

HOW TO USE SNMPCOLLECTOR

Basic Guide for General Use
CA TECHNOLOGIES

Documentation and Requirements

- [Release Notes](#)
 - Be sure to read all of the release notes
 - This page includes software and hardware requirements, as well as recommended memory settings and performance and scalability considerations
- [Snmpcollector 3.0 Admin Console Configuration](#)
- [Snmpcollector 2.2 Admin Console Configuration](#)
- [Snmpcollector Theory of Operations](#)
- [Snmpcollector Device Support](#)
- [Snmpcollector Metrics](#)
- [Snmpcollector APIs](#)

Initial Setup

- Snmpcollector should be on its own hub with **minimal other components**.
- This image shows all of the components on my secondary snmpcollector-designated hub, called snmpcRobot. The probe can have a very high memory usage and we recommend using a separate server to run it.
- Besides robot/snmpcollector related probes, we also want **discovery_agent** deployed here, so that we can organize discovered devices for monitoring.
- Note – if integrating with NFA, the secondary hub running snmpcollector must have the same Origin as the primary hub.

snmpcRobot

Type: Regular

Address: /Domain83/snmpcHub/snmpcRobot

IP: 10.130.230.76

OS Major: Windows


OS Minor: Windows Server


OS Description: Service Pack 1 l

Installed Packages

Environment Variables

p

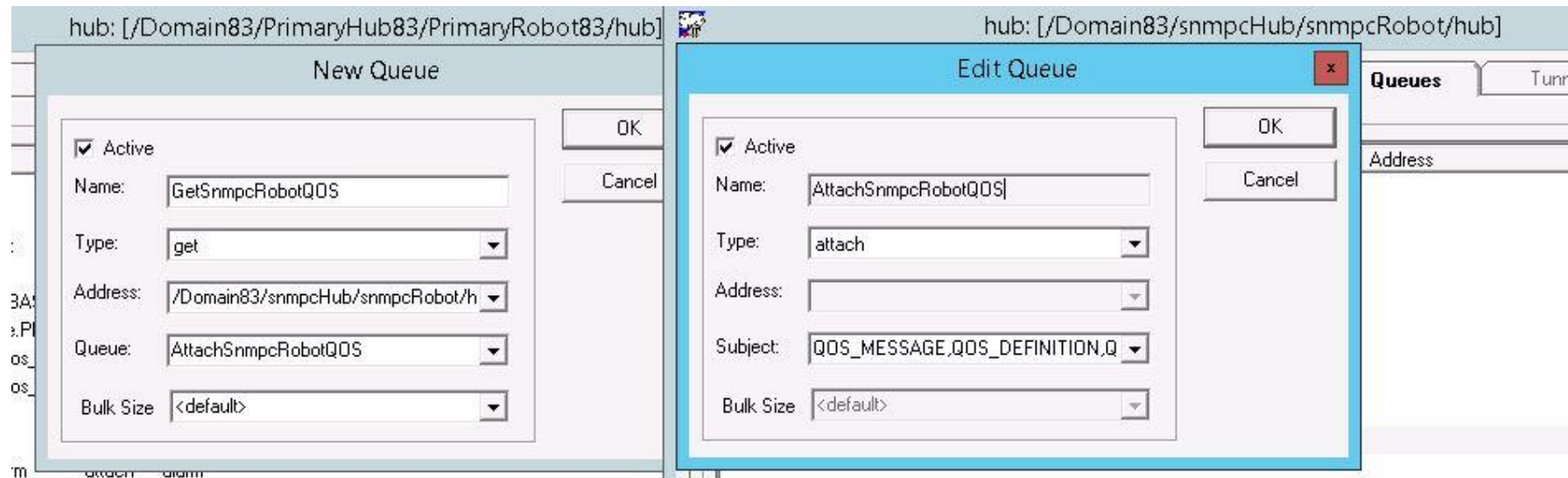




Probe ▲	Port	PID	Version	Description	Category	Last Start
alarm_enrichment	48009	3168	4.73	Alarm Enrichment Server	Infrastructure	Thu Sep 3 2015 12:56:50 PM
baseline_engine	48010	3400	2.60	Baseline Engine	SLM	Thu Sep 3 2015 12:56:53 PM
cdm	48015	1164	5.50	CPU, Disk and Memory performa...	System	Thu Sep 3 2015 12:57:00 PM
controller	48000	5000	7.80	Robot process and port controller	Infrastructure	Thu Sep 3 2015 12:56:39 PM
discovery_agent	48008	140	8.31	Discovery Agent	Service	Thu Sep 3 2015 12:56:49 PM
hdb	48007	4852	7.80	Robot database server	Infrastructure	Thu Sep 3 2015 12:56:47 PM
hub	48002	1808	7.80	Message concentrator and redistr...	Infrastructure	Thu Sep 3 2015 12:56:40 PM
nas	48014	4284	4.73	Nimsoft Alarm Server	Infrastructure	Thu Sep 3 2015 12:56:59 PM
pollagent	48012	3620	2.23	Polling Agent Probe	Network	Thu Sep 3 2015 12:56:55 PM
ppm	48011	1212	3.22	Probe Provisioning Manager	Service	Thu Sep 3 2015 12:56:54 PM
prediction_engine	48016	4632	1.31	Prediction Engine	SLM	Thu Sep 3 2015 12:57:09 PM
snmpcollector	48013	372	2.23	SNMP Collector Engine Probe	Network	Thu Sep 3 2015 12:56:56 PM
spooler	48001		7.80	Robot message spooler	Infrastructure	

Initial Setup

- A queue needs to be setup from the secondary hub to the primary hub.
- The queue will need the following subject – **'QOS_MESSAGE,QOS_DEFINITION,QOS_BASELINE'**.
- It may be called whatever you wish, just make sure that you have an attach/get (with GET queue on primary) setup
- Check out the attach/get queue I setup between my snmpcRobot-hub and the PrimaryRobot83-hub. You may use a 'post' setup.



Initial Setup

- Using the discovery_agent deployed on the snmpcollector hub, run the Discovery Wizard in USM.
- Add snmp credentials and individual IPs or IP ranges to discover the devices you want to monitor.
- [More info on Discovery Wizard](#)



Initial Setup

- Once that's done, reload USM and check to see that these devices show under the discovery_agent you used.
- You can see the four devices I discovered appear under the 'simScope' range I created when working through the Discovery Wizard.

The screenshot displays the 'viceManager' application interface. On the left, a tree view shows a hierarchy of discovery ranges: 'Groups (8)', 'No View', 'Inventory (12)', 'PrimaryHub83/PrimaryRobot83 (1)', 'snmpcHub/snmpcRobot (7)', 'simScope (4)' (highlighted in blue and enclosed in a red box), 'Automatic (4)', 'External (0)', and 'Search Results (0)'. On the right, the 'Inventory for si' panel shows a table with four discovered devices, also enclosed in a red box:

No discovery sc	
	N
	casph02-u1
	casph02-u1
	casph02-u1
	ledda02-U1

Initial Setup

- The next check is to see if the newly discovered devices have a **KEY** symbol in the last column displaying in USM.
- If the key symbol is missing, it was likely just discovered using ICMP (ping). The key indicates that the snmp credentials have been verified.
- Snmpcollector will not be able to see or configure devices without verified snmp credentials.

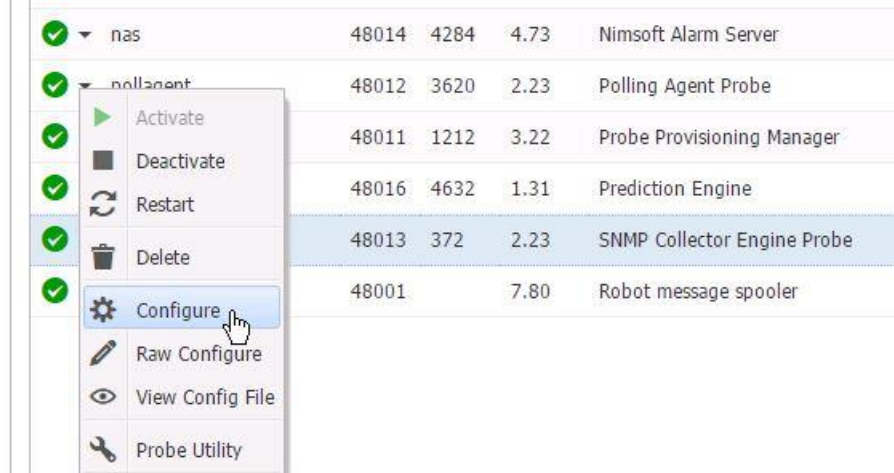


The screenshot shows the snmpcollector web interface. On the left, there is a sidebar with navigation options: "simScope (4)", "Automatic (4)", "External (0)", and "Search Results (0)". The main area displays a table of discovered devices. The table has the following columns: Name, Alias, IP Address, Type, Changed, OS Name, and Origin. The last column, Origin, contains key symbols indicating verified SNMP credentials. A red box highlights the key symbols in the last column.

Name	Alias	IP Address	Type	Changed	OS Name	Origin
casph02-u127985.ca.c...	casph02-u127985.ca.com	10.130.220.52	Virtual Server	9/1 4:05 PM	Windows	snmpcHub
casph02-u141520.ca.c...	casph02-u141520.ca.com	10.130.237.1	Virtual Server	9/1 3:44 PM	Windows	snmpcHub
casph02-u141521.ca.c...	casph02-u141521.ca.com	10.130.237.31	Virtual Server	9/1 3:39 PM	Windows	snmpcHub
ledda02-U117255.lede...	ledda02-U117255.ledeaux.	10.130.248.32	Virtual Server	9/1 3:35 PM	Windows	snmpcHub

Import discovered devices in Admin Console

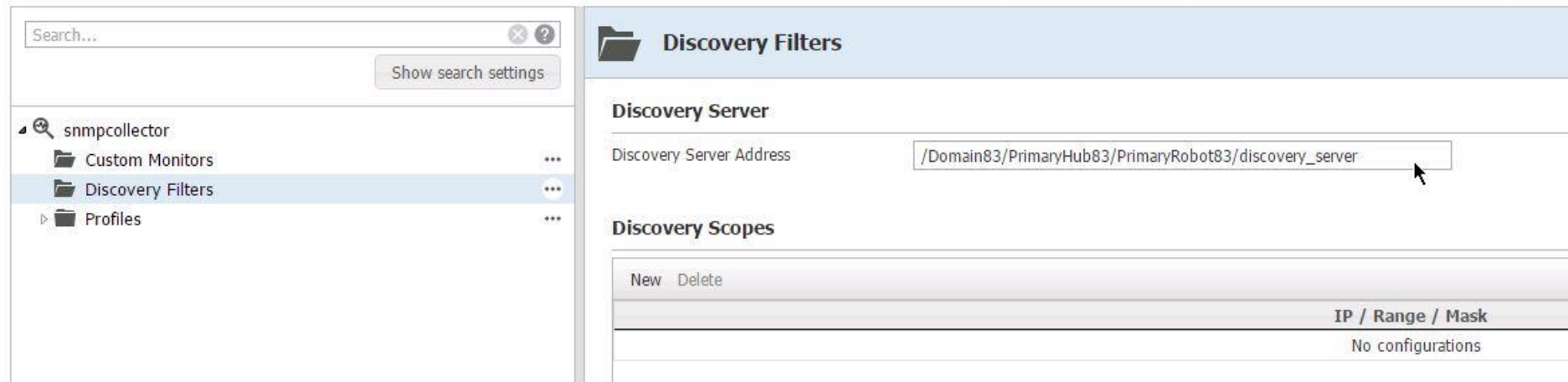
- In Admin Console, click on the snmpcollector and select 'configure'
- Next, navigate to 'Discovery Filters' and make sure that the Discovery Server address is correct



nas	48014	4284	4.73	Nimsoft Alarm Server
pollagent	48012	3620	2.23	Polling Agent Probe
	48011	1212	3.22	Probe Provisioning Manager
	48016	4632	1.31	Prediction Engine
	48013	372	2.23	SNMP Collector Engine Probe
	48001		7.80	Robot message spooler

- Activate
- Deactivate
- Restart
- Delete
- Configure
- Raw Configure
- View Config File
- Probe Utility

Probe Configuration - /Domain83/snmpcHub/snmpcRobot/snmpcollector



Search... Show search settings

snmpcollector

- Custom Monitors
- Discovery Filters
- Profiles

Discovery Filters

Discovery Server

Discovery Server Address: /Domain83/PrimaryHub83/PrimaryRobot83/discovery_server

Discovery Scopes

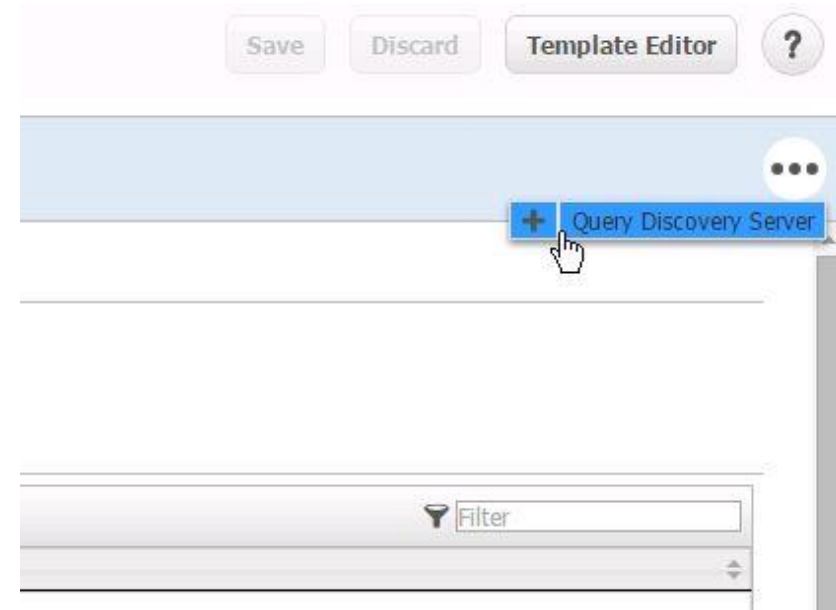
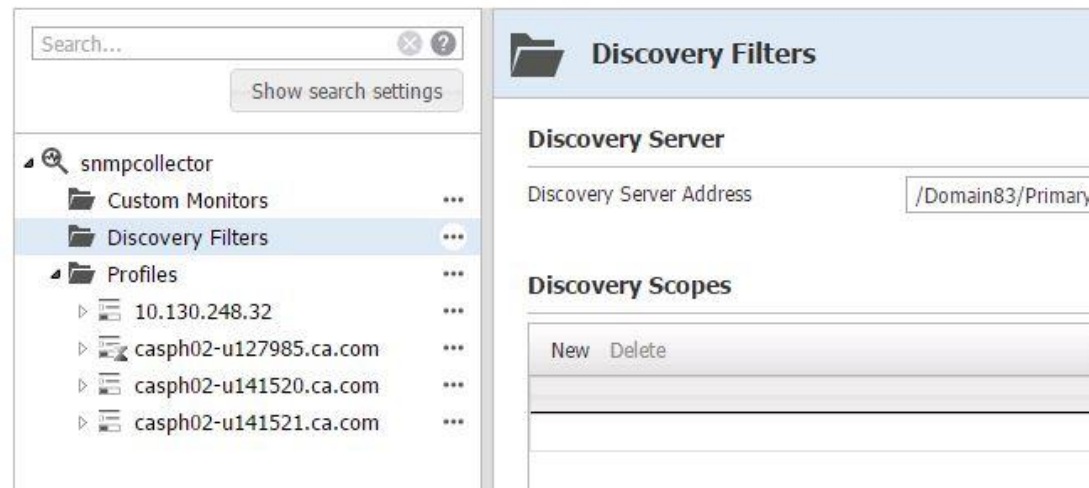
New Delete

IP / Range / Mask
No configurations

Import discovered devices in Admin Console

- Using the Options button, 'Query the Discovery Server'. This will import devices that have been discovered to snmpcollector's configuration.
- Once this is complete, those devices should show up under the Profiles folder.

Probe Configuration - /Domain83/snmpcHub/snmpcRobot/snmpcollector



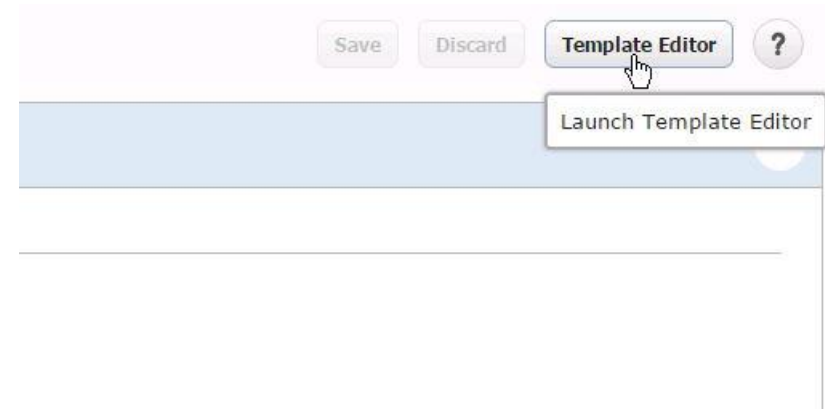
Import discovered devices in Admin Console

- Use the filters on the page to limit which devices appear – i.e. ‘Discovery Agents’.
- This is why we used a specific discovery_agent to discover these devices. Devices discovered by other agents will not be shown once the filter is applied.

Discovery Agents	
New	Delete
Discovery Agent	
Domain83/snmpcHub/snmpcRobot/discovery_agent	
Showing 1 to 1 of 1 entries	
Discovery Agent	Domain83/snmpcHub/snmpcRobot/discovery_agent ?

Create a Monitoring Template

- Click on the Template Editor button to get started configuring monitors that will apply to your discovered devices.
- Copy the default template (default cannot be edited). Rename it and add a relevant description. Set it to Active, then click Submit.



Template Editor - snmpcollector v2.23

This screenshot shows the 'Template Editor' interface for 'snmpcollector v2.23'. On the left, there is a search bar and a tree view of templates. The tree view includes 'snmpcollector probe' (with sub-items 'Default Load Balancer', 'Default Router-Switch', 'Default Wireless LAN - Aruba Networks', and 'Default Wireless LAN - Cisco WLC') and 'snmpcollector 2.23 Default Template' (with sub-item 'Device Filters'). The 'snmpcollector 2.23 Default Template' is selected, and a 'Copy' button is visible next to it. On the right, the details for the selected template are shown. The title is 'snmpcollector 2.23 Default Template' with a note 'Resource is in read only mode'. The 'Template' section contains the following fields: 'Template Name *' (value: 'snmpcollector 2.23'), 'Description *' (value: 'This is the UIM Defa'), 'Precedence *' (value: '0'), and 'Active' (checkbox, currently unchecked).

Create a Monitoring Template

- Expanding the new template's tree menu, navigate the default filter and add a **new rule** so that it only applies to the devices you intend.
- I created a filter to only include devices that contain 'casph02'. I discovered four devices, but only three with casph02 in the hostname.
- Add an appropriate name and click Save. This template should now be applied to my 'casph02' devices.

Template Editor - snmpcollector v2.23

Search...

Show search settings

snmpcollector probe

Default Load Balancer

Default Router-Switch

Default Wireless LAN - Aruba Networks

Default Wireless LAN - Cisco WLC

snmpcollector 2.23 Default Template

TestTemplate

Device Filters

Default Filter - match casph02

Application

Chassis

Circuits and Signalling

Converge Infrastructure Device

CPU

Environmental Sensors

Host

Interface

Memory

Network Device

Network QOS

Network Response Time

Protocol

Storage

System

Telecom

Tunnels

Default Filter - match casph02

Filter

Filter Name *
Default Filter - match casph02

Precedence *
0

Rules ?

New Delete

Rule
Hostname => [Condition="Contains", Value="casph02"]

Showing 1 to 1 of 1 entries

Rule

Hostname

Condition
Contains

Value
casph02

Create a Monitoring Template

- In the new template, navigate down the menu to add or modify which monitors are being used and how.
- Once completed, click Save and close the tab. In the example below, I wanted to enable publishing of alarms and data for issues related to availability.

Template Editor - snmpcollector v2.23

Search...

Show search settings

- snmpcollector probe
 - Default Load Balancer
 - Default Router-Switch
 - Default Wireless LAN - Aruba Networks
 - Default Wireless LAN - Cisco WLC
 - snmpcollector 2.23 Default Template
- TestTemplate
 - Device Filters
 - Default Filter - match casph02
 - Application
 - Chassis
 - Circuits and Signalling
 - Converge Infrastructure Device
 - CPU
 - Environmental Sensors
 - Host
 - Interface
 - Memory
 - Network Device
 - Network QoS
 - Network Response Time
 - Protocol
 - Storage
 - System
 - Availability
 - Availability Filter Rules
 - Default Availability Fiter

Default Availability Fiter

Monitor	Include in Template	Data	Alarms	QoS Name
Availability	On	On	On	QOS_AVAILABILITY_AV

Showing 1 to 1 of 1 entries

Availability

Include in Template

☒

QoS Name

QOS_AVAILABILITY_AVAILABILITY

Description

Metric Type

Availability

Units

pct

Publish Data

☒

Publish Alarms

☒

Compute Baseline

☐ ?

Dynamic Alarm

☐ ?

Algorithm *

Percent

Create a Monitoring Template

- Navigate back to the snmpcollector's main configuration tab and reload the page.
- Using a device that the template applies to, navigate down to the metric and see that it has updated.
- The options here are greyed out from this view – the template editor modifies these values.
- Note that the available metrics are organized differently under the devices in the main configuration page than in the template editor – i.e. 'Availability' is its own entry in the probe configuration page but is in the 'System' folder on the template editor.

Probe Configuration - /Domain83/snmpcHub/snmpcRobot/snmpcollector

The screenshot displays the 'Probe Configuration' interface for the 'snmpcollector' device. The left sidebar shows a tree view of configuration categories: Custom Monitors, Discovery Filters, Profiles, and a list of devices. Under the 'Availability' category, various metrics are listed, including CPU, Disk, Disk Partitions, Generic System, Interface, IPv4 Stats, Physical Memory, Reachability, Server Statistics, Swap, TCP Stats, Virtual Memory, and Virtual Session. The 'Availability' metric is selected, and its configuration is shown on the right. The configuration includes fields for QoS Name, Description, Metric Type, Units, Publish Data, Publish Alarms, Compute Baseline, Dynamic Alarm, Algorithm, and Critical Level. The 'Publish Data' and 'Publish Alarms' checkboxes are highlighted with a red box.

Search...

Show search settings

snmpcollector

- Custom Monitors
- Discovery Filters
- Profiles
 - 10.130.248.32
 - casph02-u127985.ca.com
 - casph02-u141520.ca.com
 - casph02-u141521.ca.com
 - 10.130.237.31
 - ATM
 - Availability
 - CPU
 - Disk
 - Disk Partitions
 - Generic System
 - Interface
 - IPv4 Stats
 - Physical Memory
 - Reachability
 - Server Statistics
 - Swap
 - TCP Stats
 - Virtual Memory
 - Virtual Session

Availability

Showing 1 to 1 of 1 entries

Availability

This configuration is managed by Templates.
Template: [TestTemplate](#)
Template Filter: [Default Availability Filter](#)

QoS Name: QOS_AVAILABILITY_AVAILABILITY

Description:

Metric Type: Availability

Units: pct

Publish Data: ☒

Publish Alarms: ☒

Compute Baseline: ☐ ?

Dynamic Alarm: ☐ ?

Algorithm *: Percent

Critical Level 5: >

Create a Monitoring Template

- Availability is now being alarmed on for each of my devices whose hostname includes 'casph02.'
- Since the 'publish data' box was also checked, we can see QOS data in USM.

