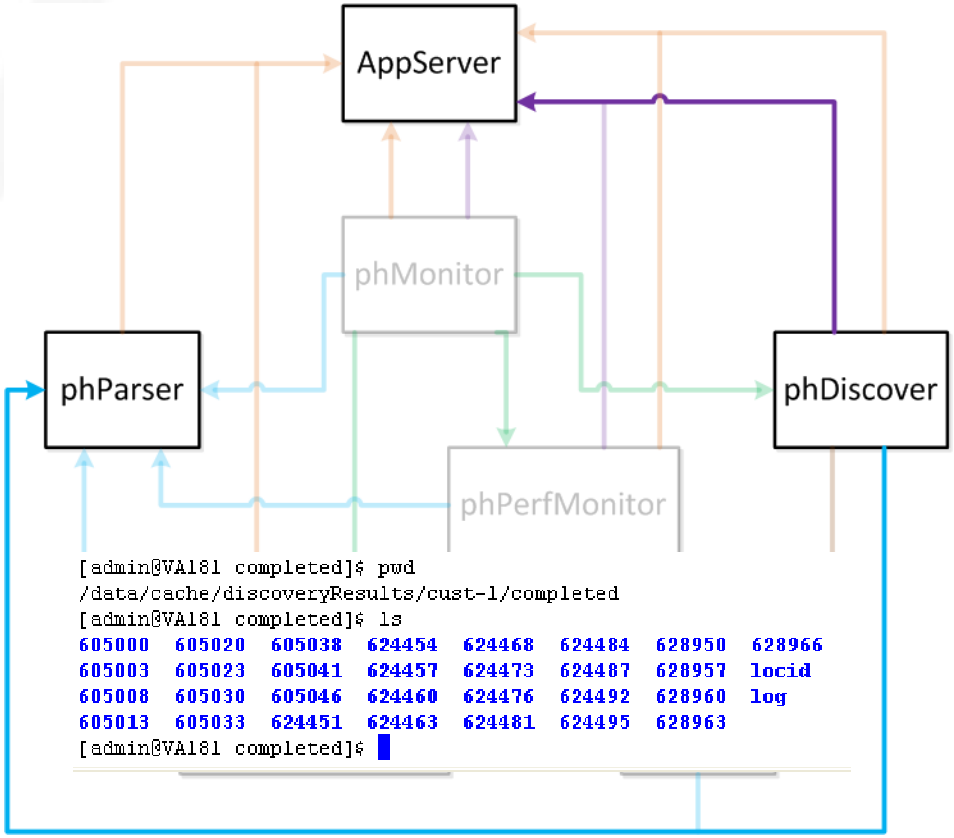
Device Monitor – Discover

- phDiscover output result
  - To App Server (Http Post)
  - To phParser (LOG)



```
▼<discoveryResult custId="1" taskId="1396921" seqNo="2" l2Scan="false">
   <discoverAgent>1</discoverAgent>
   <source>Discovery</source>
   <status>80</status>
   <devsUnderDiscovery/>
 ▼<success>
   ▼<device tmpId="1" custId="1">
       <discoverMethod>SNMP, JDBC, PING</discoverMethod>
       <accessMethodIds>1360601,1360603,</accessMethodIds>
       <discoverTime>1359430251000</discoverTime>
       <name>Win2k8-ShrPnt.sh-accelops.com</name>
       <accessIp>10.1.2.11</accessIp>
       <vendor>Microsoft</vendor>
       <model>Windows</model>
       <version>6.1</version>
       <assetCategory>Generic Server</assetCategory>
       <assetWeight>5</assetWeight>
     ▶<description>...</description>
       <sysUptime>1635424</sysUptime>
     ▶<processors custId="1">...</processors>
     ▶<storages custId="1">...</storages>
     ▶<interfaces custId="1">...</interfaces>
       <installedSoftware custId="1" count="72"/>
     ▶<runningSoftware custId="1">...</runningSoftware>
     ▼<monitorTypes>
         <monitorType refId="1031451">SYS_PROCESSES</monitorType>
         <monitorType refId="1031452">SYS_CPU</monitorType>
         <monitorType refId="1031453">SYS_MEM</monitorType>
         <monitorType refId="1031455">SYS_DISK</monitorType>
         <monitorType refId="1031456">PROC_RESOURCE</monitorType>
         <monitorType refId="1031457">PING_STATUS</monitorType>
         <monitorType refId="1031459">SNMP_PING_STATUS</monitorType>
         <monitorType refId="1031467">SYS_UPTIME</monitorType>
         <monitorType refId="1031469">INST_SW</monitorType>
         <monitorType refId="1031581">INTERFACE</monitorType>
       </monitorTypes>
     ▼<eventPullingTypes>
         <id>1360603,</id>
       </eventPullingTypes>
     </device>
   </success>
   <failure/>
 </discoveryResult>
```

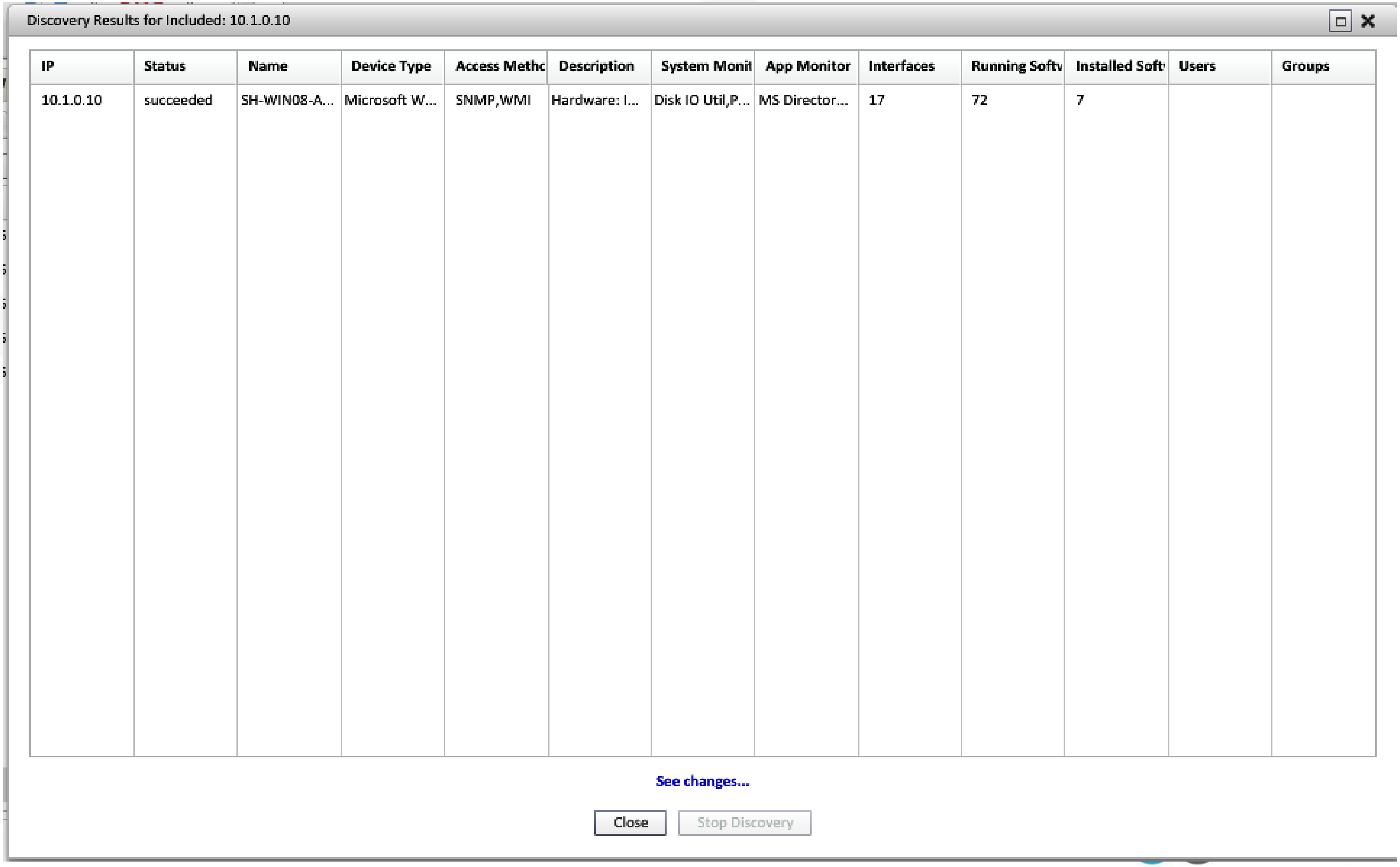
File:/data/cache/discoveryResult/cust-1/completed



```
[admin@VA181 completed]$ pwd
/data/cache/discoveryResults/cust-1/completed
[admin@VA181 completed]$ ls
605000  605020  605038  624454  624468  624484  628950  628966
605003  605023  605041  624457  624473  624487  628957  locid
605008  605030  605046  624460  624476  624492  628960  log
605013  605033  624451  624463  624481  624495  628963
[admin@VA181 completed]$ 
```

Device Monitor – Discover

- Discover Succeed!

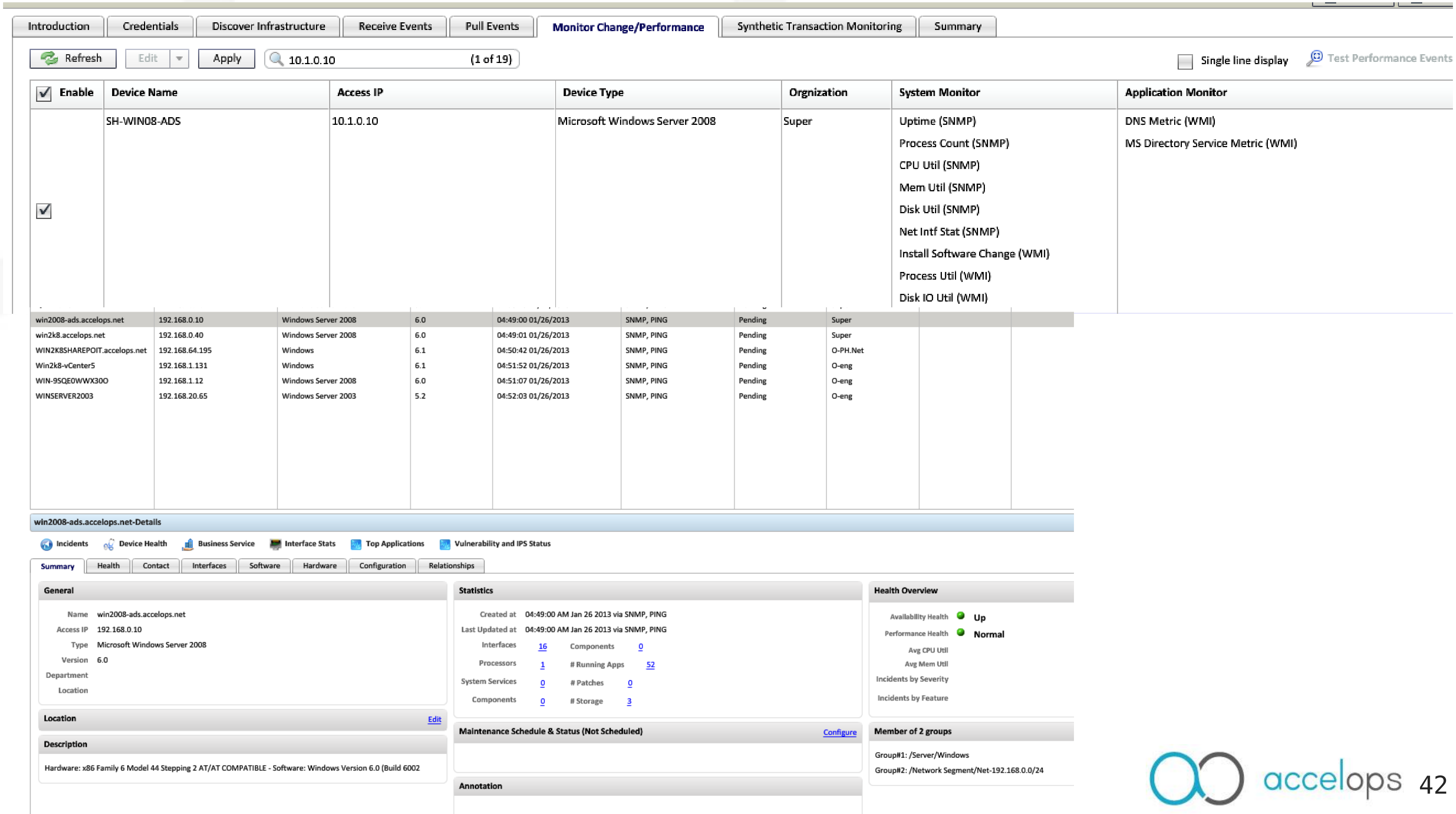


Discovery Results for Included: 10.1.0.10

IP	Status	Name	Device Type	Access Methc	Description	System Monit	App Monitor	Interfaces	Running Softv	Installed Soft	Users	Groups
10.1.0.10	succeeded	SH-WIN08-A...	Microsoft W...	SNMP,WMI	Hardware: I...	Disk IO Util,P...	MS Director...	17	72	7		

Device Monitor – Discover

- Discover Succeed!



Introduction | Credentials | Discover Infrastructure | Receive Events | Pull Events | **Monitor Change/Performance** | Synthetic Transaction Monitoring | Summary

Refresh | Edit | Apply | 10.1.0.10 (1 of 19) | □ Single line display | Test Performance Events

☑ Enable	Device Name	Access IP	Device Type	Orgnization	System Monitor	Application Monitor
☑	SH-WIN08-ADS	10.1.0.10	Microsoft Windows Server 2008	Super	Uptime (SNMP) Process Count (SNMP) CPU Util (SNMP) Mem Util (SNMP) Disk Util (SNMP) Net Intf Stat (SNMP) Install Software Change (WMI) Process Util (WMI) Disk IO Util (WMI)	DNS Metric (WMI) MS Directory Service Metric (WMI)

win2008-ads.accelops.net	192.168.0.10	Windows Server 2008	6.0	04:49:00 01/26/2013	SNMP, PING	Pending	Super
win2k8.accelops.net	192.168.0.40	Windows Server 2008	6.0	04:49:01 01/26/2013	SNMP, PING	Pending	Super
WIN2K8SHAREPOIT.accelops.net	192.168.64.195	Windows	6.1	04:50:42 01/26/2013	SNMP, PING	Pending	O-PH.Net
Win2k8-vCenter5	192.168.1.131	Windows	6.1	04:51:52 01/26/2013	SNMP, PING	Pending	O-eng
WIN-9SQE0WWX30O	192.168.1.12	Windows Server 2008	6.0	04:51:07 01/26/2013	SNMP, PING	Pending	O-eng
WINSERVER2003	192.168.20.65	Windows Server 2003	5.2	04:52:03 01/26/2013	SNMP, PING	Pending	O-eng

win2008-ads.accelops.net-Details

Incidents | Device Health | Business Service | Interface Stats | Top Applications | Vulnerability and IPS Status

Summary | Health | Contact | Interfaces | Software | Hardware | Configuration | Relationships

General

Name	win2008-ads.accelops.net
Access IP	192.168.0.10
Type	Microsoft Windows Server 2008
Version	6.0
Department	
Location	

Location Edit

Description

Hardware: x86 Family 6 Model 44 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.0 (Build 6002

Statistics

Created at	04:49:00 AM Jan 26 2013 via SNMP, PING		
Last Updated at	04:49:00 AM Jan 26 2013 via SNMP, PING		
Interfaces	16	Components	0
Processors	1	# Running Apps	52
System Services	0	# Patches	0
Components	0	# Storage	3

Maintenance Schedule & Status (Not Scheduled) Configure

Annotation

Health Overview

Availability Health	● Up
Performance Health	● Normal
Avg CPU Util	
Avg Mem Util	
Incidents by Severity	
Incidents by Feature	

Member of 2 groups

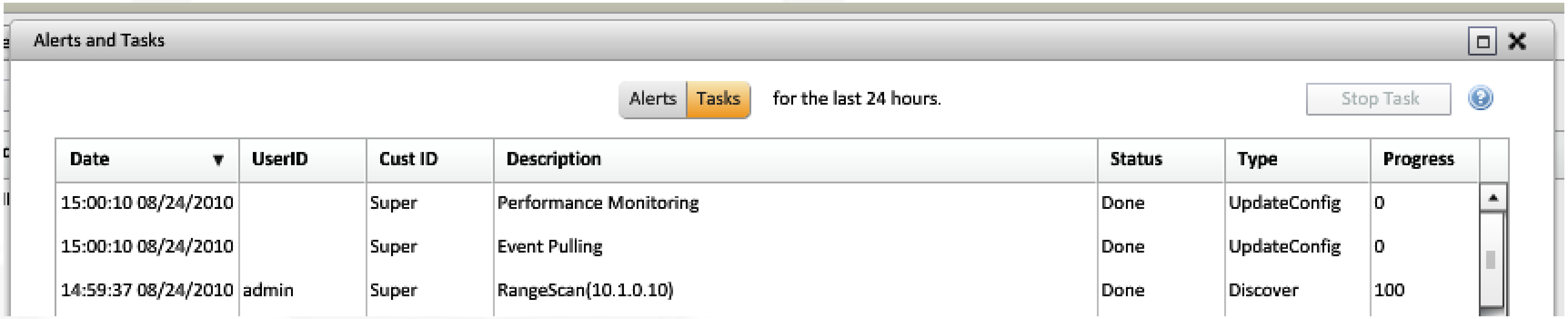
Group#1: /Server/Windows

Group#2: /Network Segment/Net-192.168.0.0/24

accelops

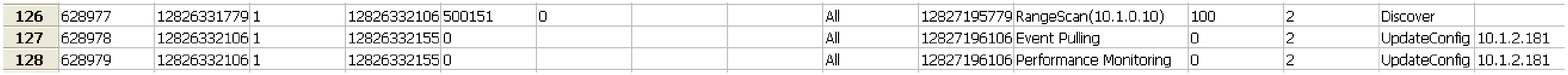
Device Monitor – Monitor

- Update Task Triggered



Alerts | Tasks for the last 24 hours.

Date ▼	UserID	Cust ID	Description	Status	Type	Progress
15:00:10 08/24/2010		Super	Performance Monitoring	Done	UpdateConfig	0
15:00:10 08/24/2010		Super	Event Pulling	Done	UpdateConfig	0
14:59:37 08/24/2010	admin	Super	RangeScan(10.1.0.10)	Done	Discover	100

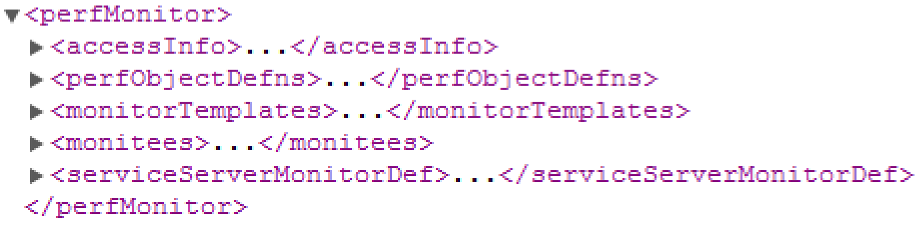


126	628977	12826331779	1	12826332106	500151	0			All	12827195779	RangeScan(10.1.0.10)	100	2	Discover	
127	628978	12826332106	1	12826332155	0				All	12827196106	Event Pulling	0	2	UpdateConfig	10.1.2.181
128	628979	12826332106	1	12826332155	0				All	12827196106	Performance Monitoring	0	2	UpdateConfig	10.1.2.181

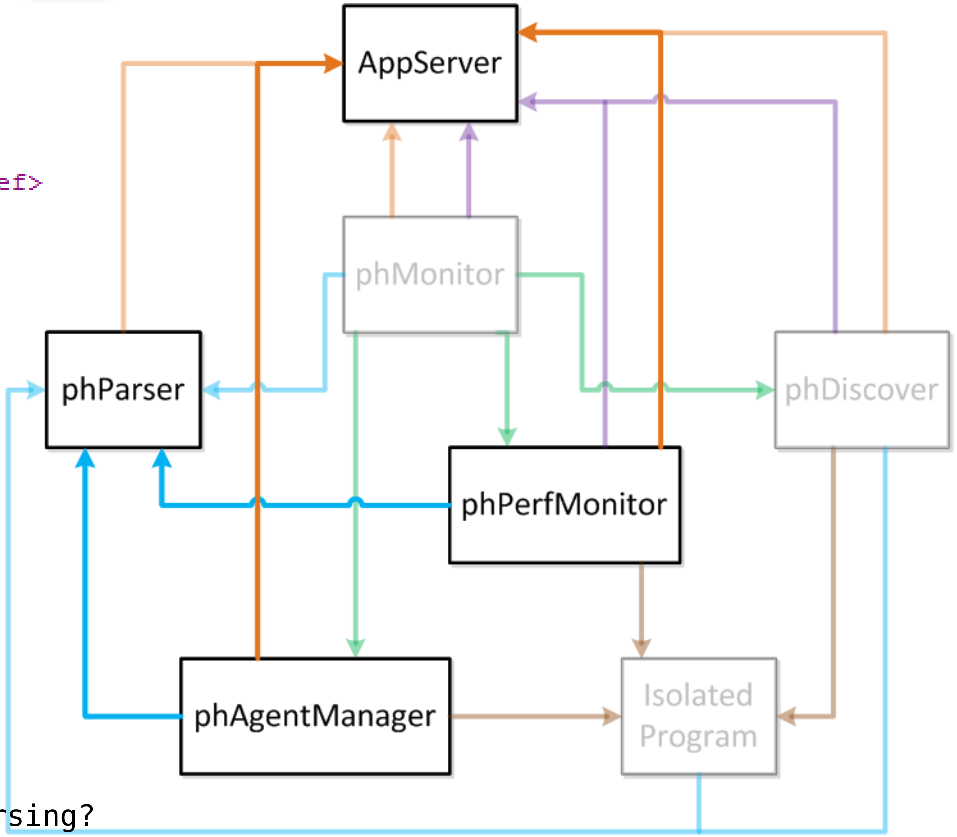
Table: ph_task

Device Monitor – Monitor

- phPerfMonitor Get Task



```
▼<perfMonitor>
  ▶<accessInfo>...</accessInfo>
  ▶<perfObjectDefns>...</perfObjectDefns>
  ▶<monitorTemplates>...</monitorTemplates>
  ▶<monitees>...</monitees>
  ▶<serviceServerMonitorDef>...</serviceServerMonitorDef>
 </perfMonitor>
```

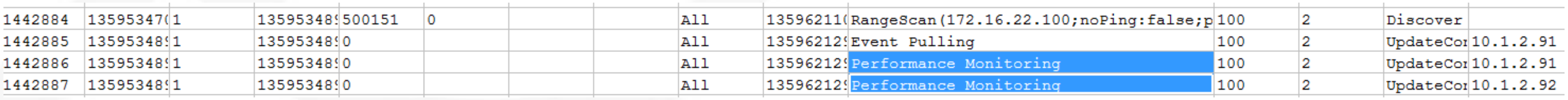


https://192.168.20.116/phoenix/rest/deviceInfo/parsing?taskId=2026050&custId=1&agentId=1

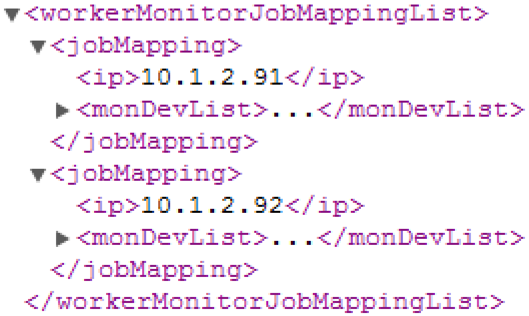
https://192.168.20.116/phoenix/rest/deviceInfo/perfMonitor?custId=1&taskId=2026051

Device Monitor – Monitor

- Job distribution in AOSP
  - Super and Worker both monitor devices
  - App Server allocate devices
  - Multiple tasks created



1442884	13595347	1	13595348	500151	0			All	13596211	RangeScan(172.16.22.100;noPing:false;p	100	2	Discover	
1442885	13595348	1	13595348	0				All	13596212	Event Pulling	100	2	UpdateCo	10.1.2.91
1442886	13595348	1	13595348	0				All	13596212	Performance Monitoring	100	2	UpdateCo	10.1.2.91
1442887	13595348	1	13595348	0				All	13596212	Performance Monitoring	100	2	UpdateCo	10.1.2.92

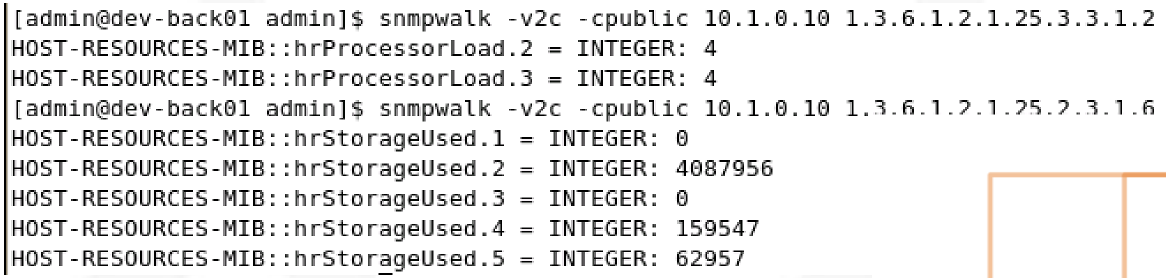


```
▼<workerMonitorJobMappingList>
  ▼<jobMapping>
     <ip>10.1.2.91</ip>
   ▶<monDevList>...</monDevList>
   </jobMapping>
  ▼<jobMapping>
     <ip>10.1.2.92</ip>
   ▶<monDevList>...</monDevList>
   </jobMapping>
 </workerMonitorJobMappingList>
```

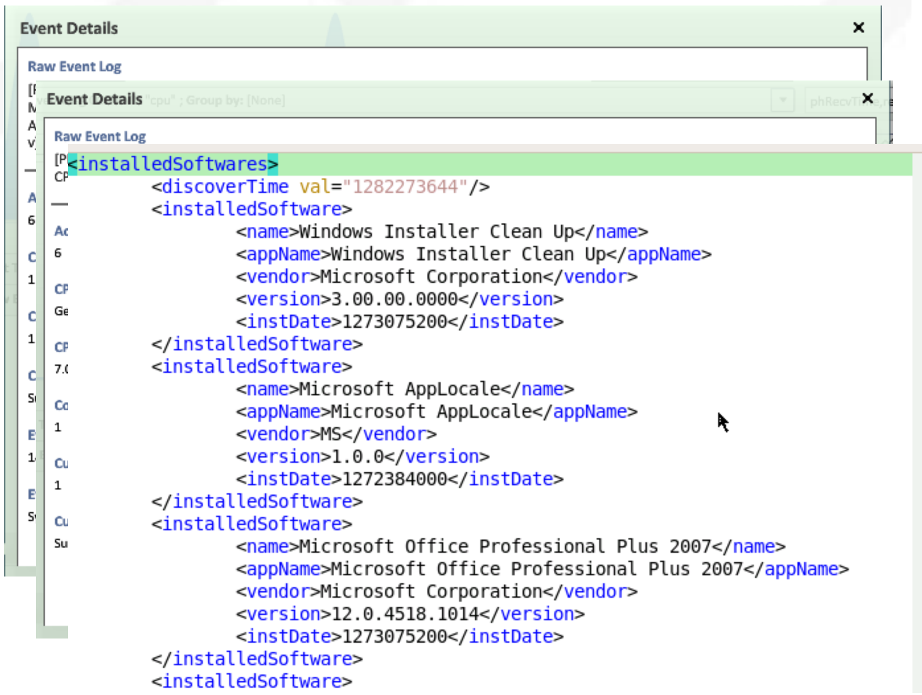
File:/data/cache/worker_mon_job.xml

Device Monitor – Monitor

- phPerfMonitor Add Task and Execute



```
[admin@dev-back01 admin]$ snmpwalk -v2c -cpublic 10.1.0.10 1.3.6.1.2.1.25.3.3.1.2
HOST-RESOURCES-MIB::hrProcessorLoad.2 = INTEGER: 4
HOST-RESOURCES-MIB::hrProcessorLoad.3 = INTEGER: 4
[admin@dev-back01 admin]$ snmpwalk -v2c -cpublic 10.1.0.10 1.3.6.1.2.1.25.2.3.1.6
HOST-RESOURCES-MIB::hrStorageUsed.1 = INTEGER: 0
HOST-RESOURCES-MIB::hrStorageUsed.2 = INTEGER: 4087956
HOST-RESOURCES-MIB::hrStorageUsed.3 = INTEGER: 0
HOST-RESOURCES-MIB::hrStorageUsed.4 = INTEGER: 159547
HOST-RESOURCES-MIB::hrStorageUsed.5 = INTEGER: 62957
```



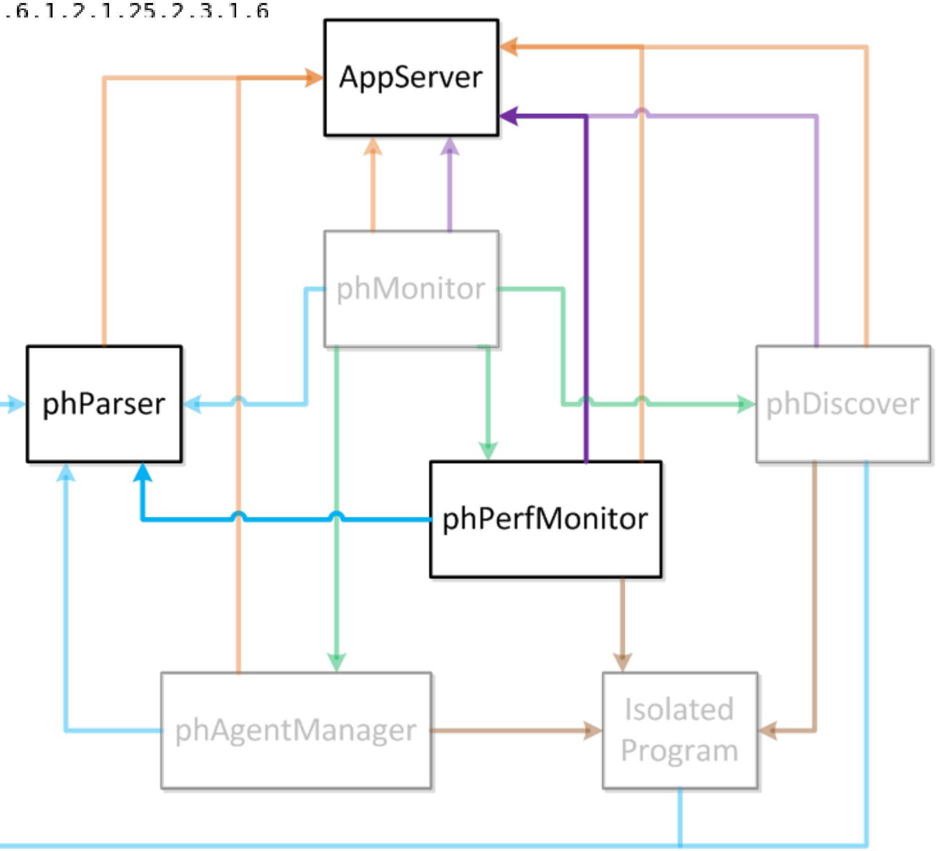
Event Details

Raw Event Log

Event Details

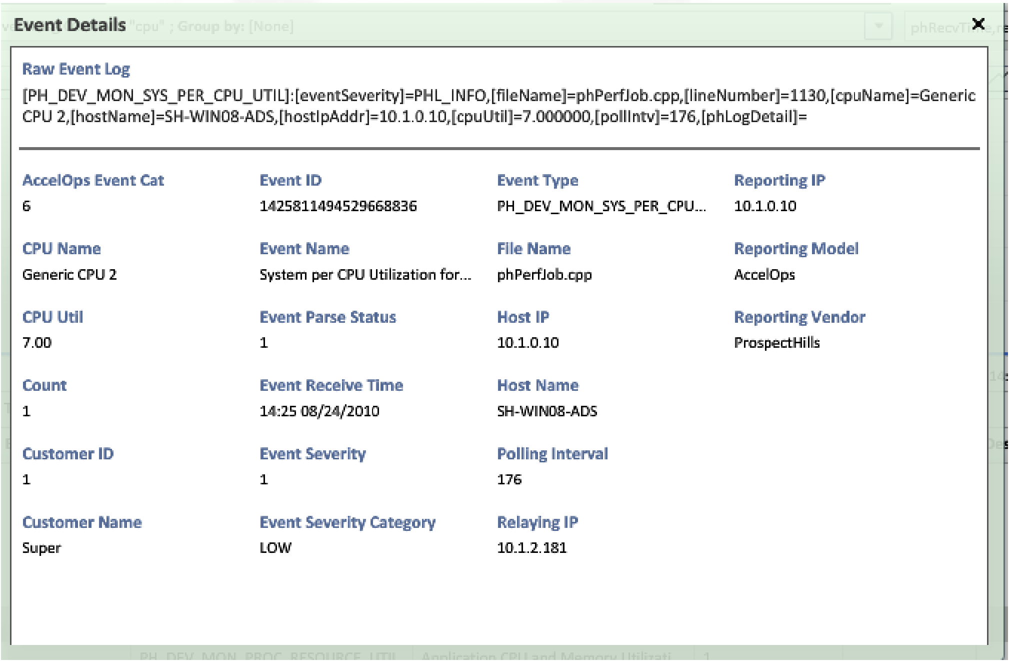
Raw Event Log

```
<installedSoftwares>
        <discoverTime val="1282273644"/>
        <installedSoftware>
                <name>Windows Installer Clean Up</name>
                <appName>Windows Installer Clean Up</appName>
                <vendor>Microsoft Corporation</vendor>
                <version>3.00.00.0000</version>
                <instDate>1273075200</instDate>
        </installedSoftware>
        <installedSoftware>
                <name>Microsoft AppLocale</name>
                <appName>Microsoft AppLocale</appName>
                <vendor>MS</vendor>
                <version>1.0.0</version>
                <instDate>1272384000</instDate>
        </installedSoftware>
        <installedSoftware>
                <name>Microsoft Office Professional Plus 2007</name>
                <appName>Microsoft Office Professional Plus 2007</appName>
                <vendor>Microsoft Corporation</vendor>
                <version>12.0.4518.1014</version>
                <instDate>1273075200</instDate>
        </installedSoftware>
        <installedSoftware>
```



Life of Event

- What means event?
  - It's a string or binary
  - It contains information
  - It has been received by AO
  - It's expected to be parsed



Event Details

Raw Event Log

```
[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1130,[cpuName]=Generic CPU 2,[hostName]=SH-WIN08-ADS,[hostIpAddr]=10.1.0.10,[cpuUtil]=7.000000,[pollIntv]=176,[phLogDetail]=
```

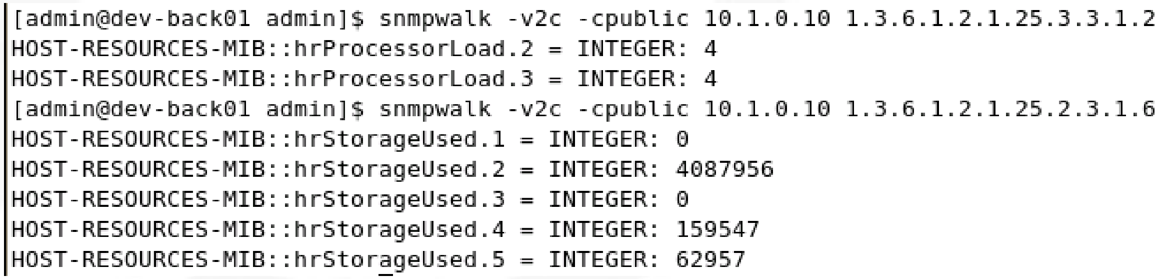
AccelOps Event Cat	Event ID	Event Type	Reporting IP
6	1425811494529668836	PH_DEV_MON_SYS_PER_CPU...	10.1.0.10
CPU Name	Event Name	File Name	Reporting Model
Generic CPU 2	System per CPU Utilization for...	phPerfJob.cpp	AccelOps
CPU Util	Event Parse Status	Host IP	Reporting Vendor
7.00	1	10.1.0.10	ProspectHills
Count	Event Receive Time	Host Name	
1	14:25 08/24/2010	SH-WIN08-ADS	
Customer ID	Event Severity	Polling Interval	
1	1	176	
Customer Name	Event Severity Category	Relaying IP	
Super	LOW	10.1.2.181	

Life of Event – Event Source

- Outside Event
  - Syslog
  - SNMP TRAP
  - Snail
  - Net flow
  - ……
- Self Created Event
  - Syslog
  - Socket

Life of Event – Construct and Send

- phPerfMonitor monitoring target
  - Get data from target device by SNMP



```
[admin@dev-back01 admin]$ snmpwalk -v2c -cpublic 10.1.0.10 1.3.6.1.2.1.25.3.3.1.2
HOST-RESOURCES-MIB::hrProcessorLoad.2 = INTEGER: 4
HOST-RESOURCES-MIB::hrProcessorLoad.3 = INTEGER: 4
[admin@dev-back01 admin]$ snmpwalk -v2c -cpublic 10.1.0.10 1.3.6.1.2.1.25.2.3.1.6
HOST-RESOURCES-MIB::hrStorageUsed.1 = INTEGER: 0
HOST-RESOURCES-MIB::hrStorageUsed.2 = INTEGER: 4087956
HOST-RESOURCES-MIB::hrStorageUsed.3 = INTEGER: 0
HOST-RESOURCES-MIB::hrStorageUsed.4 = INTEGER: 159547
HOST-RESOURCES-MIB::hrStorageUsed.5 = INTEGER: 62957
```

  - Construct string contain those data

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=3248,[cpuName]=CPU x 1,[hostName]=frankwin2008,[hostIpAddr]=172.16.22.134,[cpuUtil]=18.000000,[pollIntv]=176,[phLogDetail]=
```

  - Send to port 514 (phParser) through UDP

Life of Event – Construct and Send

- phPerfMonitor monitoring target
  - Fail to get data from target device by WMI
  - Construct string contain debug info

```
Jan 27 11:54:17 PH-QA-AUTOTEST phPerfMonitor[9024]:
[PH_GENERIC_WARNING]:[eventSeverity]=PHL_WARNING,[procName]=phPerfMonitor,[f
ileName]=phPerfJob.cpp,[lineNumber]=5775,[phLogDetail]=WMI lookup for
Win32_PerfRawData_PerfDisk_LogicalDisk failed for WIN-IIKW9EG1676(172.16.22.134):
Retrieve result data.
```

  - Send by syslog service
  - Syslog service found forwarding rule for this user (local5) and this log level

```
*.info;cron.none                    @127.0.0.1:6100
local5.*                            /opt/phoenix/log/phoenix.log
```

  - phParser receive string by port 6100

File:/etc/rsyslog.conf

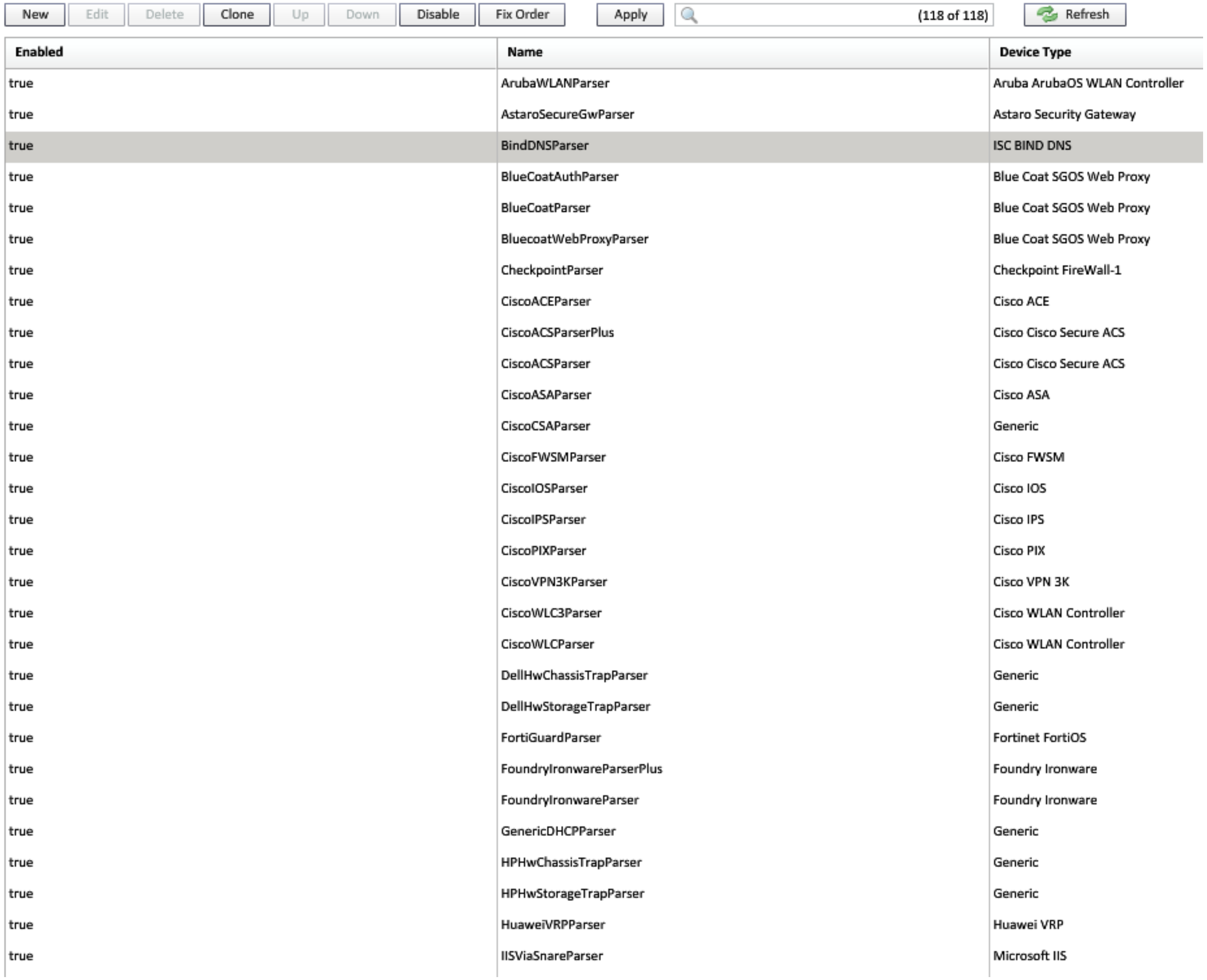
Life of Event – Parsing

- phParser listening ports

Port	Event	TCP	UDP
162	SNMP TRAP		√
514	Syslog	√	√
1470	No Idea…	√	
2055	NET FLOW		√
6100	Internal Event		√
6343	SFLOW		√
7912	IPS, Checkpoint, Incident	√	
7914	Command Port	√	

Life of Event – Parsing

- phParser parsing event

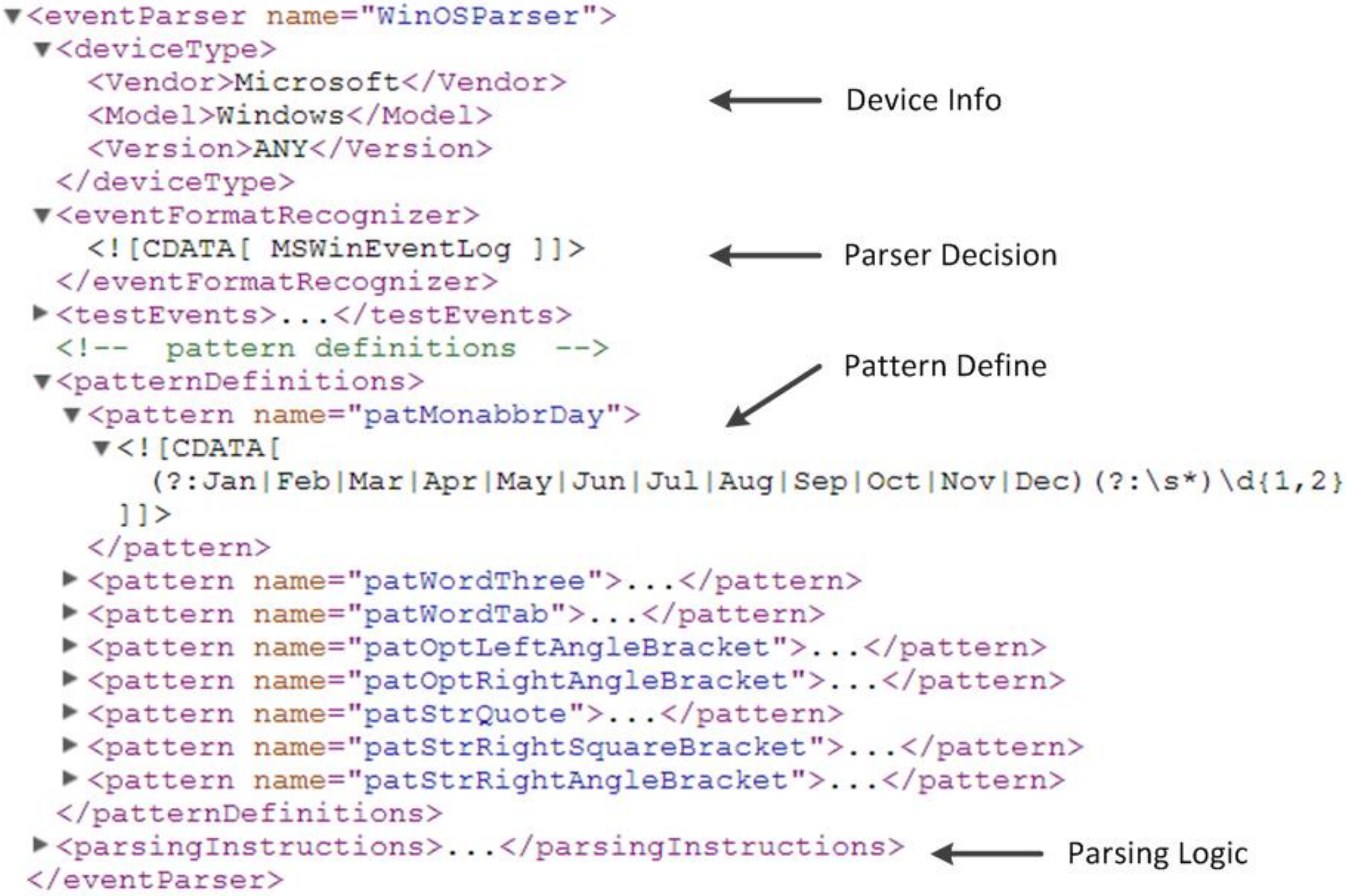


Enabled	Name	Device Type
true	ArubaWLANParser	Aruba ArubaOS WLAN Controller
true	AstaroSecureGwParser	Astaro Security Gateway
true	BindDNSParser	ISC BIND DNS
true	BlueCoatAuthParser	Blue Coat SGOS Web Proxy
true	BlueCoatParser	Blue Coat SGOS Web Proxy
true	BluecoatWebProxyParser	Blue Coat SGOS Web Proxy
true	CheckpointParser	Checkpoint FireWall-1
true	CiscoACEParser	Cisco ACE
true	CiscoACSParserPlus	Cisco Cisco Secure ACS
true	CiscoACSParser	Cisco Cisco Secure ACS
true	CiscoASAParser	Cisco ASA
true	CiscoCSAParser	Generic
true	CiscoFWSMParser	Cisco FWSM
true	CiscoIOSParser	Cisco IOS
true	CiscoIPSParser	Cisco IPS
true	CiscoPIXParser	Cisco PIX
true	CiscoVPN3KParser	Cisco VPN 3K
true	CiscoWLC3Parser	Cisco WLAN Controller
true	CiscoWLCParser	Cisco WLAN Controller
true	DellHwChassisTrapParser	Generic
true	DellHwStorageTrapParser	Generic
true	FortiGuardParser	Fortinet FortiOS
true	FoundryIronwareParserPlus	Foundry Ironware
true	FoundryIronwareParser	Foundry Ironware
true	GenericDHCPParser	Generic
true	HPHwChassisTrapParser	Generic
true	HPHwStorageTrapParser	Generic
true	HuaweiVRPParser	Huawei VRP
true	IISViaSnareParser	Microsoft IIS

File:/opt/phoenix/config/xml

Life of Event – Parsing

- Parsing XML



```
▼<eventParser name="WinOSParser">
  ▼<deviceType>
     <Vendor>Microsoft</Vendor>
     <Model>Windows</Model>
     <Version>ANY</Version>
   </deviceType>
  ▼<eventFormatRecognizer>
     <![CDATA[ MSWinEventLog ]]>
   </eventFormatRecognizer>
  ▶<testEvents>...</testEvents>
   <!--  pattern definitions  -->
  ▼<patternDefinitions>
    ▼<pattern name="patMonabbrDay">
      ▼<![CDATA[
          (?:Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)(?:\s*)\d{1,2}
        ]]>
     </pattern>
    ▶<pattern name="patWordThree">...</pattern>
    ▶<pattern name="patWordTab">...</pattern>
    ▶<pattern name="patOptLeftAngleBracket">...</pattern>
    ▶<pattern name="patOptRightAngleBracket">...</pattern>
    ▶<pattern name="patStrQuote">...</pattern>
    ▶<pattern name="patStrRightSquareBracket">...</pattern>
    ▶<pattern name="patStrRightAngleBracket">...</pattern>
   </patternDefinitions>
  ▶<parsingInstructions>...</parsingInstructions>
 </eventParser>
```

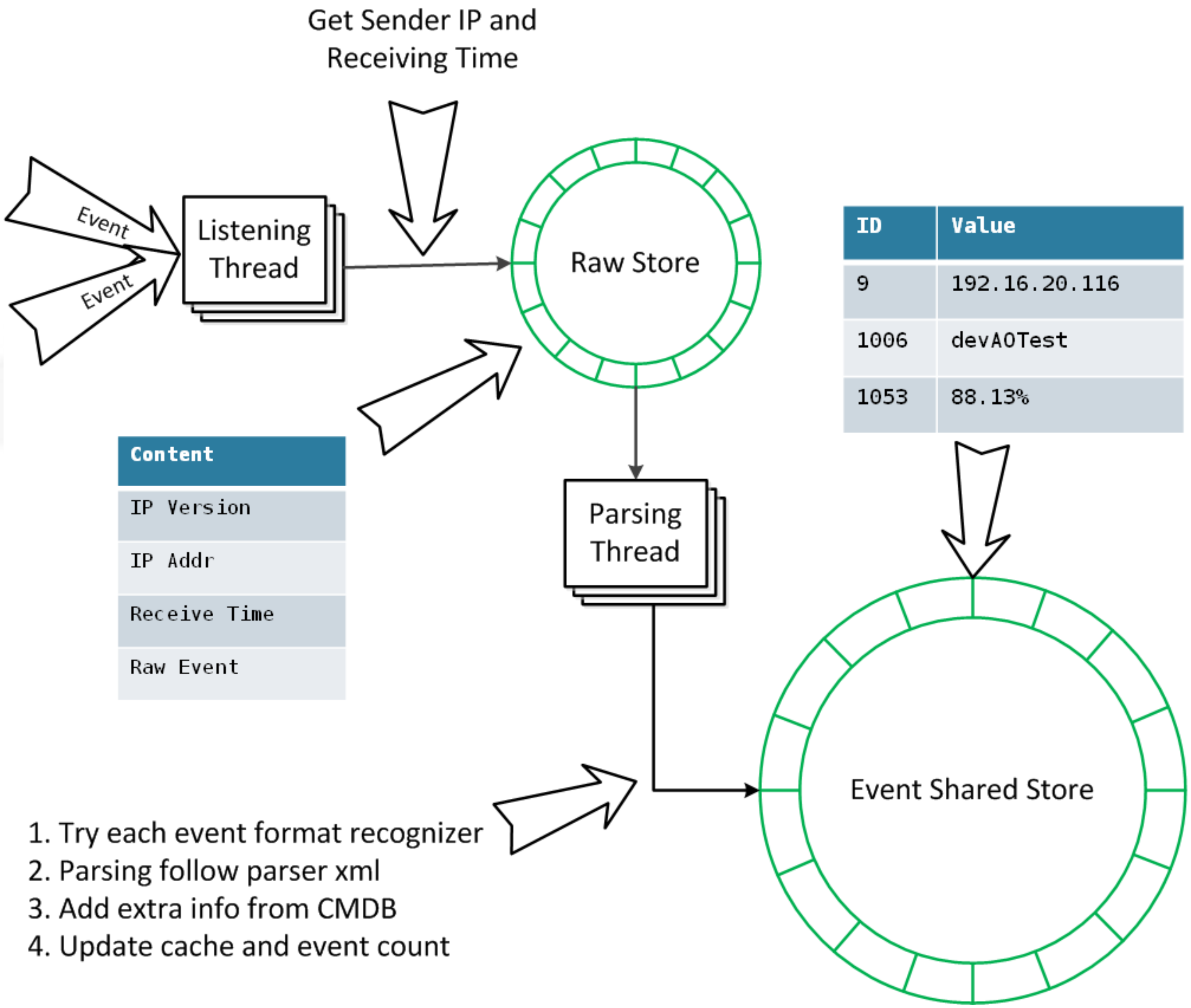
← Device Info

← Parser Decision

Pattern Define

← Parsing Logic

Life of Event – Parsing



Get Sender IP and Receiving Time

Event

Event

Listening Thread

Raw Store

Parsing Thread

Event Shared Store

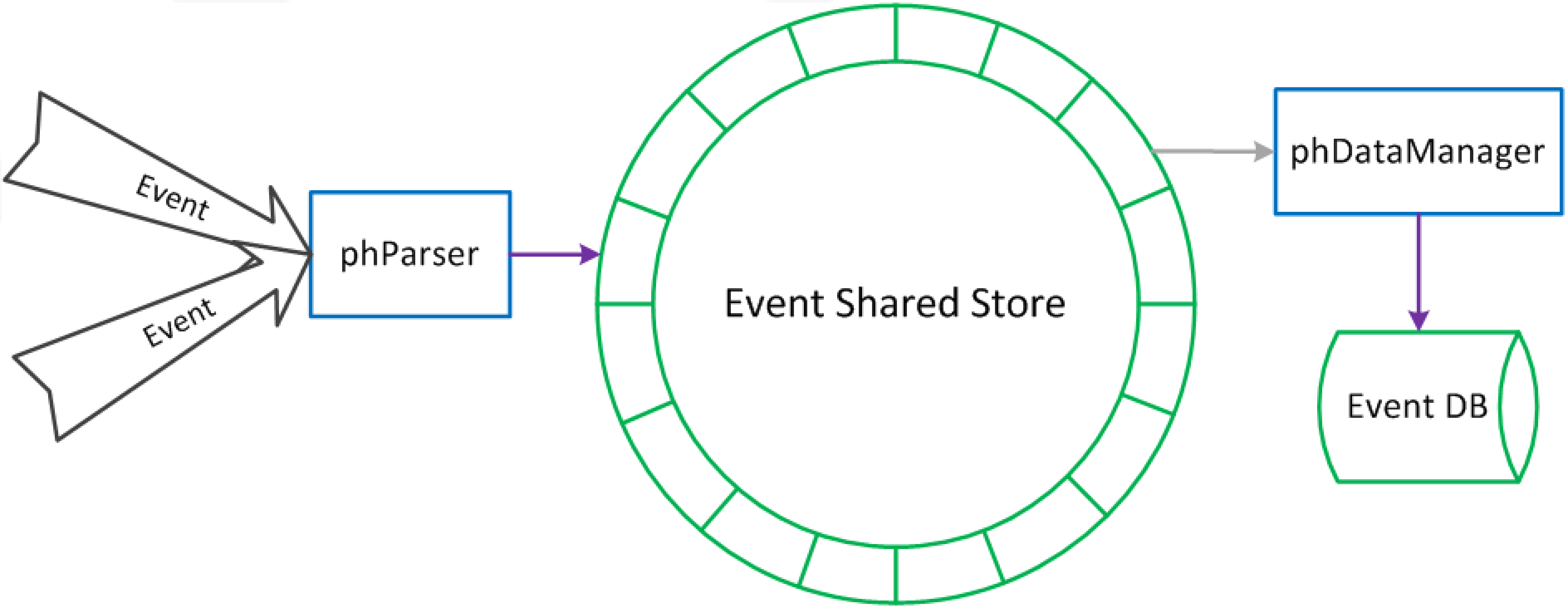
Content
IP Version
IP Addr
Receive Time
Raw Event

ID	Value
9	192.16.20.116
1006	devAOTest
1053	88.13%

1. Try each event format recognizer
2. Parsing follow parser xml
3. Add extra info from CMDB
4. Update cache and event count

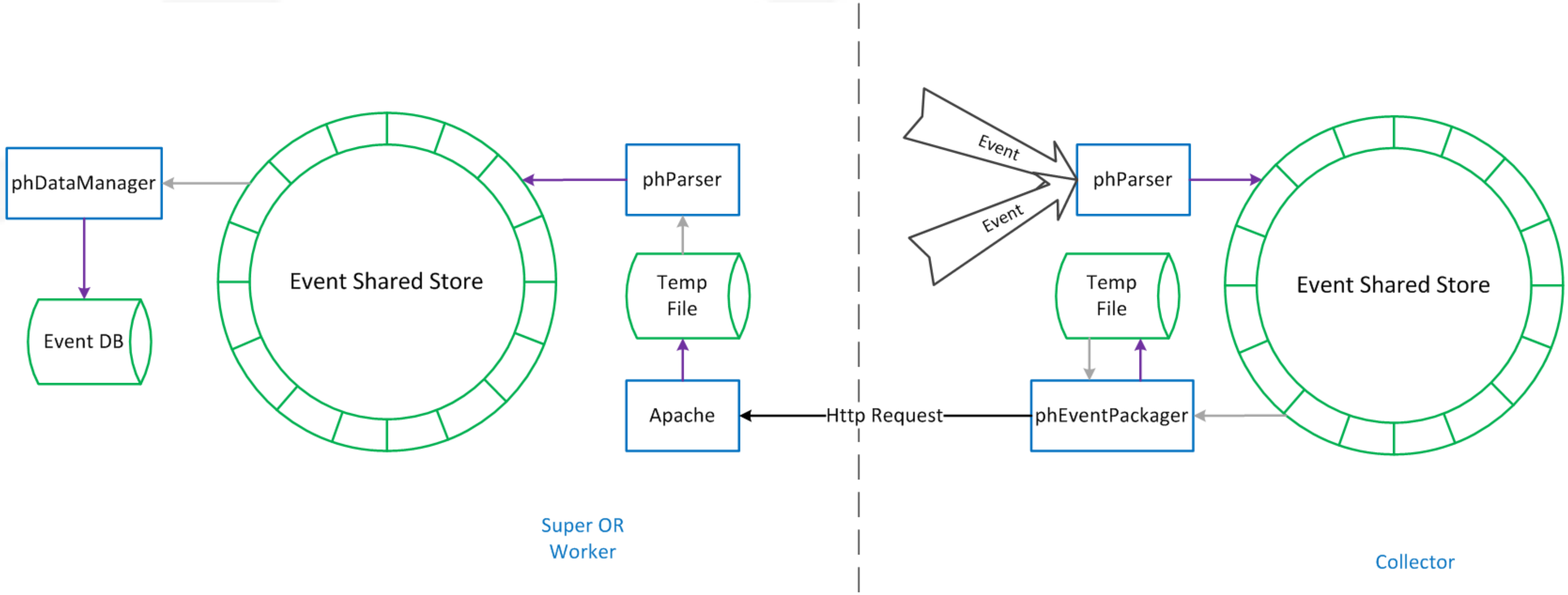
Life of Event – Storing

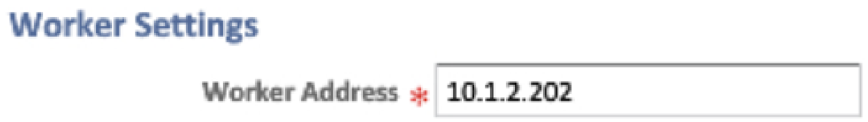
- Simple on non collector machine
  - Type: Super, Worker, VA



Life of Event – Storing

- Need to upload file to cloud on collector
  - Randomly pick super or one of workers
  - SS content on super and workers



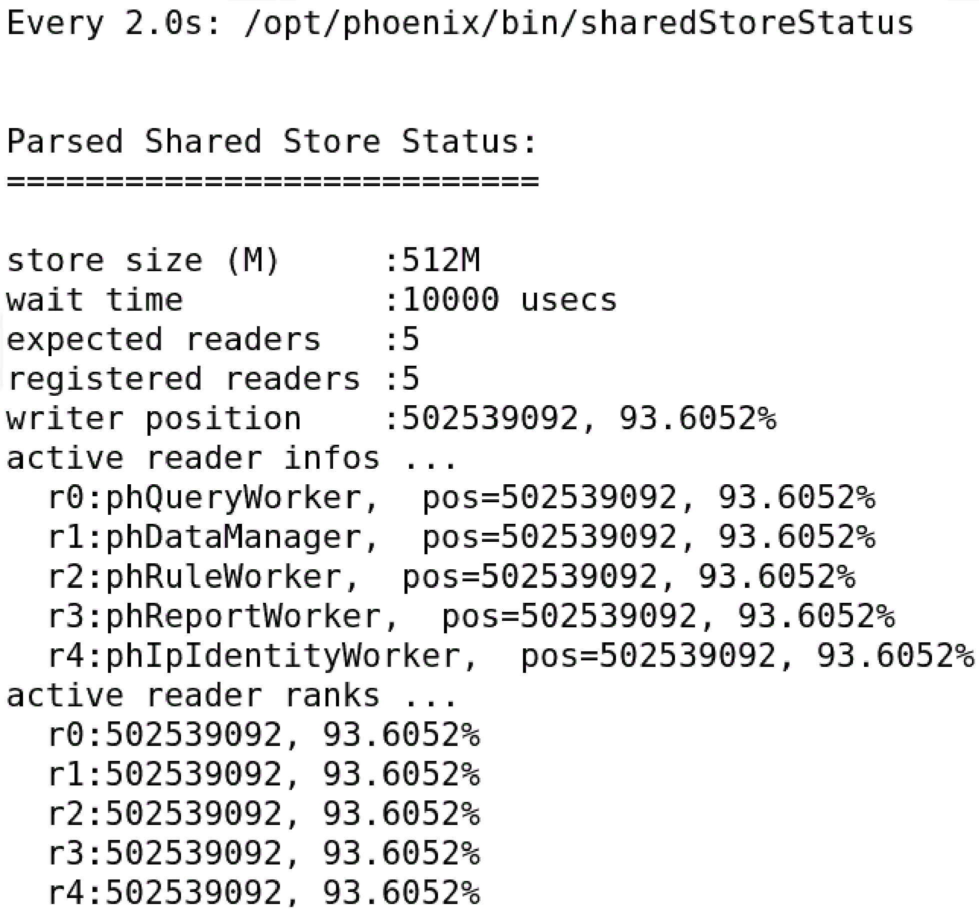


Worker Settings

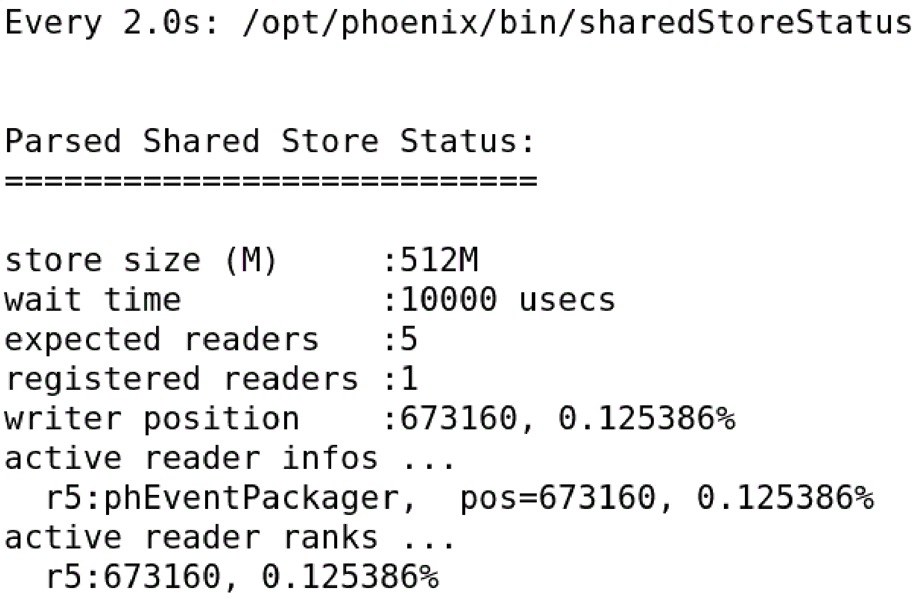
Worker Address * 10.1.2.202

Life of Event – Storing

- sss – Shared Store Status

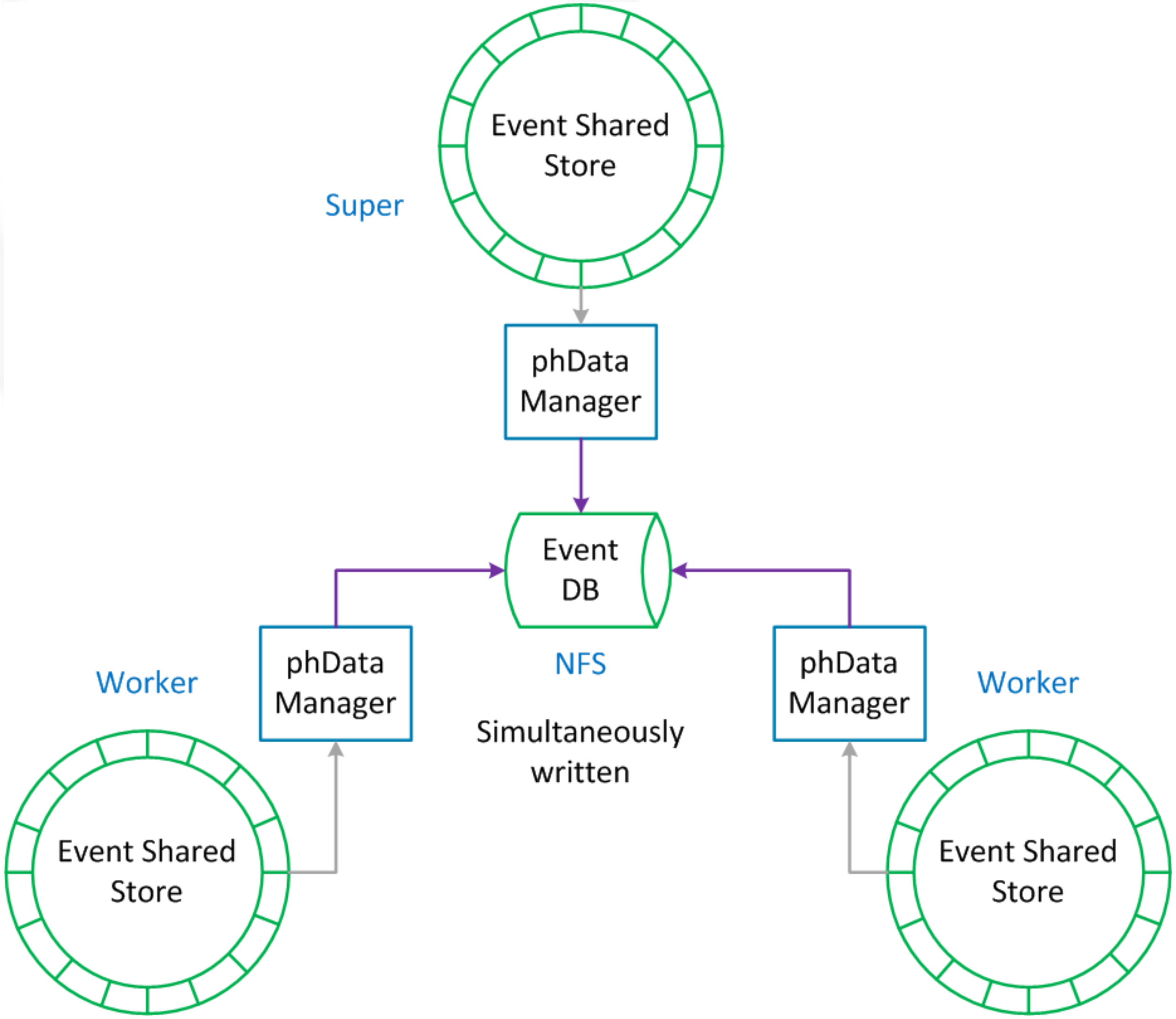


```
Every 2.0s: /opt/phoenix/bin/sharedStoreStatus


Parsed Shared Store Status:
===========================

store size (M)     :512M
wait time          :10000 usecs
expected readers   :5
registered readers :5
writer position    :502539092, 93.6052%
active reader infos ...
  r0:phQueryWorker,  pos=502539092, 93.6052%
  r1:phDataManager,  pos=502539092, 93.6052%
  r2:phRuleWorker,  pos=502539092, 93.6052%
  r3:phReportWorker,  pos=502539092, 93.6052%
  r4:phIpIdentityWorker,  pos=502539092, 93.6052%
active reader ranks ...
  r0:502539092, 93.6052%
  r1:502539092, 93.6052%
  r2:502539092, 93.6052%
  r3:502539092, 93.6052%
  r4:502539092, 93.6052%
```



```
Every 2.0s: /opt/phoenix/bin/sharedStoreStatus


Parsed Shared Store Status:
===========================

store size (M)     :512M
wait time          :10000 usecs
expected readers   :5
registered readers :1
writer position    :673160, 0.125386%
active reader infos ...
  r5:phEventPackager,  pos=673160, 0.125386%
active reader ranks ...
  r5:673160, 0.125386%
```

Life of Event – Storing



File:/data/eventdb

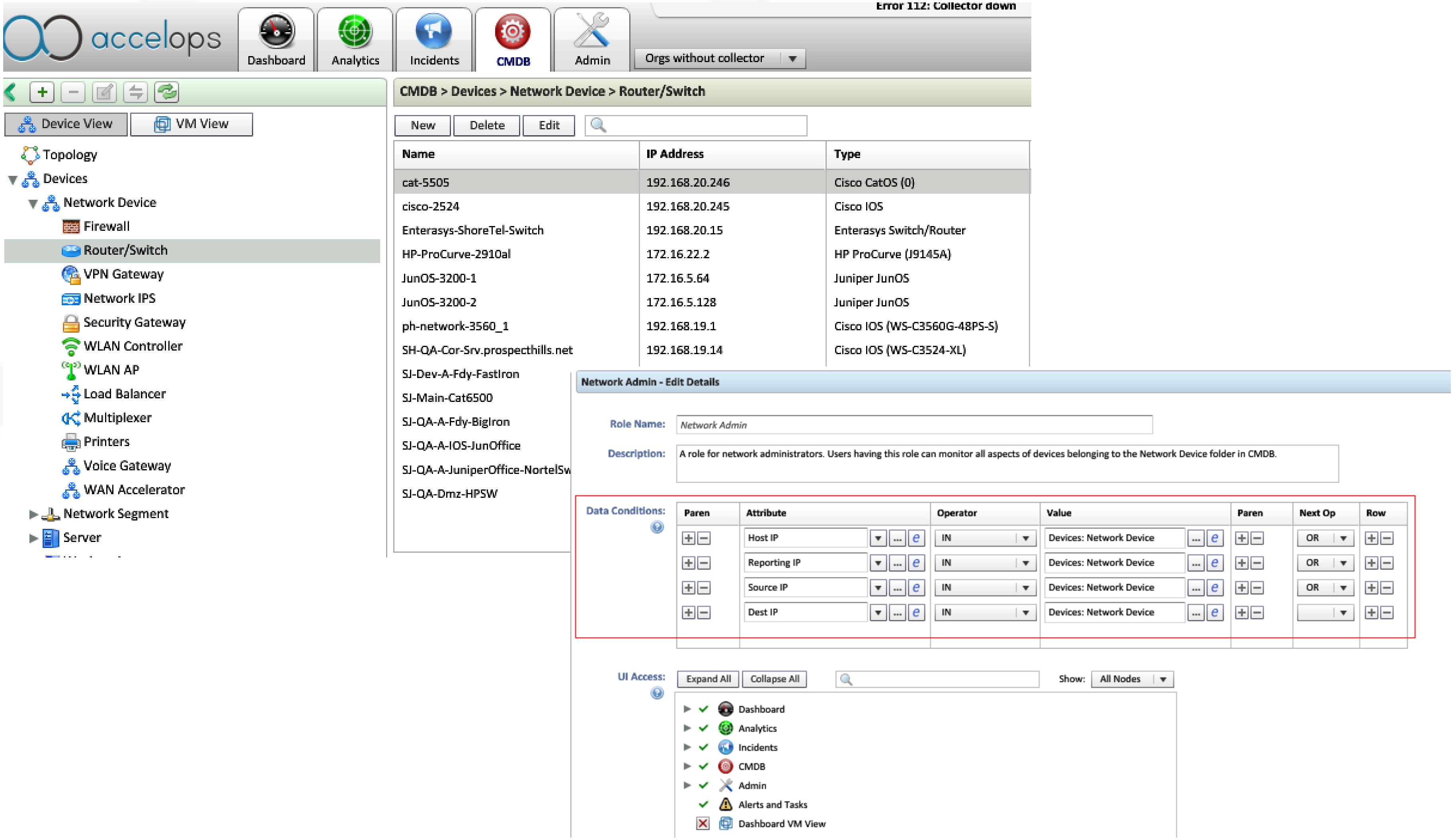
A&B C

- App Server and Backend Communication
  - Time driven
    - Server configuration
  - Task driven
    - Discover
    - Performance job update
  - Socket driven
  - Change set driven

A&C – Socket Driven

- Task
  - Query & Summary Report
  - Rule Update
  - Rule Exception Update
  - Manually Clear Incident
- Trait
  - Server Side
  - Fast Response

A&B C – Change Set Driven



CMDB > Devices > Network Device > Router/Switch

Name	IP Address	Type
cat-5505	192.168.20.246	Cisco CatOS (0)
cisco-2524	192.168.20.245	Cisco IOS
Enterasys-ShoreTel-Switch	192.168.20.15	Enterasys Switch/Router
HP-ProCurve-2910al	172.16.22.2	HP ProCurve (J9145A)
JunOS-3200-1	172.16.5.64	Juniper JunOS
JunOS-3200-2	172.16.5.128	Juniper JunOS
ph-network-3560_1	192.168.19.1	Cisco IOS (WS-C3560G-48PS-S)
SH-QA-Cor-Srv.prospecthills.net	192.168.19.14	Cisco IOS (WS-C3524-XL)
SJ-Dev-A-Fdy-FastIron		
SJ-Main-Cat6500		
SJ-QA-A-Fdy-BigIron		
SJ-QA-A-IOS-JunOffice		
SJ-QA-A-JuniperOffice-NortelSw		
SJ-QA-Dmz-HPSW		

Network Admin - Edit Details

Role Name: Network Admin

Description: A role for network administrators. Users having this role can monitor all aspects of devices belonging to the Network Device folder in CMDB.

Data Conditions:

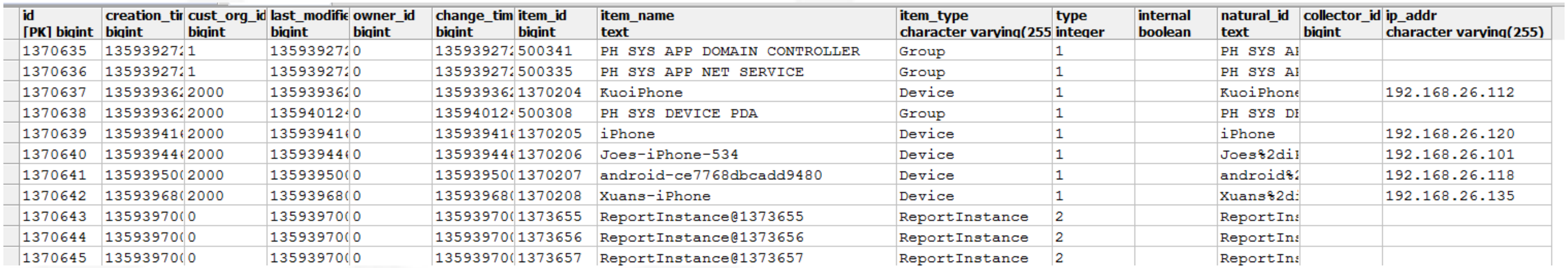
Paren	Attribute	Operator	Value	Paren	Next Op	Row
+ −	Host IP	IN	Devices: Network Device	+ −	OR	+ −
+ −	Reporting IP	IN	Devices: Network Device	+ −	OR	+ −
+ −	Source IP	IN	Devices: Network Device	+ −	OR	+ −
+ −	Dest IP	IN	Devices: Network Device	+ −		+ −

UI Access: Expand All | Collapse All | Show: All Nodes

- ✓ Dashboard
- ✓ Analytics
- ✓ Incidents
- ✓ CMDB
- ✓ Admin
- ✓ Alerts and Tasks
- ☒ Dashboard VM View

A&B C – Change Set Driven

- App Server Maintain Change



id [PK] bigint	creation_tir bigint	cust_org_id bigint	last_modifie bigint	owner_id bigint	change_tim bigint	item_id bigint	item_name text	item_type character varying(255	type integer	internal boolean	natural_id text	collector_id bigint	ip_addr character varying(255)
1370635	13593927	1	13593927	0	13593927	500341	PH SYS APP DOMAIN CONTROLLER	Group	1		PH SYS A		
1370636	13593927	1	13593927	0	13593927	500335	PH SYS APP NET SERVICE	Group	1		PH SYS A		
1370637	13593936	2000	13593936	0	13593936	1370204	KuoiPhone	Device	1		KuoiPhone		192.168.26.112
1370638	13593936	2000	13594012	0	13594012	500308	PH SYS DEVICE PDA	Group	1		PH SYS D		
1370639	13593941	2000	13593941	0	13593941	1370205	iPhone	Device	1		iPhone		192.168.26.120
1370640	13593944	2000	13593944	0	13593944	1370206	Joes-iPhone-534	Device	1		Joes%2di		192.168.26.101
1370641	13593950	2000	13593950	0	13593950	1370207	android-ce7768dbcadd9480	Device	1		android%		192.168.26.118
1370642	13593968	2000	13593968	0	13593968	1370208	Xuans-iPhone	Device	1		Xuans%2d		192.168.26.135
1370643	13593970	0	13593970	0	13593970	1373655	ReportInstance@1373655	ReportInstance	2		ReportIn		
1370644	13593970	0	13593970	0	13593970	1373656	ReportInstance@1373656	ReportInstance	2		ReportIn		
1370645	13593970	0	13593970	0	13593970	1373657	ReportInstance@1373657	ReportInstance	2		ReportIn		

- Backend Keep Asking Change

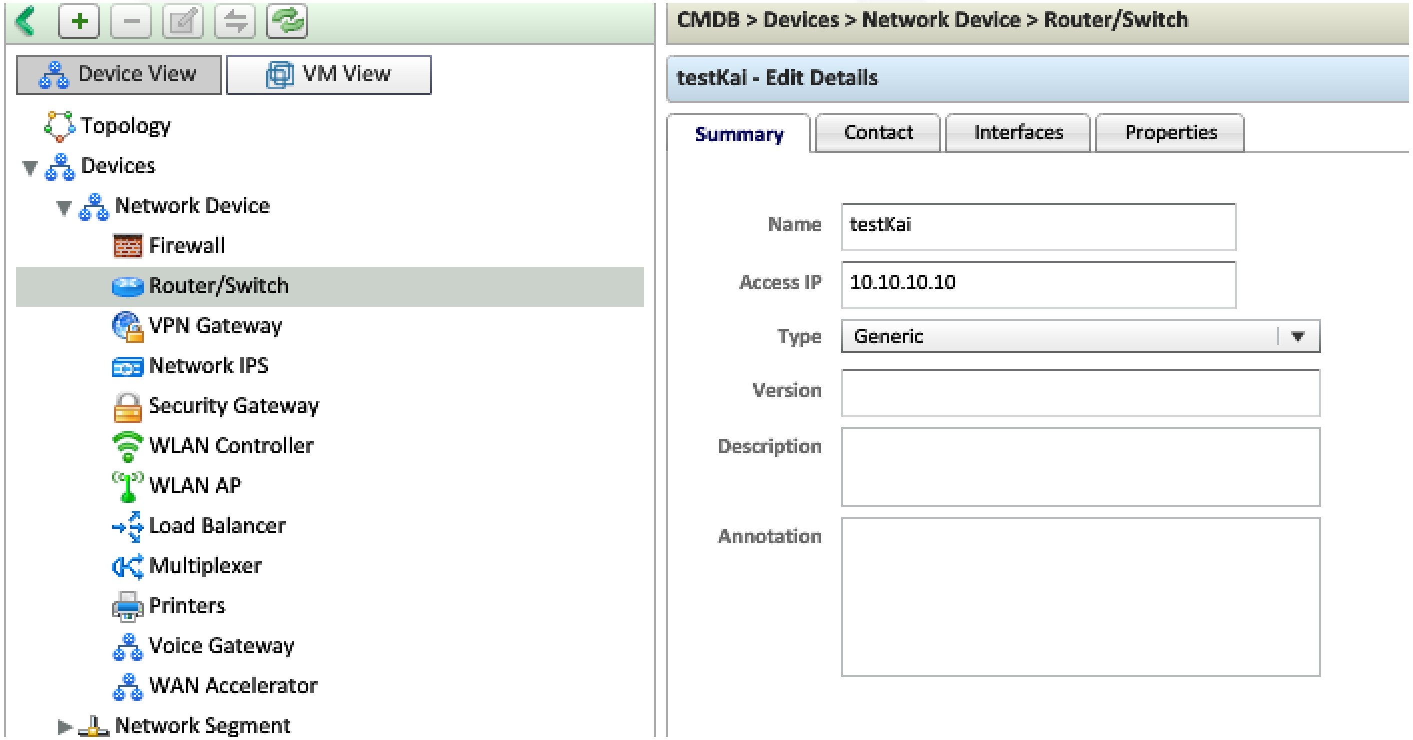
```
172.16.22.212 - - [28/Jan/2013:13:29:57 -0800] "GET /phoenix/rest/changeSet?since=1359408567788&phProcessName=phMonitorWorker HTTP/1.1" 200 221
172.16.20.109 - - [28/Jan/2013:13:29:59 -0800] "GET /phoenix/rest/changeSet?since=1359408568918&phProcessName=phMonitorWorker HTTP/1.1" 200 221
172.16.22.204 - - [28/Jan/2013:13:30:01 -0800] "GET /phoenix/rest/changeSet?since=1359408571259&phProcessName=phMonitorAgent HTTP/1.1" 200 221
172.16.22.211 - - [28/Jan/2013:13:30:07 -0800] "GET /phoenix/rest/changeSet?since=1359408577267&phProcessName=phMonitorSupervisor HTTP/1.1" 200 221
172.16.22.203 - - [28/Jan/2013:13:30:08 -0800] "GET /phoenix/rest/changeSet?since=1359408578416&phProcessName=phMonitorAgent HTTP/1.1" 200 221
172.16.22.202 - - [28/Jan/2013:13:30:14 -0800] "GET /phoenix/rest/changeSet?since=1359408584765&phProcessName=phMonitorAgent HTTP/1.1" 200 221
172.16.22.215 - - [28/Jan/2013:13:30:17 -0800] "GET /phoenix/rest/changeSet?since=1359408587456&phProcessName=phMonitorAgent HTTP/1.1" 200 221
172.16.22.213 - - [28/Jan/2013:13:30:17 -0800] "GET /phoenix/rest/changeSet?since=1359408587605&phProcessName=phMonitorAgent HTTP/1.1" 200 221
172.16.22.214 - - [28/Jan/2013:13:30:21 -0800] "GET /phoenix/rest/changeSet?since=1359408591864&phProcessName=phMonitorWorker HTTP/1.1" 200 221
```

Table: ph_change_set

Rest API: https://192.168.20.116/phoenix/rest/changeSet?since=1359407989

A&B C – Change Set Driven

- Sample – Create New Device
  - Create new device on GUI manually



CMDB > Devices > Network Device > Router/Switch

testKai - Edit Details

Name: testKai

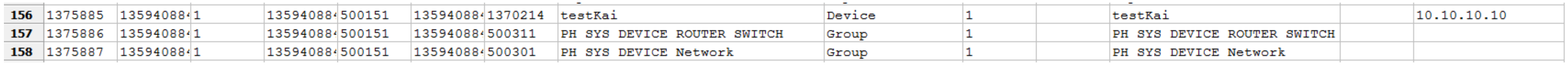
Access IP: 10.10.10.10

Type: Generic

Version:

Description:

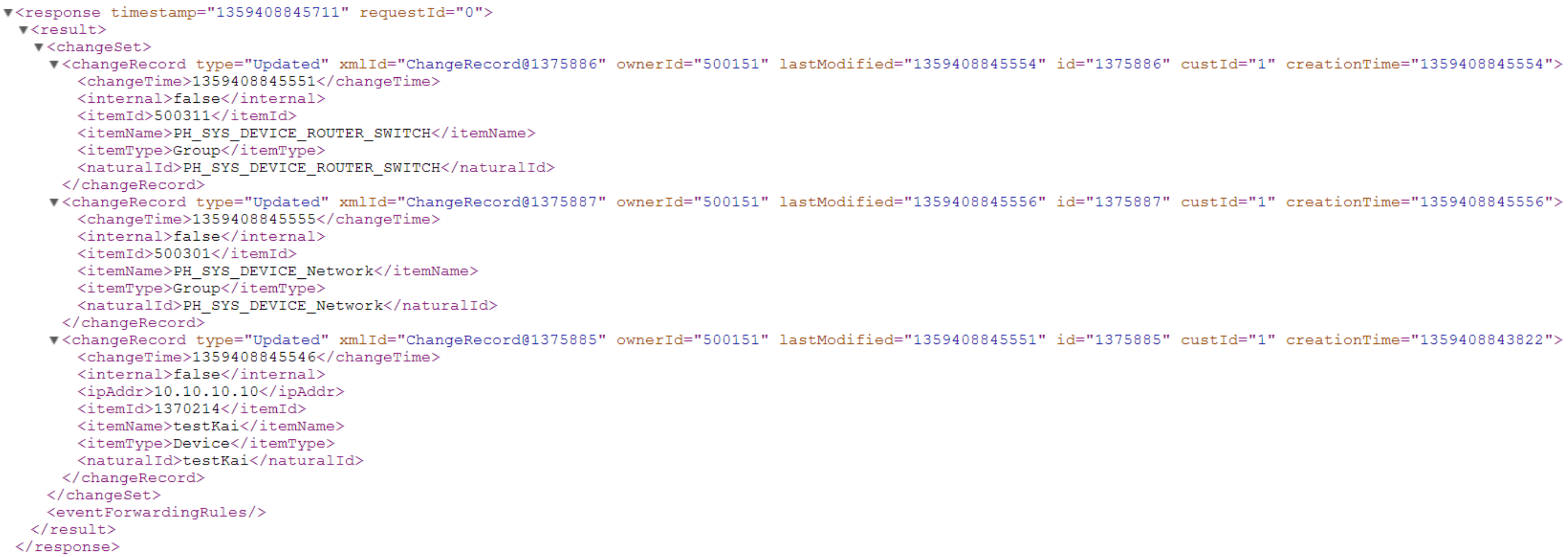
Annotation:



156	1375885	13594088	1	13594088	500151	13594088	1370214	testKai	Device	1		testKai		10.10.10.10
157	1375886	13594088	1	13594088	500151	13594088	500311	PH SYS DEVICE ROUTER SWITCH	Group	1		PH SYS DEVICE ROUTER SWITCH		
158	1375887	13594088	1	13594088	500151	13594088	500301	PH SYS DEVICE Network	Group	1		PH SYS DEVICE Network		

A&B C – Change Set Driven

- Sample – Create New Device
    - Change set receive



```
▼<response timestamp="1359408845711" requestId="0">
  ▼<result>
    ▼<changeSet>
      ▼<changeRecord type="Updated" xmlId="ChangeRecord@1375886" ownerId="500151" lastModified="1359408845554" id="1375886" custId="1" creationTime="1359408845554">
          <changeTime>1359408845551</changeTime>
          <internal>false</internal>
          <itemId>500311</itemId>
          <itemName>PH_SYS_DEVICE_ROUTER_SWITCH</itemName>
          <itemType>Group</itemType>
          <naturalId>PH_SYS_DEVICE_ROUTER_SWITCH</naturalId>
        </changeRecord>
      ▼<changeRecord type="Updated" xmlId="ChangeRecord@1375887" ownerId="500151" lastModified="1359408845556" id="1375887" custId="1" creationTime="1359408845556">
          <changeTime>1359408845555</changeTime>
          <internal>false</internal>
          <itemId>500301</itemId>
          <itemName>PH_SYS_DEVICE_Network</itemName>
          <itemType>Group</itemType>
          <naturalId>PH_SYS_DEVICE_Network</naturalId>
        </changeRecord>
      ▼<changeRecord type="Updated" xmlId="ChangeRecord@1375885" ownerId="500151" lastModified="1359408845551" id="1375885" custId="1" creationTime="1359408843822">
          <changeTime>1359408845546</changeTime>
          <internal>false</internal>
          <ipAddr>10.10.10.10</ipAddr>
          <itemId>1370214</itemId>
          <itemName>testKai</itemName>
          <itemType>Device</itemType>
          <naturalId>testKai</naturalId>
        </changeRecord>
      </changeSet>
      <eventForwardingRules/>
    </result>
  </response>
```

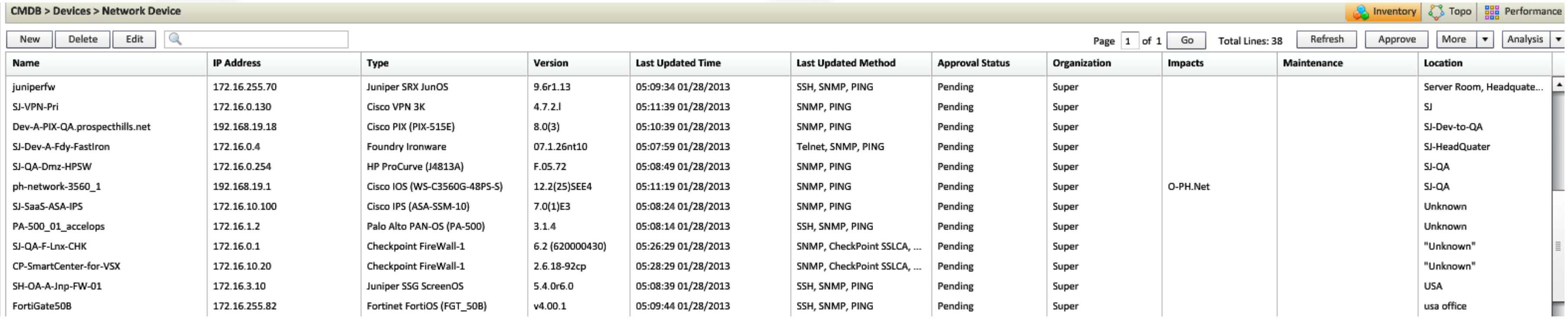
A&B C – Change Set Driven

- Sample – Create New Device
  - Update related group in memory cache

Type	Incremental Update	Lazy Update	Rest API
Network Interface			https://192.168.20.116/phoenix/rest/config/networkInterface
RBAC Profile	√		https://192.168.20.116/phoenix/rest/system/rbac/eventQueryCondition
Device Properties	√		https://192.168.20.116/phoenix/rest/device/properties
Domain (Org Scope)			https://192.168.20.116/phoenix/rest/config/domain
Application Package			https://192.168.20.116/phoenix/rest/config/applicationPackage
Business Service	√		https://192.168.20.116/phoenix/rest/cmdb/bizServices
Event Type Group	√		https://192.68.20.116/phoenix/rest/cmdb/event/type2group
Device Maintenance	√		https://192.68.20.116/phoenix/rest/devMaintenance
Group	√	√	https://192.68.20.116/phoenix/rest/namedValue

A&B C – Change Set Driven

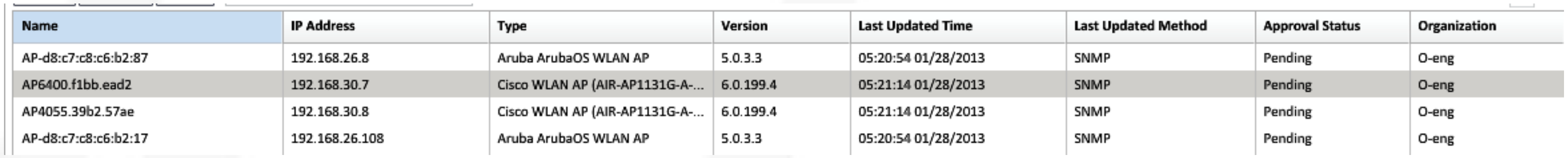
- Customer Id in ChangeSet
  - CustId 1 – Super Local (Default Customer)



Name	IP Address	Type	Version	Last Updated Time	Last Updated Method	Approval Status	Organization	Impacts	Maintenance	Location
juniperfw	172.16.255.70	Juniper SRX JunOS	9.6r1.13	05:09:34 01/28/2013	SSH, SNMP, PING	Pending	Super			Server Room, Headquate...
SJ-VPN-Pri	172.16.0.130	Cisco VPN 3K	4.7.2.l	05:11:39 01/28/2013	SNMP, PING	Pending	Super			SJ
Dev-A-PIX-QA.prospecthills.net	192.168.19.18	Cisco PIX (PIX-515E)	8.0(3)	05:10:39 01/28/2013	SNMP, PING	Pending	Super			SJ-Dev-to-QA
SJ-Dev-A-Fdy-FastIron	172.16.0.4	Foundry Ironware	07.1.26nt10	05:07:59 01/28/2013	Telnet, SNMP, PING	Pending	Super			SJ-HeadQuater
SJ-QA-Dmz-HPSW	172.16.0.254	HP ProCurve (J4813A)	F.05.72	05:08:49 01/28/2013	SNMP, PING	Pending	Super			SJ-QA
ph-network-3560_1	192.168.19.1	Cisco IOS (WS-C3560G-48PS-S)	12.2(25)SEE4	05:11:19 01/28/2013	SNMP, PING	Pending	Super	O-PH.Net		SJ-QA
SJ-SaaS-ASA-IPS	172.16.10.100	Cisco IPS (ASA-SSM-10)	7.0(1)E3	05:08:24 01/28/2013	SNMP, PING	Pending	Super			Unknown
PA-500_01_accelops	172.16.1.2	Palo Alto PAN-OS (PA-500)	3.1.4	05:08:14 01/28/2013	SSH, SNMP, PING	Pending	Super			Unknown
SJ-QA-F-Lnx-CHK	172.16.0.1	Checkpoint FireWall-1	6.2 (620000430)	05:26:29 01/28/2013	SNMP, CheckPoint SSLCA, ...	Pending	Super			"Unknown"
CP-SmartCenter-for-VSX	172.16.10.20	Checkpoint FireWall-1	2.6.18-92cp	05:28:29 01/28/2013	SNMP, CheckPoint SSLCA, ...	Pending	Super			"Unknown"
SH-OA-A-Jnp-FW-01	172.16.3.10	Juniper SSG ScreenOS	5.4.0r6.0	05:08:39 01/28/2013	SSH, SNMP, PING	Pending	Super			USA
FortiGate50B	172.16.255.82	Fortinet FortiOS (FGT_50B)	v4.00.1	05:09:44 01/28/2013	SSH, SNMP, PING	Pending	Super			usa office

A&B C – Change Set Driven

- Customer Id in ChangeSet
  - CustId > 2000 – Other customer

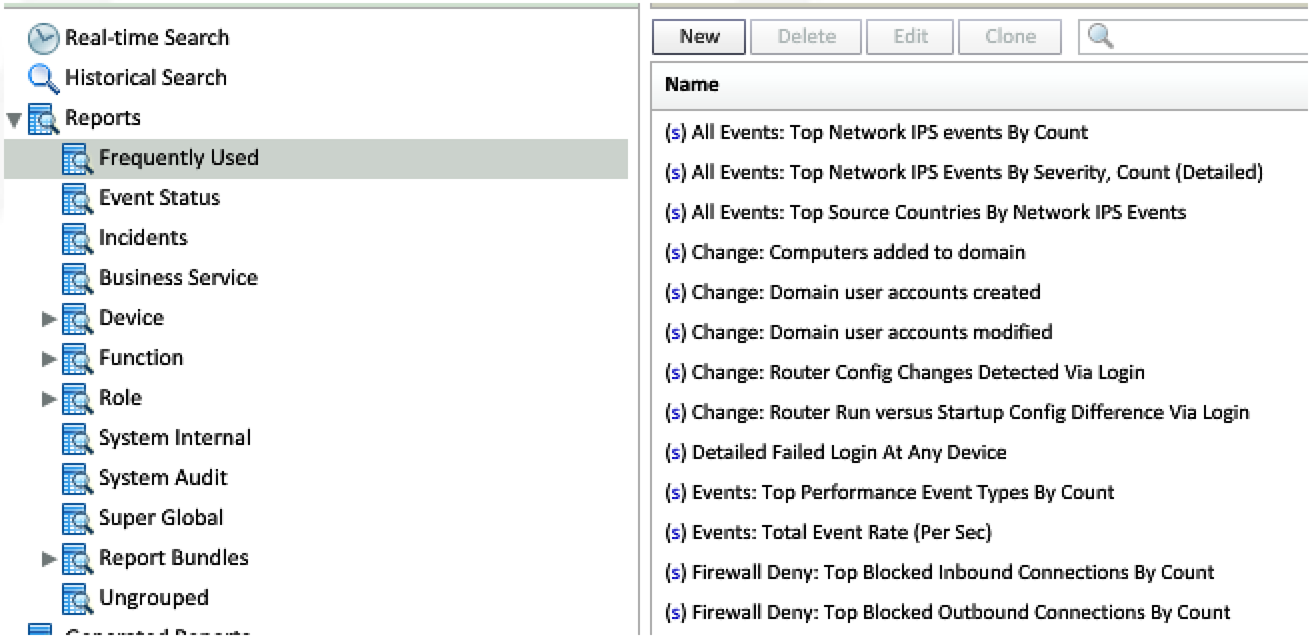


Name	IP Address	Type	Version	Last Updated Time	Last Updated Method	Approval Status	Organization
AP-d8:c7:c8:c6:b2:87	192.168.26.8	Aruba ArubaOS WLAN AP	5.0.3.3	05:20:54 01/28/2013	SNMP	Pending	O-eng
AP6400.f1bb.ead2	192.168.30.7	Cisco WLAN AP (AIR-AP1131G-A-...	6.0.199.4	05:21:14 01/28/2013	SNMP	Pending	O-eng
AP4055.39b2.57ae	192.168.30.8	Cisco WLAN AP (AIR-AP1131G-A-...	6.0.199.4	05:21:14 01/28/2013	SNMP	Pending	O-eng
AP-d8:c7:c8:c6:b2:17	192.168.26.108	Aruba ArubaOS WLAN AP	5.0.3.3	05:20:54 01/28/2013	SNMP	Pending	O-eng

  - CustId 3 – Super global (Cross Customers)

A&B C – Change Set Driven

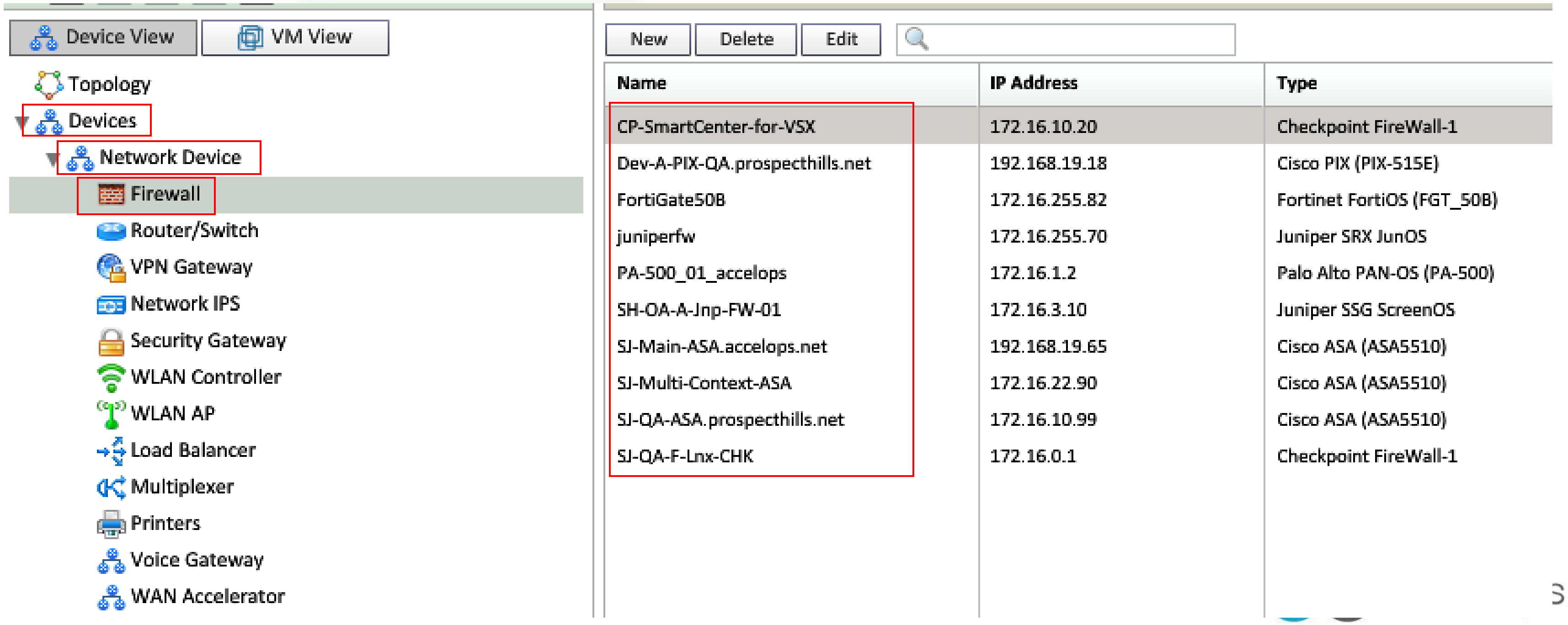
- Customer Id in ChangeSet
  - CustId 0 – System and Share



Name
(s) All Events: Top Network IPS events By Count
(s) All Events: Top Network IPS Events By Severity, Count (Detailed)
(s) All Events: Top Source Countries By Network IPS Events
(s) Change: Computers added to domain
(s) Change: Domain user accounts created
(s) Change: Domain user accounts modified
(s) Change: Router Config Changes Detected Via Login
(s) Change: Router Run versus Startup Config Difference Via Login
(s) Detailed Failed Login At Any Device
(s) Events: Top Performance Event Types By Count
(s) Events: Total Event Rate (Per Sec)
(s) Firewall Deny: Top Blocked Inbound Connections By Count
(s) Firewall Deny: Top Blocked Outbound Connections By Count

A&B C – Change Set Driven

- Customer Id in Change Set
  - Item has customer Id, group also has customer Id
  - Group has father group, customer Id might be different
  - Group has item for multiple customers



Name	IP Address	Type
CP-SmartCenter-for-VSX	172.16.10.20	Checkpoint FireWall-1
Dev-A-PIX-QA.prospecthills.net	192.168.19.18	Cisco PIX (PIX-515E)
FortiGate50B	172.16.255.82	Fortinet FortiOS (FGT_50B)
juniperfw	172.16.255.70	Juniper SRX JunOS
PA-500_01_accelops	172.16.1.2	Palo Alto PAN-OS (PA-500)
SH-OA-A-Jnp-FW-01	172.16.3.10	Juniper SSG ScreenOS
SJ-Main-ASA.accelops.net	192.168.19.65	Cisco ASA (ASA5510)
SJ-Multi-Context-ASA	172.16.22.90	Cisco ASA (ASA5510)
SJ-QA-ASA.prospecthills.net	172.16.10.99	Cisco ASA (ASA5510)
SJ-QA-F-Lnx-CHK	172.16.0.1	Checkpoint FireWall-1

A&B C – Change Set Driven

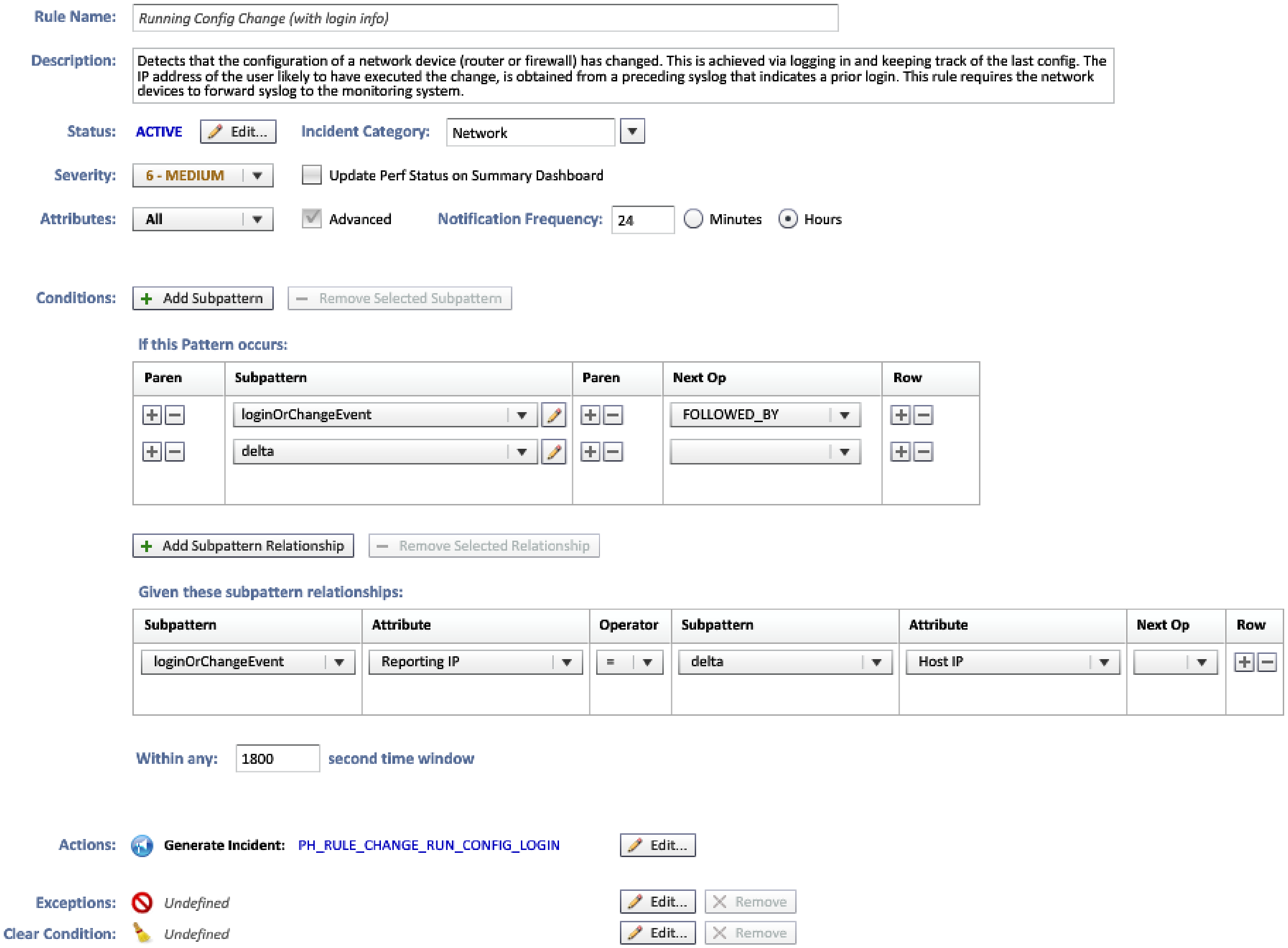
- Customer Id in Change Set
  - Backend required quick response for change set query
  - Super Global is a special customer Id

Data Analysis

- Rule – What’s happening?
  - Event Scan
  - Incident
- Report – What’s the status?
  - Ad hoc
  - Real Time
  - Inline
  - Summary

Data Analysis – Rule

- Definition



Rule Name: *Running Config Change (with login info)*

Description: Detects that the configuration of a network device (router or firewall) has changed. This is achieved via logging in and keeping track of the last config. The IP address of the user likely to have executed the change, is obtained from a preceding syslog that indicates a prior login. This rule requires the network devices to forward syslog to the monitoring system.

Status: ACTIVE Incident Category: Network

Severity: 6 - MEDIUM □ Update Perf Status on Summary Dashboard

Attributes: All ☑ Advanced Notification Frequency: 24 ○ Minutes ● Hours

Conditions:

If this Pattern occurs:

Paren	Subpattern	Paren	Next Op	Row
⊞⊟	loginOrChangeEvent	⊞⊟	FOLLOWED_BY	⊞⊟
⊞⊟	delta	⊞⊟		⊞⊟

Given these subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next Op	Row
loginOrChangeEvent	Reporting IP	=	delta	Host IP		⊞⊟

Within any: 1800 second time window

Actions: Generate Incident: PH_RULE_CHANGE_RUN_CONFIG_LOGIN

Exceptions: *Undefined*

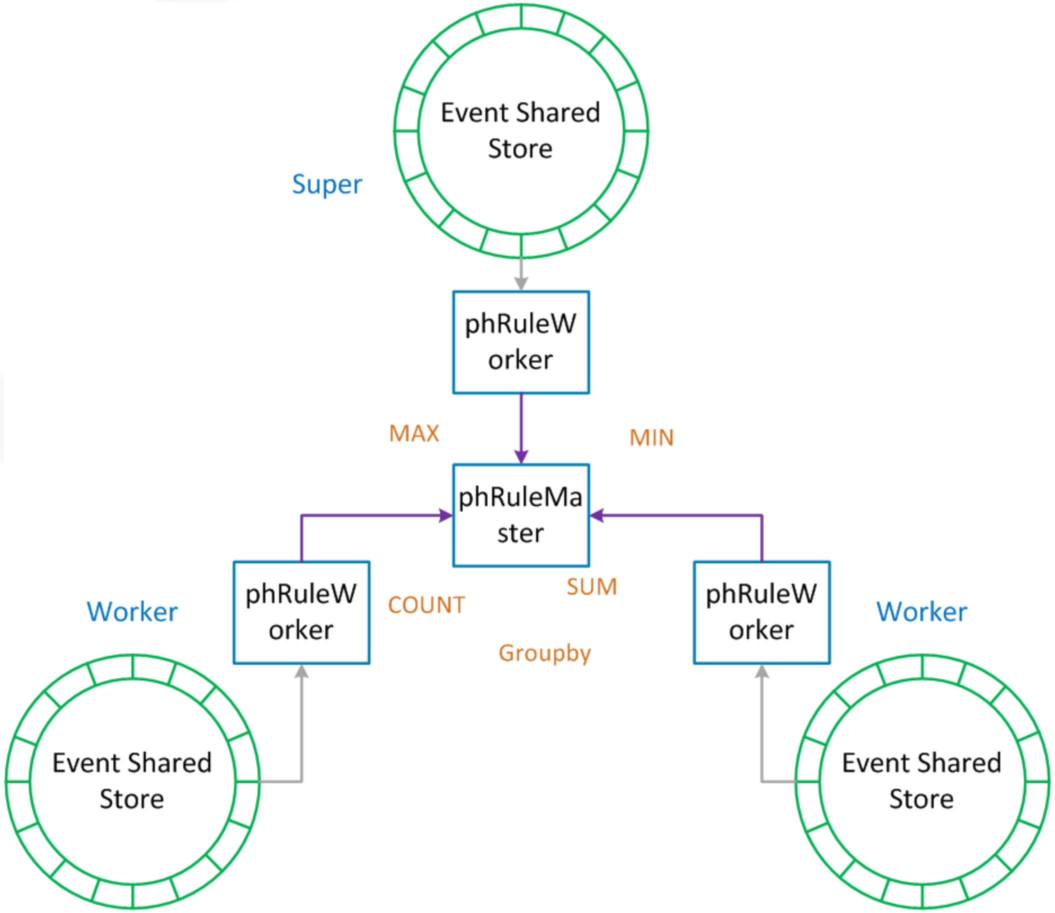
Clear Condition: *Undefined*

Edit...
Add Subpattern
Remove Selected Subpattern
Add Subpattern Relationship
Remove Selected Relationship
Edit...
Edit...
Remove
Edit...
Remove

Rest API: https://192.168.20.116/phoenix/rest/dataRequest/rule
Rest API: https://192.168.20.116/phoenix/rest/dataRequest/ruleException

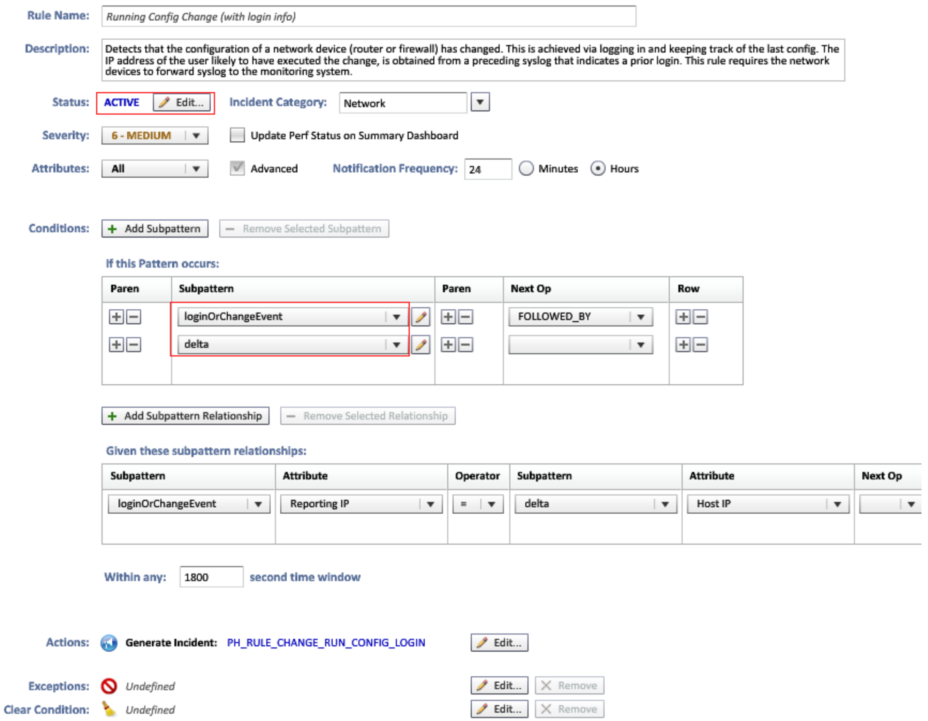
Data Analysis – Rule

- Rule Worker
  - Select Event
  - Pack Event
- Rule Master
  - Aggregator
  - Pattern Relationship
  - Incident Firing
  - Incident Clear



Data Analysis – Rule

- Rule Worker



Rule Name: Running Config Change (with login info)

Description: Detects that the configuration of a network device (router or firewall) has changed. This is achieved via logging in and keeping track of the last config. The IP address of the user likely to have executed the change, is obtained from a preceding syslog that indicates a prior login. This rule requires the network devices to forward syslog to the monitoring system.

Status: ACTIVE Edit... Incident Category: Network

Severity: 6 - MEDIUM □ Update Perf Status on Summary Dashboard

Attributes: All ☑ Advanced Notification Frequency: 24 ○ Minutes ● Hours

Conditions: + Add Subpattern — Remove Selected Subpattern

If this Pattern occurs:

Paren	Subpattern	Paren	Next Op	Row
⊞⊟	loginOrChangeEvent	⊞⊟	FOLLOWED_BY	⊞⊟
⊞⊟	delta	⊞⊟		⊞⊟

+ Add Subpattern Relationship — Remove Selected Relationship

Given these subpattern relationships:

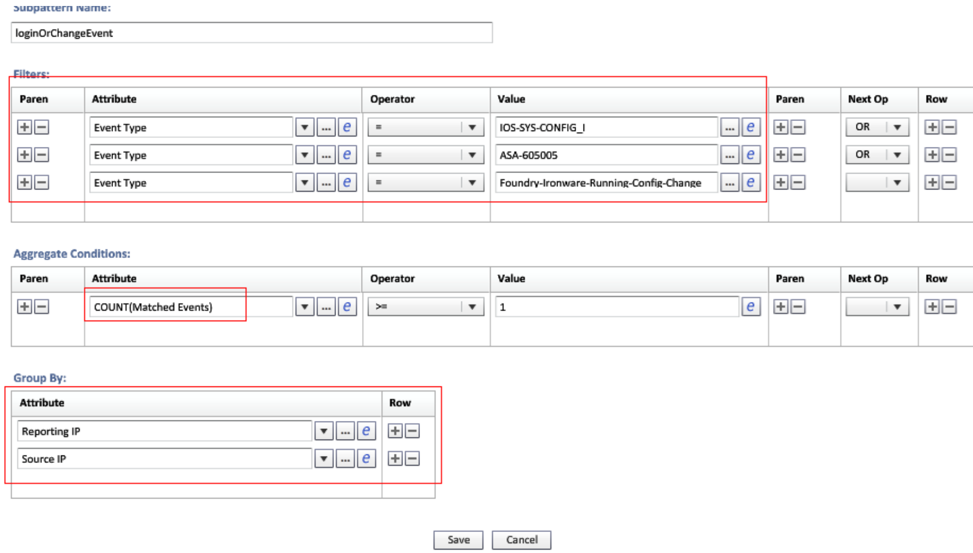
Subpattern	Attribute	Operator	Subpattern	Attribute	Next Op
loginOrChangeEvent	Reporting IP	=	delta	Host IP	

Within any: 1800 second time window

Actions: Generate Incident: PH_RULE_CHANGE_RUN_CONFIG_LOGIN Edit...

Exceptions: Undefined Edit... Remove

Clear Condition: Undefined Edit... Remove



Subpattern Name: loginOrChangeEvent

Filters:

Paren	Attribute	Operator	Value	Paren	Next Op	Row
⊞⊟	Event Type	=	IOS-SYS-CONFIG_I	⊞⊟	OR	⊞⊟
⊞⊟	Event Type	=	ASA-605005	⊞⊟	OR	⊞⊟
⊞⊟	Event Type	=	Foundry-Ironware-Running-Config-Change	⊞⊟		⊞⊟

Aggregate Conditions:

Paren	Attribute	Operator	Value	Paren	Next Op	Row
⊞⊟	COUNT(Matched Events)	>=	1	⊞⊟		⊞⊟

Group By:

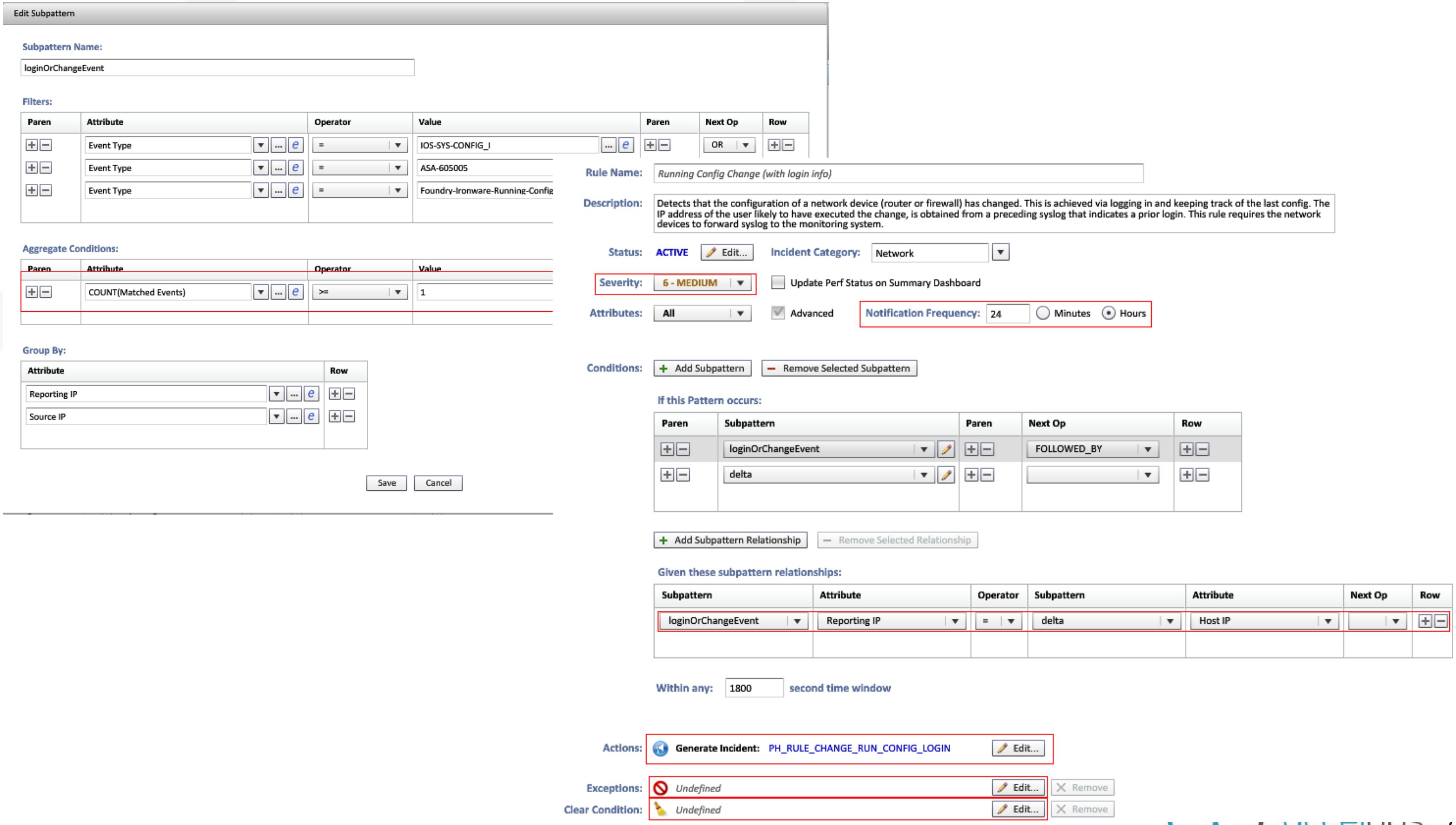
Attribute	Row
Reporting IP	⊞⊟
Source IP	⊞⊟

Save Cancel

accelops

Data Analysis – Rule

- Rule Master



Edit Subpattern

Subpattern Name: loginOrChangeEvent

Filters:

Paren	Attribute	Operator	Value	Paren	Next Op	Row
⊞⊟	Event Type	=	IOS-SYS-CONFIG_I	⊞⊟	OR	⊞⊟
⊞⊟	Event Type	=	ASA-605005			
⊞⊟	Event Type	=	Foundry-Ironware-Running-Config			

Aggregate Conditions:

Paren	Attribute	Operator	Value
⊞⊟	COUNT(Matched Events)	>=	1

Group By:

Attribute	Row
Reporting IP	⊞⊟
Source IP	⊞⊟

Rule Name: *Running Config Change (with login info)*

Description: Detects that the configuration of a network device (router or firewall) has changed. This is achieved via logging in and keeping track of the last config. The IP address of the user likely to have executed the change, is obtained from a preceding syslog that indicates a prior login. This rule requires the network devices to forward syslog to the monitoring system.

Status: ACTIVE   **Incident Category:** Network

Severity: 6 - MEDIUM   □ Update Perf Status on Summary Dashboard

Attributes: All   ☑ Advanced   **Notification Frequency:** 24 ○ Minutes ● Hours

Conditions:

If this Pattern occurs:

Paren	Subpattern	Paren	Next Op	Row
⊞⊟	loginOrChangeEvent	⊞⊟	FOLLOWED_BY	⊞⊟
⊞⊟	delta	⊞⊟		⊞⊟

Given these subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next Op	Row
loginOrChangeEvent	Reporting IP	=	delta	Host IP		⊞⊟

Within any: 1800 **second time window**

Actions: **Generate Incident:** PH_RULE_CHANGE_RUN_CONFIG_LOGIN

Exceptions: *Undefined*

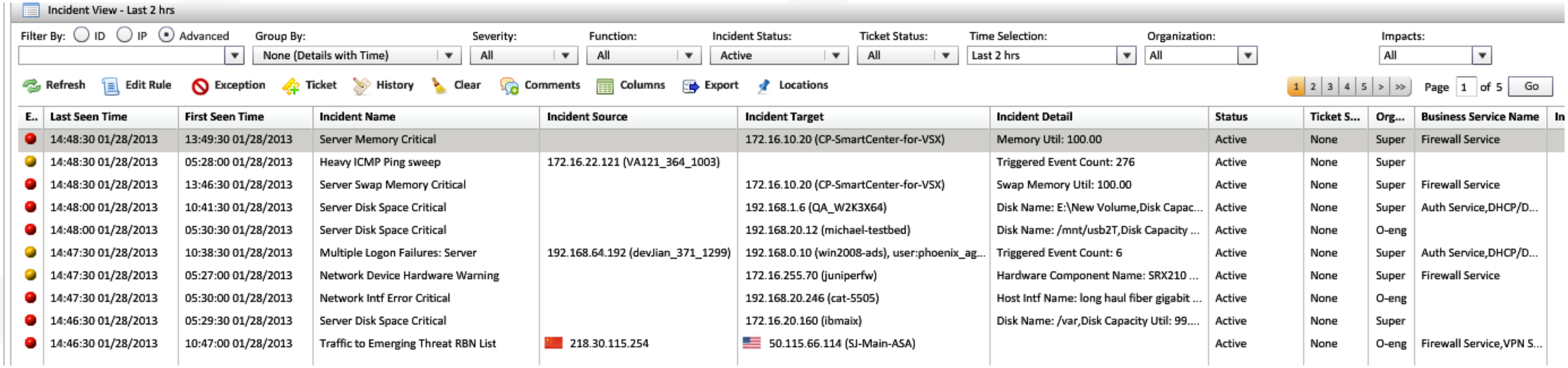
Clear Condition: *Undefined*

Data Analysis – Rule

- How to calculate aggregator distributed
  - COUNT
  - MAX
  - MIN
  - SUM
  - LAST
  - FIRST
  - AVG
  - COUNT DISTINCT
  - Percentage

Data Analysis – Rule

- Incident



Incident View - Last 2 hrs

Filter By: ○ ID ○ IP ● Advanced

Group By: None (Details with Time)

Severity: All

Function: All

Incident Status: Active

Ticket Status: All

Time Selection: Last 2 hrs

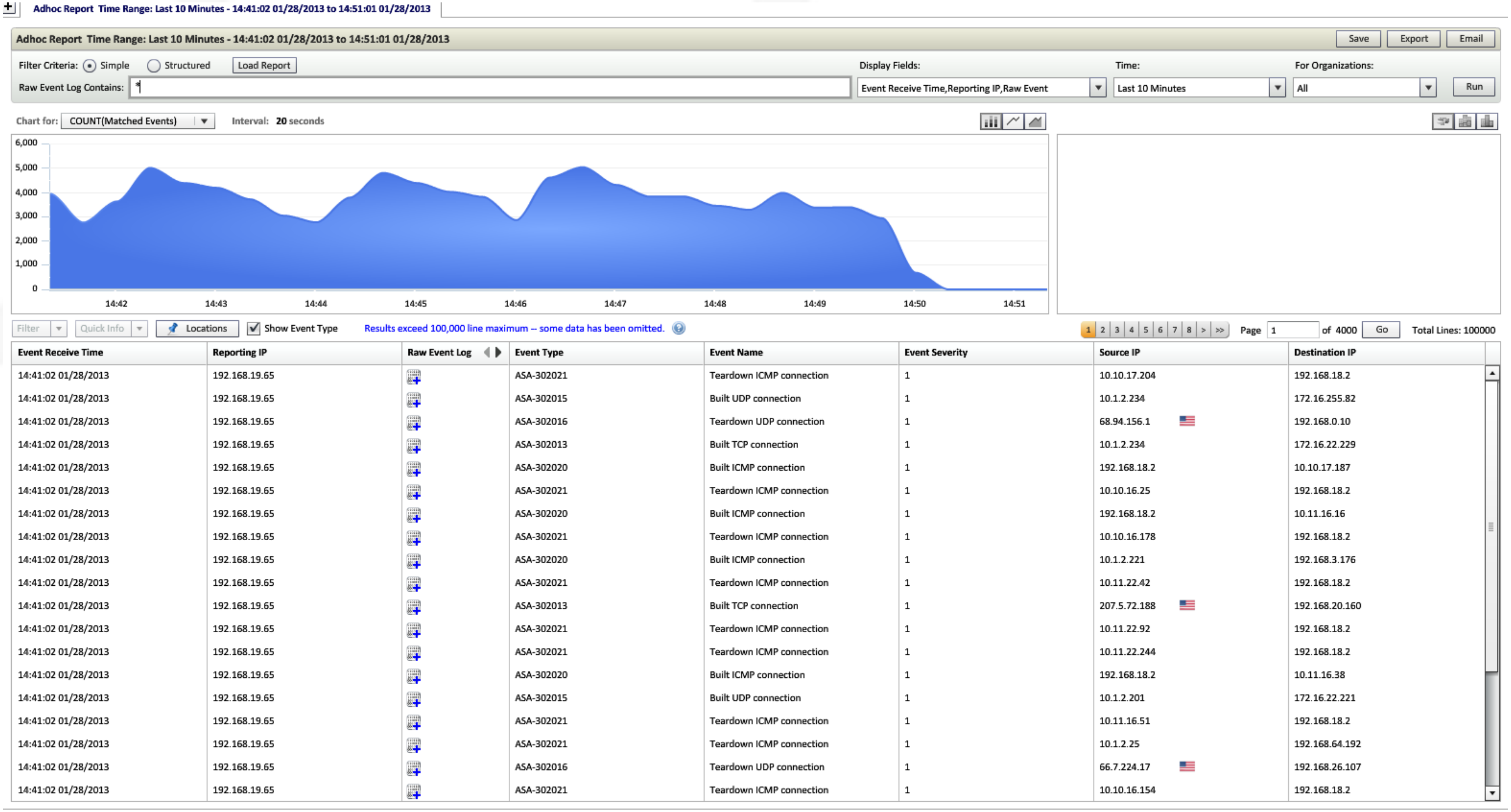
Organization: All

Impacts: All

E..	Last Seen Time	First Seen Time	Incident Name	Incident Source	Incident Target	Incident Detail	Status	Ticket S...	Org...	Business Service Name	In
●	14:48:30 01/28/2013	13:49:30 01/28/2013	Server Memory Critical		172.16.10.20 (CP-SmartCenter-for-VSX)	Memory Util: 100.00	Active	None	Super	Firewall Service	
●	14:48:30 01/28/2013	05:28:00 01/28/2013	Heavy ICMP Ping sweep	172.16.22.121 (VA121_364_1003)		Triggered Event Count: 276	Active	None	Super		
●	14:48:30 01/28/2013	13:46:30 01/28/2013	Server Swap Memory Critical		172.16.10.20 (CP-SmartCenter-for-VSX)	Swap Memory Util: 100.00	Active	None	Super	Firewall Service	
●	14:48:00 01/28/2013	10:41:30 01/28/2013	Server Disk Space Critical		192.168.1.6 (QA_W2K3X64)	Disk Name: E:\New Volume,Disk Capac...	Active	None	Super	Auth Service,DHCP/D...	
●	14:48:00 01/28/2013	05:30:30 01/28/2013	Server Disk Space Critical		192.168.20.12 (michael-testbed)	Disk Name: /mnt/usb2T,Disk Capacity ...	Active	None	O-eng		
●	14:47:30 01/28/2013	10:38:30 01/28/2013	Multiple Logon Failures: Server	192.168.64.192 (devJian_371_1299)	192.168.0.10 (win2008-ads), user:phoenix_ag...	Triggered Event Count: 6	Active	None	Super	Auth Service,DHCP/D...	
●	14:47:30 01/28/2013	05:27:00 01/28/2013	Network Device Hardware Warning		172.16.255.70 (juniperfw)	Hardware Component Name: SRX210 ...	Active	None	Super	Firewall Service	
●	14:47:30 01/28/2013	05:30:00 01/28/2013	Network Intf Error Critical		192.168.20.246 (cat-5505)	Host Intf Name: long haul fiber gigabit ...	Active	None	O-eng		
●	14:46:30 01/28/2013	05:29:30 01/28/2013	Server Disk Space Critical		172.16.20.160 (ibmaix)	Disk Name: /var,Disk Capacity Util: 99....	Active	None	Super		
●	14:46:30 01/28/2013	10:47:00 01/28/2013	Traffic to Emerging Threat RBN List	218.30.115.254	50.115.66.114 (SJ-Main-ASA)		Active	None	O-eng	Firewall Service,VPN S...	

Data Analysis – Report

- Ad hoc query – Historical Search



Adhoc Report Time Range: Last 10 Minutes - 14:41:02 01/28/2013 to 14:51:01 01/28/2013

Adhoc Report Time Range: Last 10 Minutes - 14:41:02 01/28/2013 to 14:51:01 01/28/2013

Filter Criteria: ● Simple ○ Structured

Raw Event Log Contains: *

Display Fields: Event Receive Time,Reporting IP,Raw Event

Time: Last 10 Minutes

For Organizations: All

Chart for: COUNT(Matched Events)

Interval: **20** seconds

☑ Show Event Type

Results exceed 100,000 line maximum -- some data has been omitted.

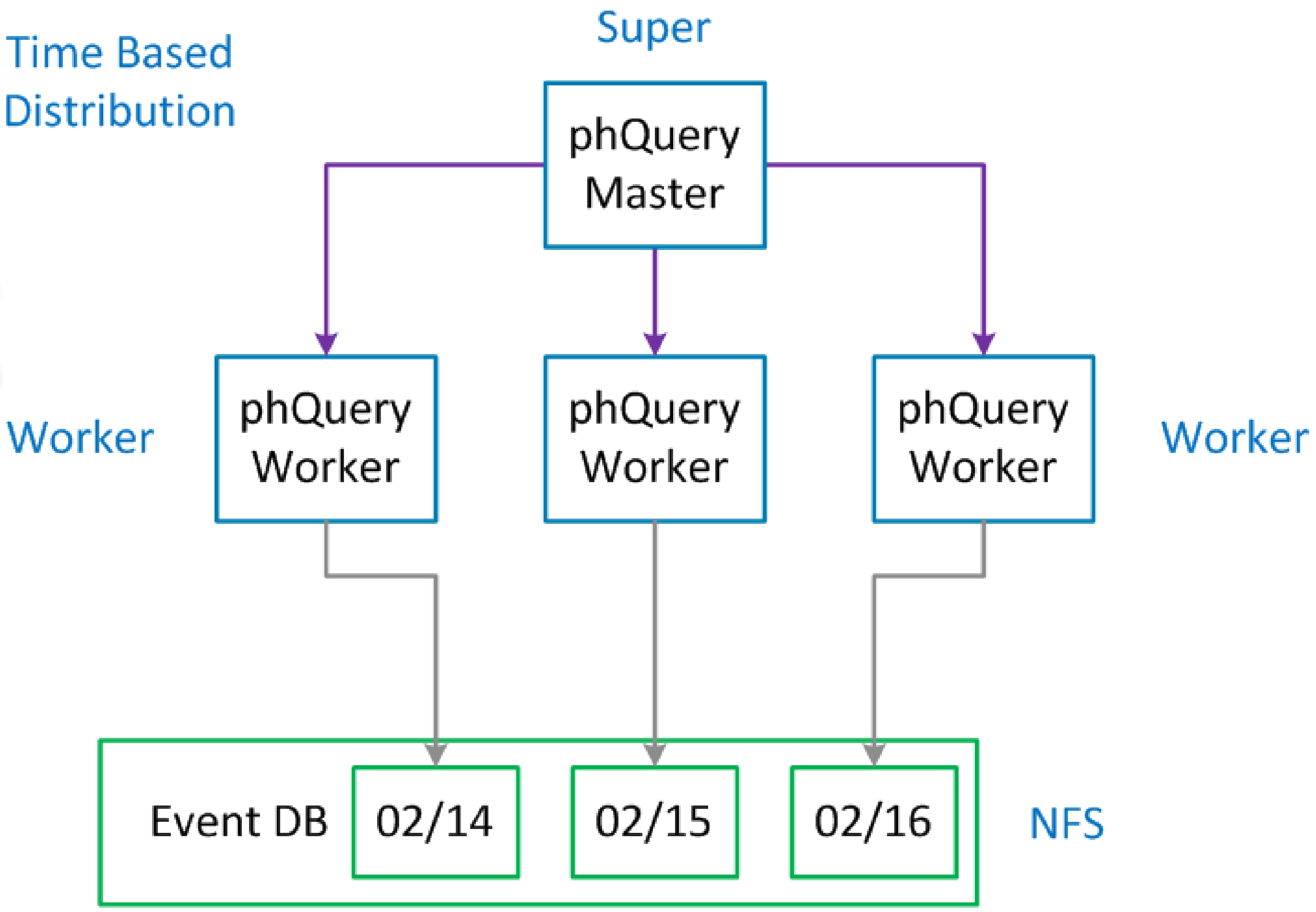
Page 1 of 4000

Total Lines: 100000

Event Receive Time	Reporting IP	Raw Event Log	Event Type	Event Name	Event Severity	Source IP	Destination IP
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.10.17.204	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302015	Built UDP connection	1	10.1.2.234	172.16.255.82
14:41:02 01/28/2013	192.168.19.65		ASA-302016	Teardown UDP connection	1	68.94.156.1	192.168.0.10
14:41:02 01/28/2013	192.168.19.65		ASA-302013	Built TCP connection	1	10.1.2.234	172.16.22.229
14:41:02 01/28/2013	192.168.19.65		ASA-302020	Built ICMP connection	1	192.168.18.2	10.10.17.187
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.10.16.25	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302020	Built ICMP connection	1	192.168.18.2	10.11.16.16
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.10.16.178	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302020	Built ICMP connection	1	10.1.2.221	192.168.3.176
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.11.22.42	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302013	Built TCP connection	1	207.5.72.188	192.168.20.160
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.11.22.92	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.11.22.244	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302020	Built ICMP connection	1	192.168.18.2	10.11.16.38
14:41:02 01/28/2013	192.168.19.65		ASA-302015	Built UDP connection	1	10.1.2.201	172.16.22.221
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.11.16.51	192.168.18.2
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.1.2.25	192.168.64.192
14:41:02 01/28/2013	192.168.19.65		ASA-302016	Teardown UDP connection	1	66.7.224.17	192.168.26.107
14:41:02 01/28/2013	192.168.19.65		ASA-302021	Teardown ICMP connection	1	10.10.16.154	192.168.18.2

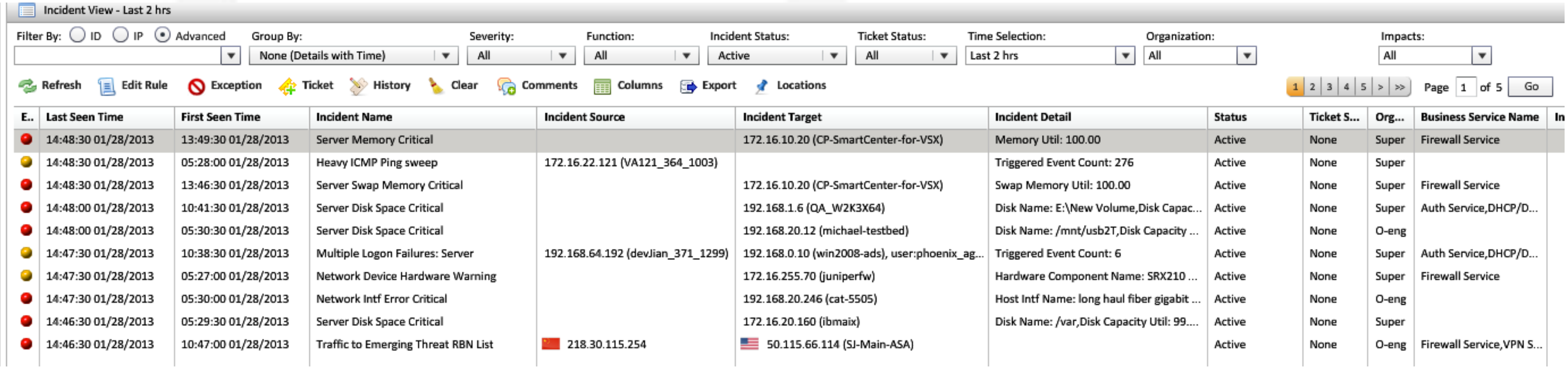
Data Analysis – Report

- Ad hoc query



Data Analysis – Report

- Ad hoc query – Incident Page

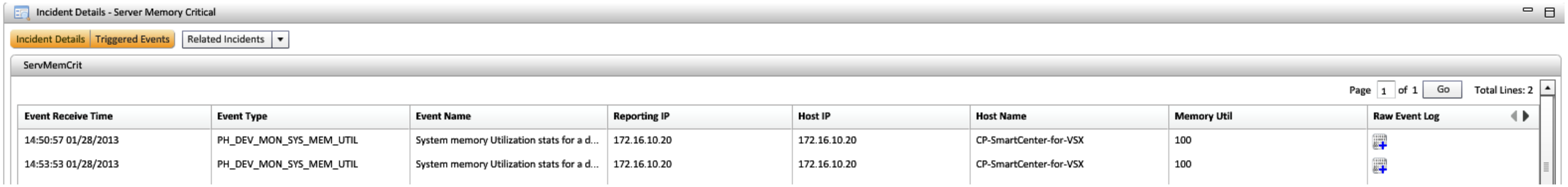


Incident View - Last 2 hrs

Filter By: ○ ID ○ IP ● Advanced | Group By: None (Details with Time) | Severity: All | Function: All | Incident Status: Active | Ticket Status: All | Time Selection: Last 2 hrs | Organization: All | Impacts: All

E..	Last Seen Time	First Seen Time	Incident Name	Incident Source	Incident Target	Incident Detail	Status	Ticket S...	Org...	Business Service Name	In
●	14:48:30 01/28/2013	13:49:30 01/28/2013	Server Memory Critical		172.16.10.20 (CP-SmartCenter-for-VSX)	Memory Util: 100.00	Active	None	Super	Firewall Service	
●	14:48:30 01/28/2013	05:28:00 01/28/2013	Heavy ICMP Ping sweep	172.16.22.121 (VA121_364_1003)		Triggered Event Count: 276	Active	None	Super		
●	14:48:30 01/28/2013	13:46:30 01/28/2013	Server Swap Memory Critical		172.16.10.20 (CP-SmartCenter-for-VSX)	Swap Memory Util: 100.00	Active	None	Super	Firewall Service	
●	14:48:00 01/28/2013	10:41:30 01/28/2013	Server Disk Space Critical		192.168.1.6 (QA_W2K3X64)	Disk Name: E:\New Volume,Disk Capac...	Active	None	Super	Auth Service,DHCP/D...	
●	14:48:00 01/28/2013	05:30:30 01/28/2013	Server Disk Space Critical		192.168.20.12 (michael-testbed)	Disk Name: /mnt/usb2T,Disk Capacity ...	Active	None	O-eng		
●	14:47:30 01/28/2013	10:38:30 01/28/2013	Multiple Logon Failures: Server	192.168.64.192 (devJian_371_1299)	192.168.0.10 (win2008-ads), user:phoenix_ag...	Triggered Event Count: 6	Active	None	Super	Auth Service,DHCP/D...	
●	14:47:30 01/28/2013	05:27:00 01/28/2013	Network Device Hardware Warning		172.16.255.70 (juniperfw)	Hardware Component Name: SRX210 ...	Active	None	Super	Firewall Service	
●	14:47:30 01/28/2013	05:30:00 01/28/2013	Network Intf Error Critical		192.168.20.246 (cat-5505)	Host Intf Name: long haul fiber gigabit ...	Active	None	O-eng		
●	14:46:30 01/28/2013	05:29:30 01/28/2013	Server Disk Space Critical		172.16.20.160 (ibmaix)	Disk Name: /var,Disk Capacity Util: 99....	Active	None	Super		
●	14:46:30 01/28/2013	10:47:00 01/28/2013	Traffic to Emerging Threat RBN List	218.30.115.254	50.115.66.114 (SJ-Main-ASA)		Active	None	O-eng	Firewall Service,VPN S...	

- Ad hoc query – Trigger Event



Incident Details - Server Memory Critical

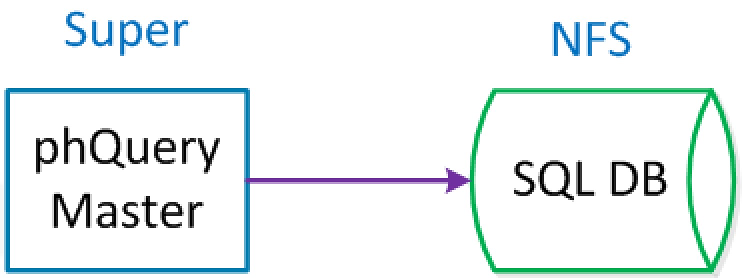
ServMemCrit

Page 1 of 1 Go Total Lines: 2

Event Receive Time	Event Type	Event Name	Reporting IP	Host IP	Host Name	Memory Util	Raw Event Log
14:50:57 01/28/2013	PH_DEV_MON_SYS_MEM_UTIL	System memory Utilization stats for a d...	172.16.10.20	172.16.10.20	CP-SmartCenter-for-VSX	100	
14:53:53 01/28/2013	PH_DEV_MON_SYS_MEM_UTIL	System memory Utilization stats for a d...	172.16.10.20	172.16.10.20	CP-SmartCenter-for-VSX	100	

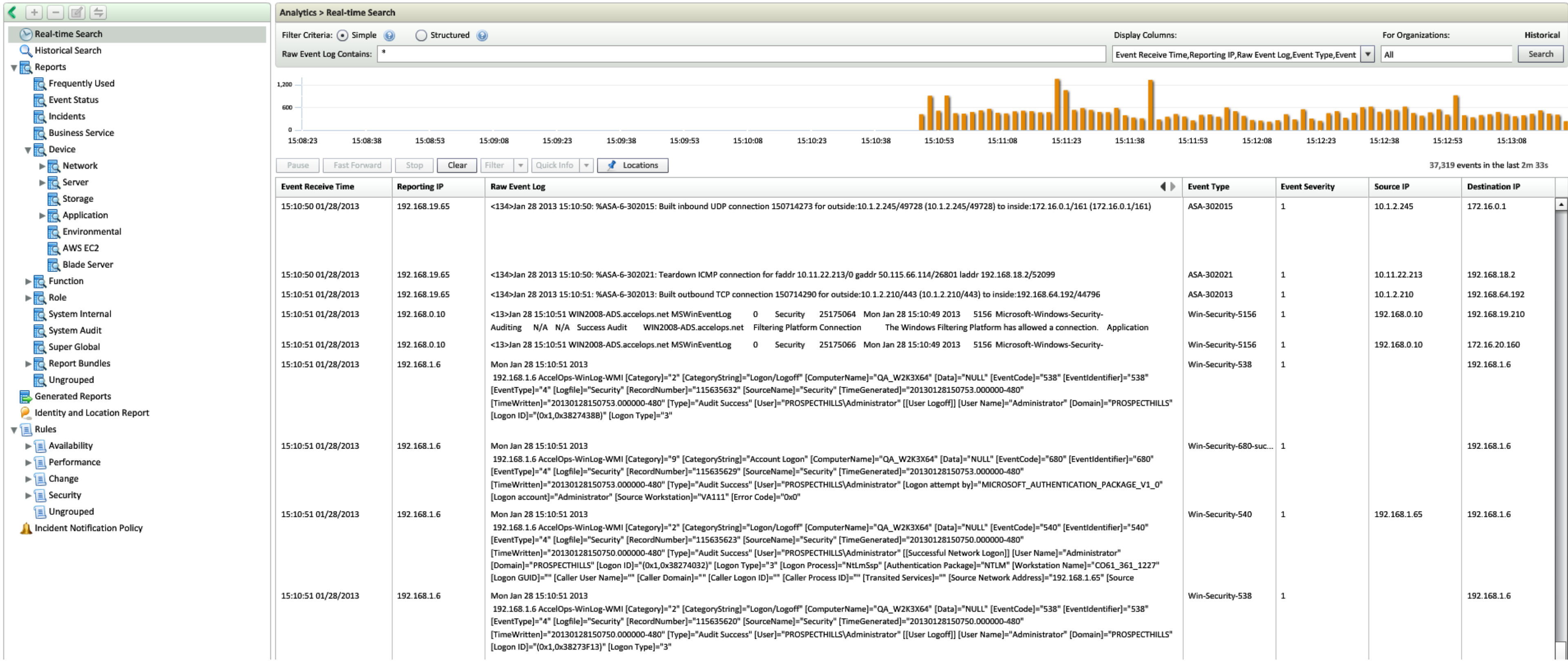
Data Analysis – Report

- Ad hoc query – Incident
  - Why?



Data Analysis – Report

- Real Time Query



Filter Criteria: ● Simple ○ Structured

Raw Event Log Contains: *

Display Columns: Event Receive Time,Reporting IP,Raw Event Log,Event Type,Event

For Organizations: All

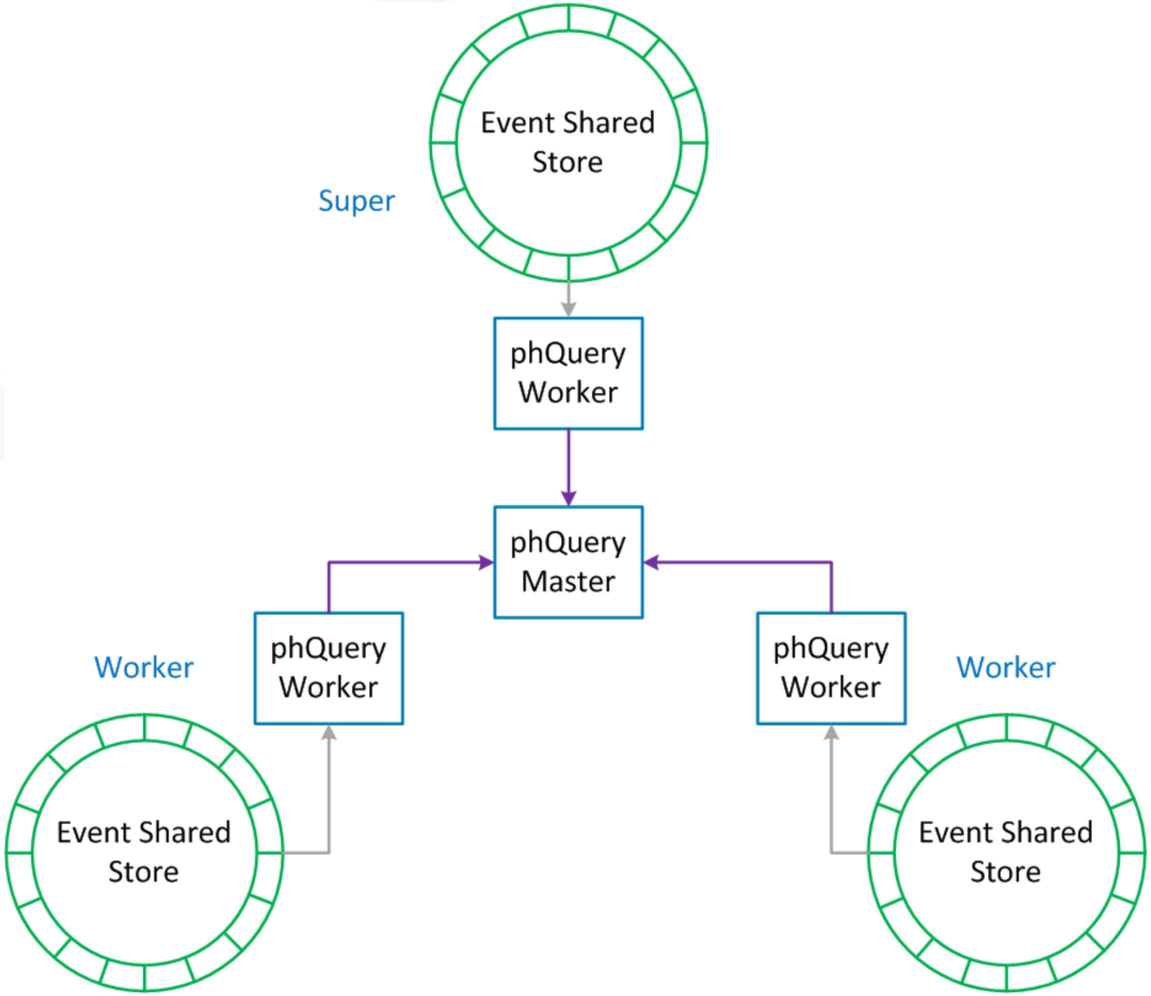
37,319 events in the last 2m 33s

Event Receive Time	Reporting IP	Raw Event Log	Event Type	Event Severity	Source IP	Destination IP
15:10:50 01/28/2013	192.168.19.65	<134>Jan 28 2013 15:10:50: %ASA-6-302015: Built inbound UDP connection 150714273 for outside:10.1.2.245/49728 (10.1.2.245/49728) to inside:172.16.0.1/161 (172.16.0.1/161)	ASA-302015	1	10.1.2.245	172.16.0.1
15:10:50 01/28/2013	192.168.19.65	<134>Jan 28 2013 15:10:50: %ASA-6-302021: Teardown ICMP connection for faddr 10.11.22.213/0 gaddr 50.115.66.114/26801 laddr 192.168.18.2/52099	ASA-302021	1	10.11.22.213	192.168.18.2
15:10:51 01/28/2013	192.168.19.65	<134>Jan 28 2013 15:10:51: %ASA-6-302013: Built outbound TCP connection 150714290 for outside:10.1.2.210/443 (10.1.2.210/443) to inside:192.168.64.192/44796	ASA-302013	1	10.1.2.210	192.168.64.192
15:10:51 01/28/2013	192.168.0.10	<13>Jan 28 15:10:51 WIN2008-ADS.accelops.net MSWinEventLog 0 Security 25175064 Mon Jan 28 15:10:49 2013 5156 Microsoft-Windows-Security- Auditing N/A N/A Success Audit WIN2008-ADS.accelops.net Filtering Platform Connection The Windows Filtering Platform has allowed a connection. Application	Win-Security-5156	1	192.168.0.10	192.168.19.210
15:10:51 01/28/2013	192.168.0.10	<13>Jan 28 15:10:51 WIN2008-ADS.accelops.net MSWinEventLog 0 Security 25175066 Mon Jan 28 15:10:49 2013 5156 Microsoft-Windows-Security-	Win-Security-5156	1	192.168.0.10	172.16.20.160
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="2" [CategoryString]="Logon/Logoff" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="538" [EventIdentifier]="538" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635632" [SourceName]="Security" [TimeGenerated]="20130128150753.000000-480" [TimeWritten]="20130128150753.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [[User Logoff]] [User Name]="Administrator" [Domain]="PROSPECTHILLS" [Logon ID]="(0x1,0x3827438B)" [Logon Type]="3"	Win-Security-538	1		192.168.1.6
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="9" [CategoryString]="Account Logon" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="680" [EventIdentifier]="680" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635629" [SourceName]="Security" [TimeGenerated]="20130128150753.000000-480" [TimeWritten]="20130128150753.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [Logon attempt by]="MICROSOFT_AUTHENTICATION_PACKAGE_V1_0" [Logon account]="Administrator" [Source Workstation]="VA111" [Error Code]="0x0"	Win-Security-680-suc...	1		192.168.1.6
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="2" [CategoryString]="Logon/Logoff" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="540" [EventIdentifier]="540" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635623" [SourceName]="Security" [TimeGenerated]="20130128150750.000000-480" [TimeWritten]="20130128150750.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [[Successful Network Logon]] [User Name]="Administrator" [Domain]="PROSPECTHILLS" [Logon ID]="(0x1,0x38274032)" [Logon Type]="3" [Logon Process]="NtLmSsp" [Authentication Package]="NTLM" [Workstation Name]="CO61_361_1227" [Logon GUID]="" [Caller User Name]="" [Caller Domain]="" [Caller Logon ID]="" [Caller Process ID]="" [Transited Services]="" [Source Network Address]="192.168.1.65" [Source	Win-Security-540	1	192.168.1.65	192.168.1.6
15:10:51 01/28/2013	192.168.1.6	Mon Jan 28 15:10:51 2013 192.168.1.6 AccelOps-WinLog-WMI [Category]="2" [CategoryString]="Logon/Logoff" [ComputerName]="QA_W2K3X64" [Data]="NULL" [EventCode]="538" [EventIdentifier]="538" [EventType]="4" [Logfile]="Security" [RecordNumber]="115635620" [SourceName]="Security" [TimeGenerated]="20130128150750.000000-480" [TimeWritten]="20130128150750.000000-480" [Type]="Audit Success" [User]="PROSPECTHILLS\Administrator" [[User Logoff]] [User Name]="Administrator" [Domain]="PROSPECTHILLS" [Logon ID]="(0x1,0x38273F13)" [Logon Type]="3"	Win-Security-538	1		192.168.1.6

accelops

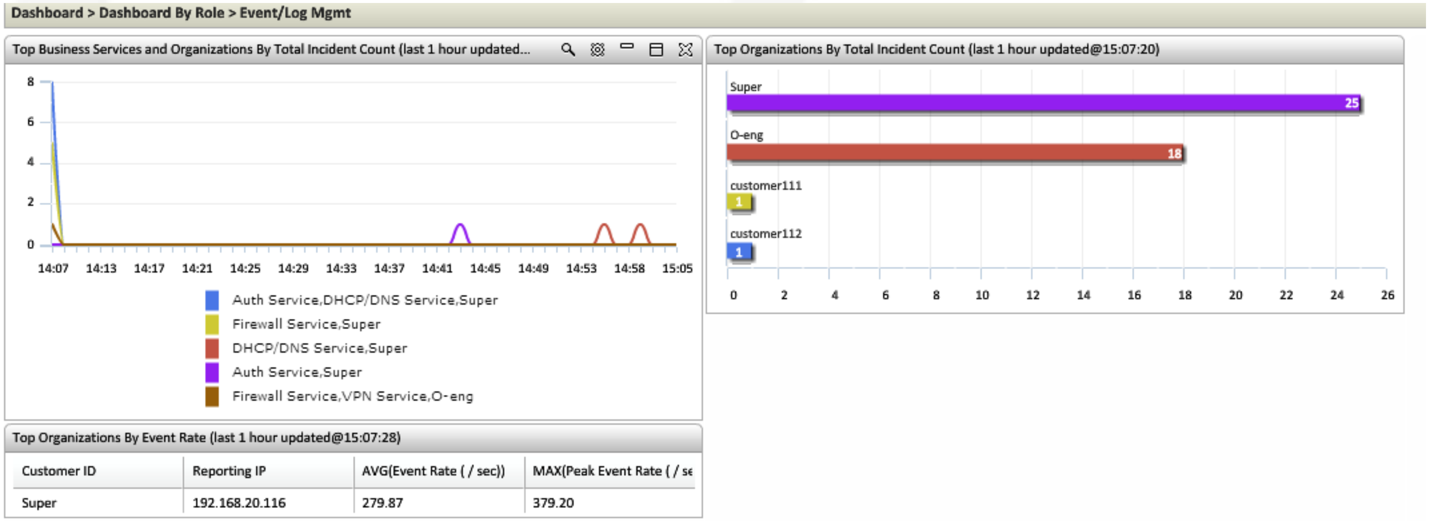
Data Analysis – Report

- Real Time Query



Data Analysis – Report

- Inline Query – Dashboard
  - Long term query



Dashboard > Dashboard By Role > Event/Log Mgmt

Top Business Services and Organizations By Total Incident Count (last 1 hour updated...

Top Organizations By Total Incident Count (last 1 hour updated@15:07:20)

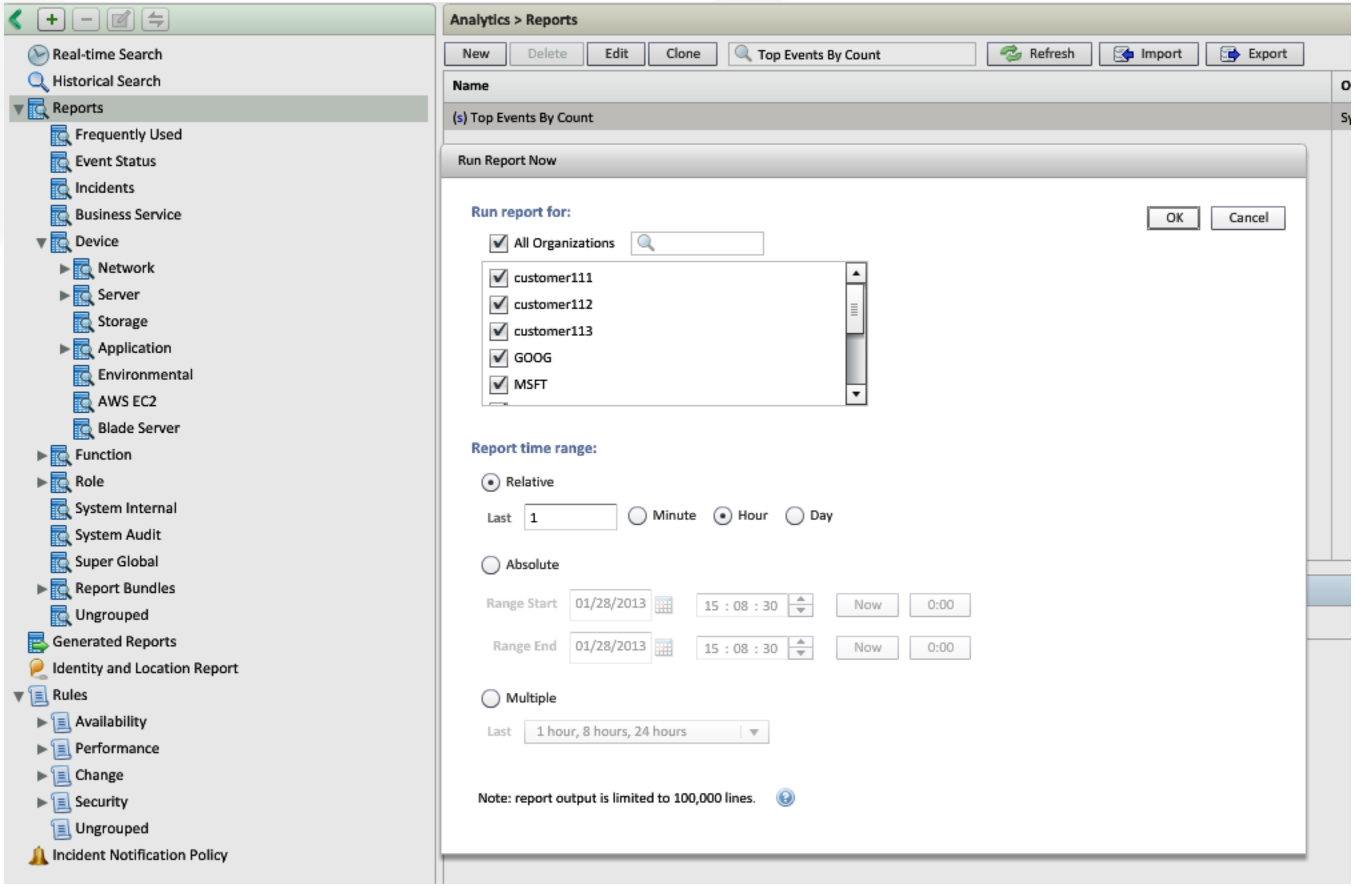
Top Organizations By Event Rate (last 1 hour updated@15:07:28)

Customer ID	Reporting IP	AVG(Event Rate (/ sec))	MAX(Peak Event Rate (/ se
Super	192.168.20.116	279.87	379.20

Rest API: https://192.168.20.116/phoenix/rest/dataRequest/report

Data Analysis – Report

- Inline Query – Run From Report



Run report for:

☑ All Organizations

☑ customer111
☑ customer112
☑ customer113
☑ GOOG
☑ MSFT

Report time range:

● Relative

Last 1 ○ Minute ● Hour ○ Day

○ Absolute

Range Start 01/28/2013 15 : 08 : 30 Now 0:00

Range End 01/28/2013 15 : 08 : 30 Now 0:00

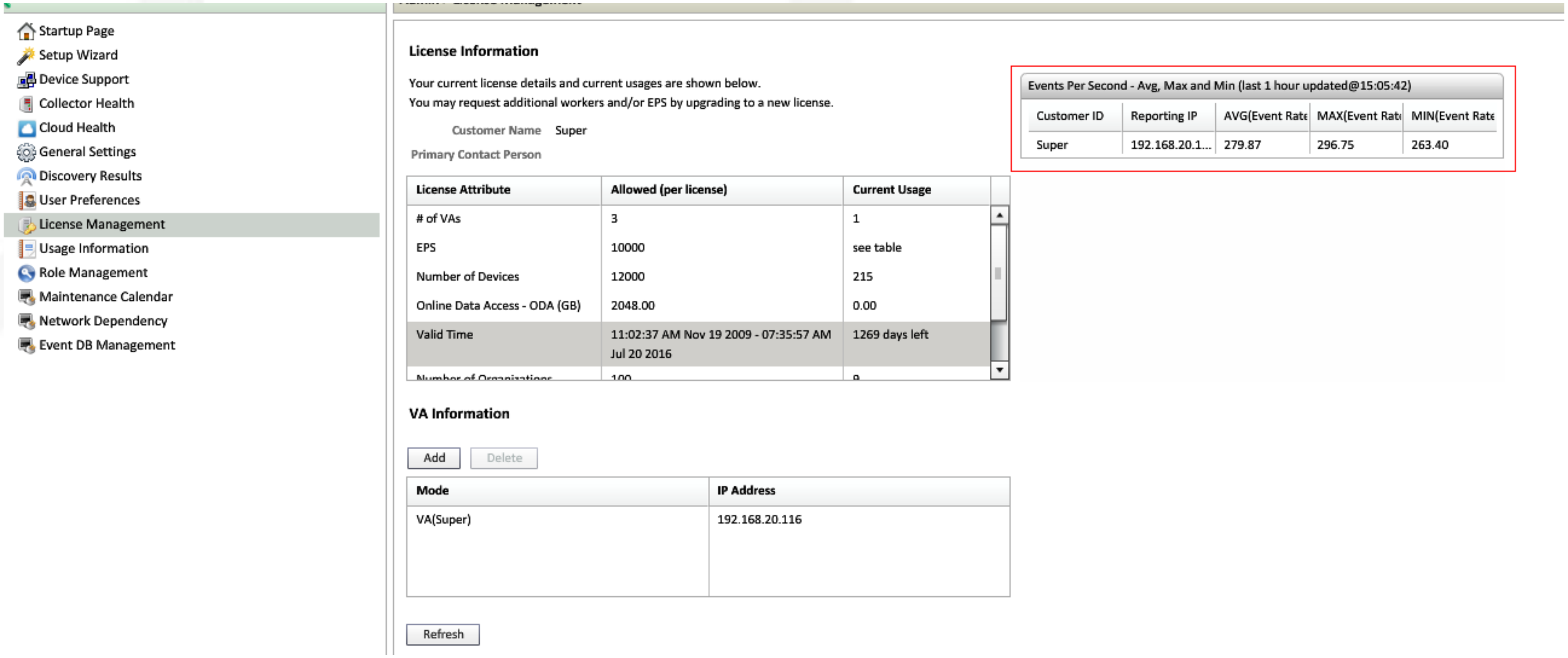
○ Multiple

Last 1 hour, 8 hours, 24 hours

Note: report output is limited to 100,000 lines.

Data Analysis – Report

- Inline Query – Other



License Information

Your current license details and current usages are shown below.
You may request additional workers and/or EPS by upgrading to a new license.

Customer Name Super

Primary Contact Person

License Attribute	Allowed (per license)	Current Usage
# of VAs	3	1
EPS	10000	see table
Number of Devices	12000	215
Online Data Access - ODA (GB)	2048.00	0.00
Valid Time	11:02:37 AM Nov 19 2009 - 07:35:57 AM Jul 20 2016	1269 days left
Number of Organizations	100	9

Events Per Second - Avg, Max and Min (last 1 hour updated@15:05:42)

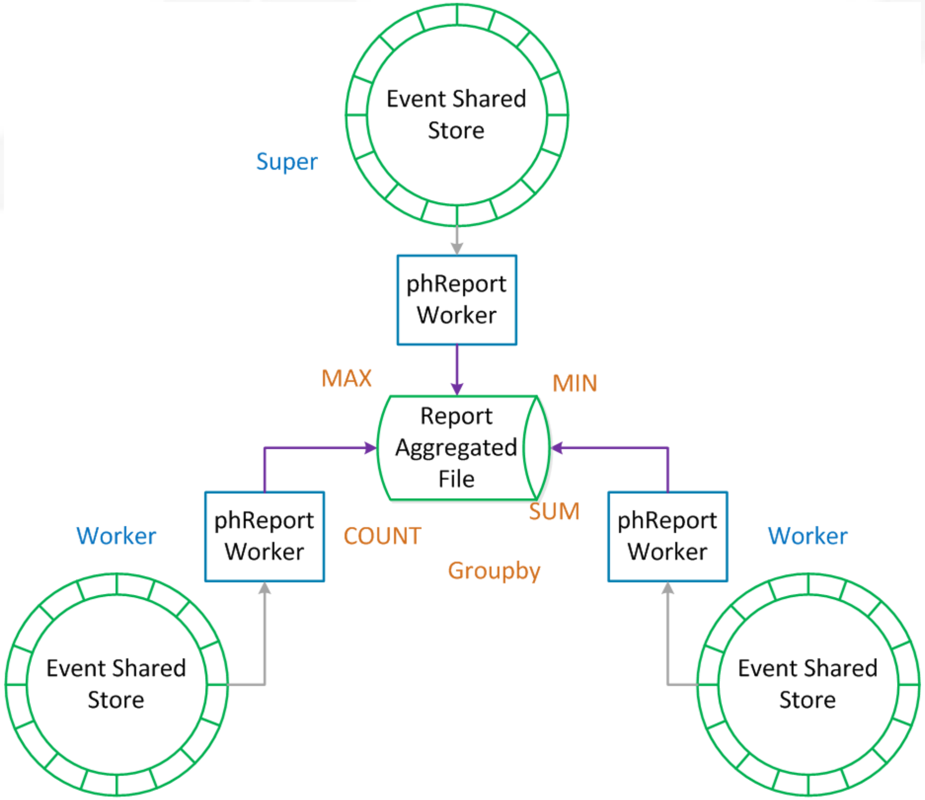
Customer ID	Reporting IP	AVG(Event Rate	MAX(Event Rat	MIN(Event Rate
Super	192.168.20.1...	279.87	296.75	263.40

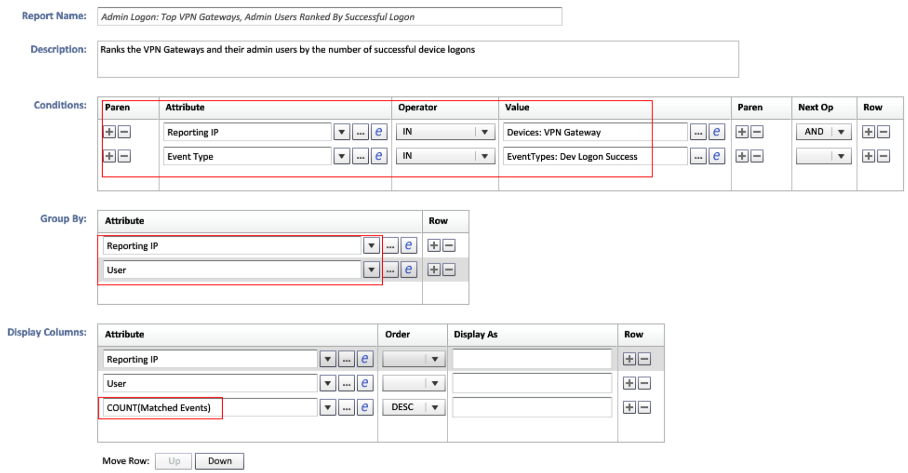
VA Information

Mode	IP Address
VA(Super)	192.168.20.116

Data Analysis – Report

- Inline Query
  - Optimize – Report Engine
    - Predefined Inline Report
    - Aggregated Middle Result





Report Name: *Admin Logon: Top VPN Gateways, Admin Users Ranked By Successful Logon*

Description: Ranks the VPN Gateways and their admin users by the number of successful device logons

Conditions:

Paren	Attribute	Operator	Value	Paren	Next Op	Row
⊞ ⊟	Reporting IP	IN	Devices: VPN Gateway	⊞ ⊟	AND	⊞ ⊟
⊞ ⊟	Event Type	IN	EventTypes: Dev Logon Success	⊞ ⊟		⊞ ⊟

Group By:

Attribute	Row
Reporting IP	⊞ ⊟
User	⊞ ⊟

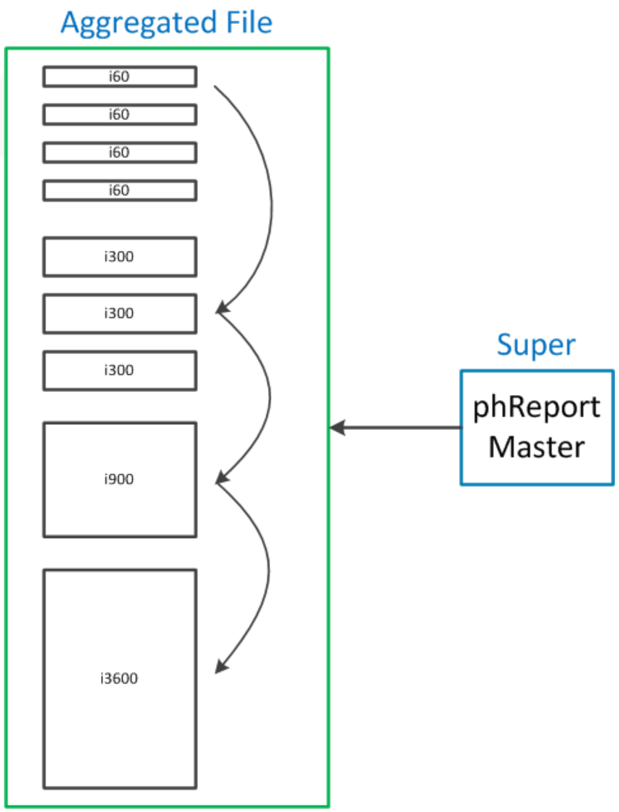
Display Columns:

Attribute	Order	Display As	Row
Reporting IP			⊞ ⊟
User			⊞ ⊟
COUNT(Matched Events)	DESC		⊞ ⊟

Move Row: Up Down

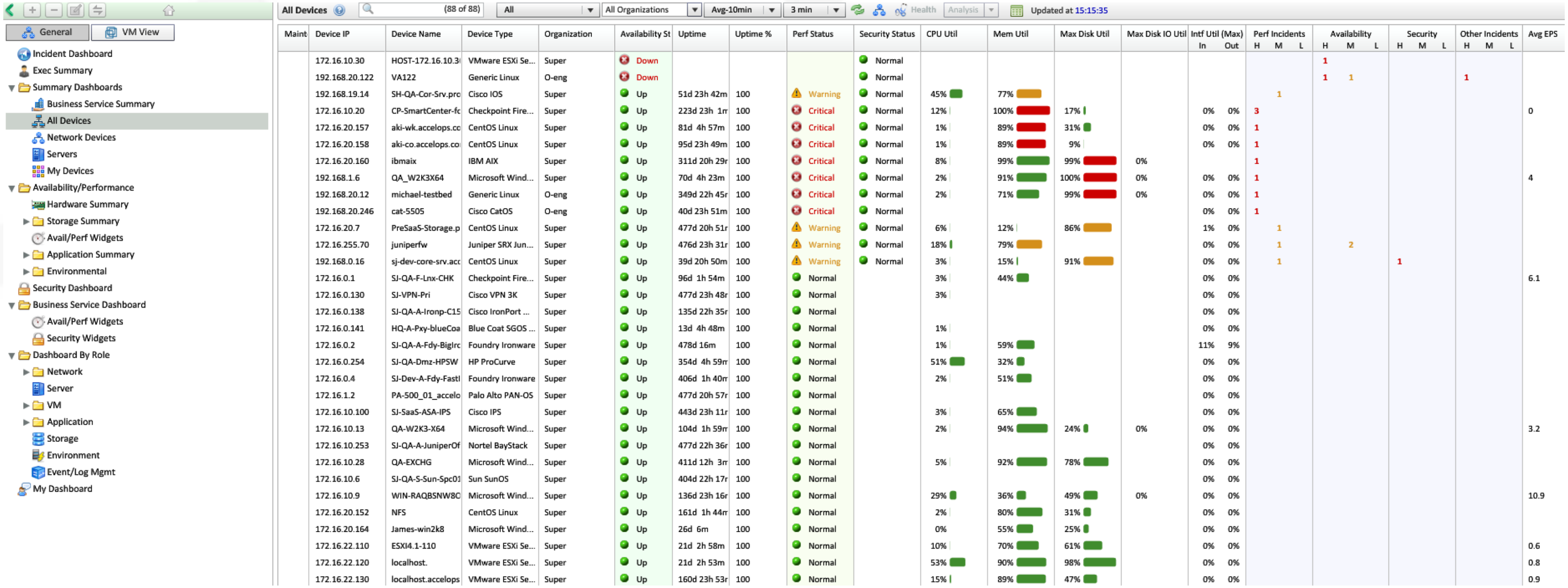
Data Analysis – Report

- Inline Query
  - Optimize – Report Master
    - From (0, 5100)
    - To (0, 3600), (3600, 4500), (4500, 4800), (4800, 5100)



Data Analysis – Report

- Summary – Dashboard
  - Short term query but frequently called

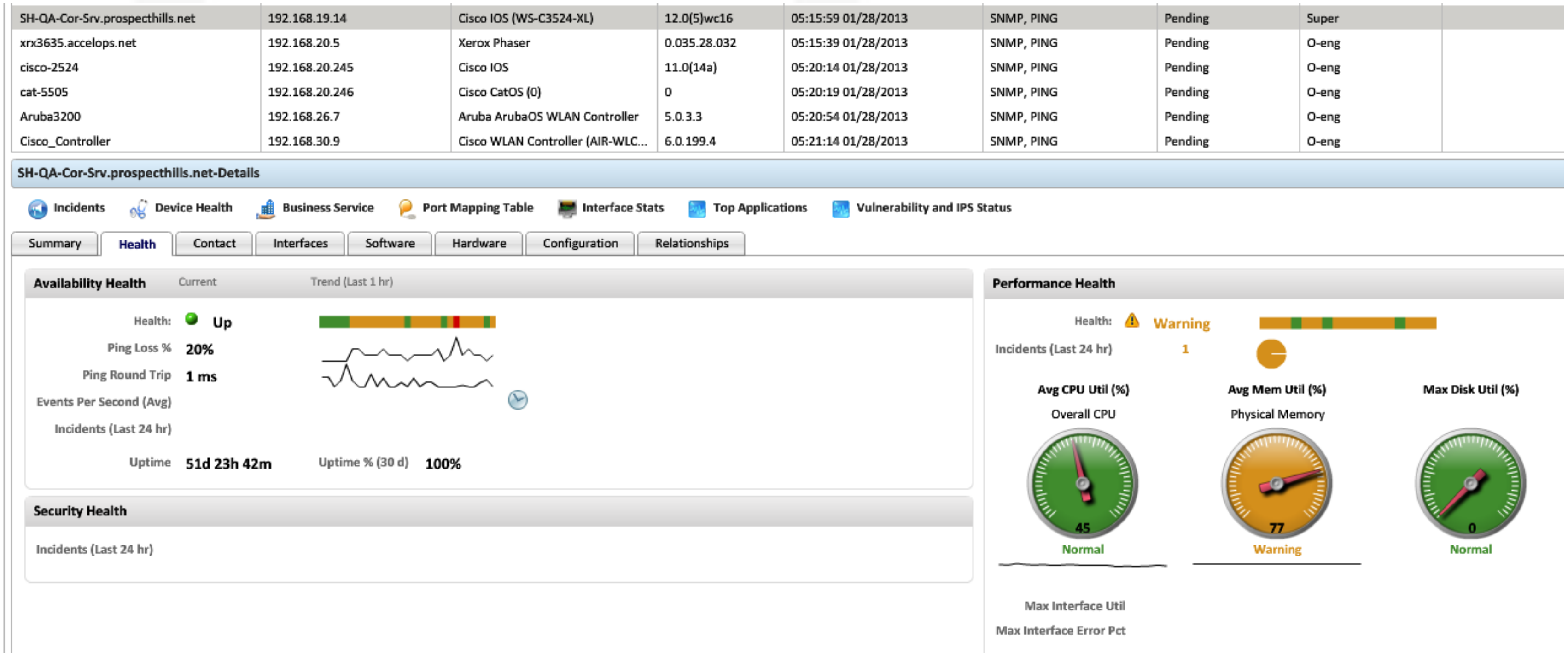


Updated at 15:15:35

Maint	Device IP	Device Name	Device Type	Organization	Availability St	Uptime	Uptime %	Perf Status	Security Status	CPU Util	Mem Util	Max Disk Util	Max Disk IO Util	Intf Util (Max)		Perf Incidents			Availability			Security			Other Incidents			Avg EPS
														In	Out	H	M	L	H	M	L	H	M	L	H	M	L	
	172.16.10.30	HOST-172.16.10.3	VMware ESXi Se...	Super	Down				Normal										1									
	192.168.20.122	VA122	Generic Linux	O-eng	Down				Normal										1	1					1			
	192.168.19.14	SH-QA-Cor-Srv.pro	Cisco IOS	Super	Up	51d 23h 42m	100	Warning	Normal	45%	77%						1											
	172.16.10.20	CP-SmartCenter-fc	Checkpoint Fire...	Super	Up	223d 23h 1m	100	Critical	Normal	12%	100%	17%		0%	0%	3												0
	172.16.20.157	aki-wk.accelops.co	CentOS Linux	Super	Up	81d 4h 57m	100	Critical	Normal	1%	89%	31%		0%	0%	1												
	172.16.20.158	aki-co.accelops.co	CentOS Linux	Super	Up	95d 23h 49m	100	Critical	Normal	1%	89%	9%		0%	0%	1												
	172.16.20.160	ibmaix	IBM AIX	Super	Up	311d 20h 29r	100	Critical	Normal	8%	99%	99%	0%			1												
	192.168.1.6	QA_W2K3X64	Microsoft Wind...	Super	Up	70d 4h 23m	100	Critical	Normal	2%	91%	100%	0%	0%	0%	1												4
	192.168.20.12	michael-testbed	Generic Linux	O-eng	Up	349d 22h 45r	100	Critical	Normal	2%	71%	99%	0%	0%	0%	1												
	192.168.20.246	cat-5505	Cisco CatOS	O-eng	Up	40d 23h 51m	100	Critical	Normal					0%	0%	1												
	172.16.20.7	PreSaaS-Storage.p	CentOS Linux	Super	Up	477d 20h 51r	100	Warning	Normal	6%	12%	86%		1%	0%		1											
	172.16.255.70	juniperfw	Juniper SRX Jun...	Super	Up	476d 23h 31r	100	Warning	Normal	18%	79%			0%	0%		1			2								
	192.168.0.16	sj-dev-core-srv.acc	CentOS Linux	Super	Up	39d 20h 50m	100	Warning	Normal	3%	15%	91%		0%	0%		1					1						
	172.16.0.1	SJ-QA-F-Lnx-CHK	Checkpoint Fire...	Super	Up	96d 1h 54m	100	Normal		3%	44%			0%	0%													6.1
	172.16.0.130	SJ-VPN-Pri	Cisco VPN 3K	Super	Up	477d 23h 48r	100	Normal		3%				0%	0%													
	172.16.0.138	SJ-QA-A-Ironp-C15	Cisco IronPort ...	Super	Up	135d 22h 35r	100	Normal						0%	0%													
	172.16.0.141	HQ-A-Pxy-blueCoa	Blue Coat SGOS ...	Super	Up	13d 4h 48m	100	Normal		1%				0%	0%													
	172.16.0.2	SJ-QA-A-Fdy-BigIrc	Foundry Ironware	Super	Up	478d 16m	100	Normal		1%	59%			11%	9%													
	172.16.0.254	SJ-QA-Dmz-HPSW	HP ProCurve	Super	Up	354d 4h 59m	100	Normal		51%	32%			0%	0%													
	172.16.0.4	SJ-Dev-A-Fdy-FastI	Foundry Ironware	Super	Up	406d 1h 40m	100	Normal		2%	51%			0%	0%													
	172.16.1.2	PA-500_01_accelo	Palo Alto PAN-OS	Super	Up	477d 20h 57r	100	Normal						0%	0%													
	172.16.10.100	SJ-SaaS-ASA-IPS	Cisco IPS	Super	Up	443d 23h 11r	100	Normal		3%	65%			0%	0%													
	172.16.10.13	QA-W2K3-X64	Microsoft Wind...	Super	Up	104d 1h 59m	100	Normal		2%	94%	24%	0%	0%	0%													3.2
	172.16.10.253	SJ-QA-A-JuniperOf	Nortel BayStack	Super	Up	477d 22h 36r	100	Normal						0%	0%													
	172.16.10.28	QA-EXCHG	Microsoft Wind...	Super	Up	411d 12h 3m	100	Normal		5%	92%	78%		0%	0%													
	172.16.10.6	SJ-QA-S-Sun-Spc01	Sun SunOS	Super	Up	404d 22h 17r	100	Normal						0%	0%													
	172.16.10.9	WIN-RAQBSNW8C	Microsoft Wind...	Super	Up	136d 23h 16r	100	Normal		29%	36%	49%	0%	0%	0%													10.9
	172.16.20.152	NFS	CentOS Linux	Super	Up	161d 1h 44m	100	Normal		2%	80%	31%		0%	0%													
	172.16.20.164	James-win2k8	Microsoft Wind...	Super	Up	26d 6m	100	Normal		0%	55%	25%		0%	0%													
	172.16.22.110	ESXI4.1-110	VMware ESXi Se...	Super	Up	21d 2h 58m	100	Normal		10%	70%	61%		0%	0%													0.6
	172.16.22.120	localhost.	VMware ESXi Se...	Super	Up	21d 2h 53m	100	Normal		53%	90%	98%		0%	0%													0.8
	172.16.22.130	localhost.accelops	VMware ESXi Se...	Super	Up	160d 23h 53r	100	Normal		15%	89%	47%		0%	0%													0.9

Data Analysis – Report

- Summary – Device Health



SH-QA-Cor-Srv.prospecthills.net	192.168.19.14	Cisco IOS (WS-C3524-XL)	12.0(5)wc16	05:15:59 01/28/2013	SNMP, PING	Pending	Super
xrx3635.accelops.net	192.168.20.5	Xerox Phaser	0.035.28.032	05:15:39 01/28/2013	SNMP, PING	Pending	O-eng
cisco-2524	192.168.20.245	Cisco IOS	11.0(14a)	05:20:14 01/28/2013	SNMP, PING	Pending	O-eng
cat-5505	192.168.20.246	Cisco CatOS (0)	0	05:20:19 01/28/2013	SNMP, PING	Pending	O-eng
Aruba3200	192.168.26.7	Aruba ArubaOS WLAN Controller	5.0.3.3	05:20:54 01/28/2013	SNMP, PING	Pending	O-eng
Cisco_Controller	192.168.30.9	Cisco WLAN Controller (AIR-WLC...	6.0.199.4	05:21:14 01/28/2013	SNMP, PING	Pending	O-eng

SH-QA-Cor-Srv.prospecthills.net-Details

Availability Health Current Trend (Last 1 hr)

Health: ● Up

Ping Loss % 20%

Ping Round Trip 1 ms

Events Per Second (Avg)

Incidents (Last 24 hr)

Uptime 51d 23h 42m Uptime % (30 d) 100%

Security Health

Incidents (Last 24 hr)

Performance Health

Health: ⚠ Warning

Incidents (Last 24 hr) 1

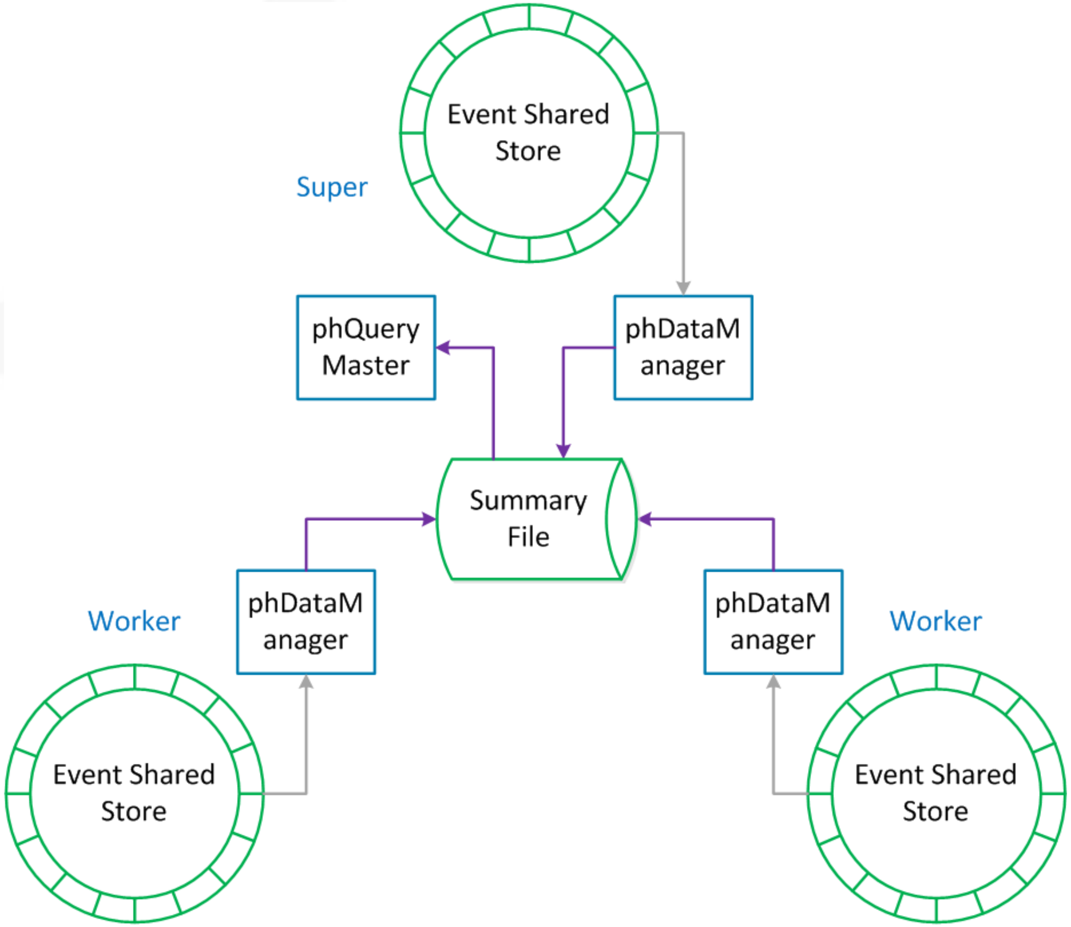
Avg CPU Util (%)	Avg Mem Util (%)	Max Disk Util (%)
Overall CPU	Physical Memory	
45	77	0
Normal	Warning	Normal

Max Interface Util

Max Interface Error Pct

Data Analysis – Report

- Summary
  - Optimize – Memory Cache



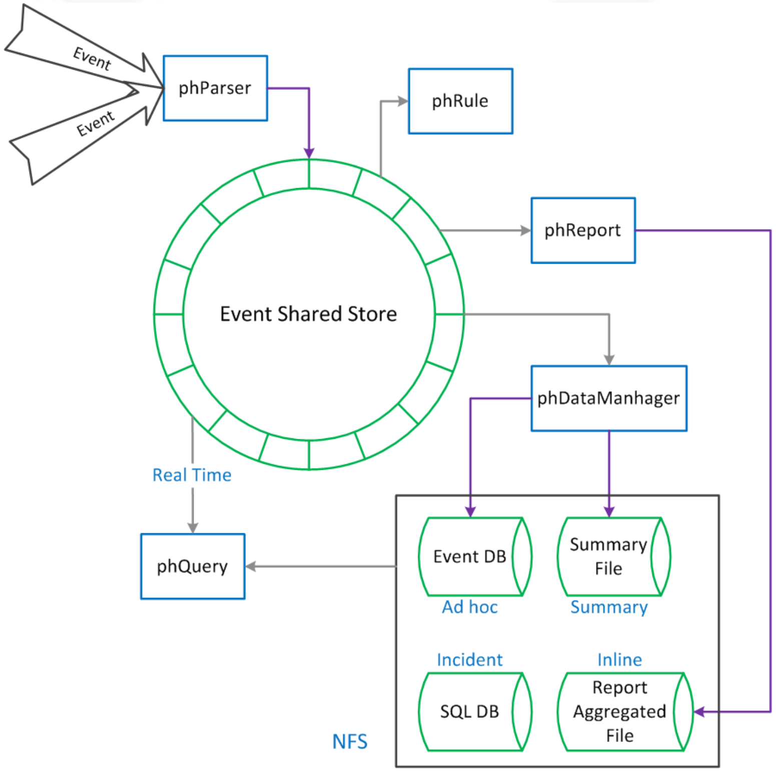
Data Analysis – Data Source

- How many of them get data from event db?

Type	Data Source
Rule	Shared Store
Ad hoc Query	Event DB
Real Time Query	Shared Store
Inline Query	Report Aggregated File
Summary	Memory Cache
Incident Query	SQL DB

Data Analysis

Type	Time Range	Define	Frequency	Response	Scope	Source	Media
Ad hoc	Random	Random	Normal	Normal	Broad	Event DB	Disk
Real Time		Random	Normal	Fast	Narrow	Shared Store	Memory
Inline	Long	Fixed	Normal	Normal	Broad	Report Aggregated File	Disk
Summary	Short	Fixed	High	Fast	Narrow	Memory Cache	Memory



Q&A