Connect Guide

To connect to 10.248.169.31:

$ ssh support@10.248.169.31

support@10.248.169.31's password: Tripwire

To connect to RAV:

-bash-4.2$ admincli

To check RAV version:

glob-rav-01> system status version read

To check for RAV updates:

glob-rav-01> system upgrades read

To upgrade current version:

glob-rav-01> system upgrade upgrade <version> (or latest)

To check for RAV upgrade porgress:

glob-rav-01> system status upgrade progress read

To check RAV status:

glob-rav-01> rav configuration status

To restart data partition:

glob-rav-01> system data partition reset CONFIRM

To revert last upgrade:

glob-rav-01> system upgrade revert

To stop iptables:

-bash-4.2$ sudo systemctl stop iptables

To check kafka topics:

-bash-4.2$ /usr/lib/rav/queues/kafka-offsets

To check journal log:

sudo journalctl -u -n 1000

-bash-4.2$ sudo journalctl -u <service> -n 1000

Options:

-b (since last boot)

--output=verbose (more detail)

Where service can be:

\*rav-scm-message-enrichment-transformer.service

\*rav-scm-postgresql-transformer.service

\*ironwood-kafka

-any other service?

// Update rpm settings

-> Viejo: /etc/upgrade\_rpm

-Change: RAV -> connect

-> /etc/ncircle-release

-Cambiar lo que esta por 3.X.X.b<master|testing>-r20170731173208.326ee01.b1

-> /etc/yum/vars/update\_url

-https://<usuario>:<pass>@artifacts-internal.scm.tripwire.com:8443/artifactory/distros-scm-local/ironwood-upgrades/master

-https://<usuario>:<pass>@artifacts-internal.scm.tripwire.com:8443/artifactory/distros-scm-local/ironwood-upgrades/testing

<pass> -> password encriptado por artifactory

-> /etc/yum/vars/gpgcheck

-Change: 1 -> 0

// Outdated

To install head plugin:

-bash-4.2$ sudo /usr/share/elasticsearch/bin/plugin --install head -u file:///data/support/elasticsearch-head-master.zip

To delete temporary documents:

-bash-4.2$ python delete\_indexes.py

To run reconciliation job:

-bash-4.2$ python -m rav\_kibana.reconciliation

Linux

-----

// Check disk space (verify /data partition)

> df

Connect UI configuration

---------------------

1) Go to https://10.248.169.31/index.html

1) Login with: passphrase

2) Change system password to: Password1@

3) Go back, and log with user: admin, and password: Tripwire

Queries Útiles

---------------------

**select \* from config.data\_source**

-> To get SourceID

**select \* from config.data\_source\_watermark**

-> Get DA watermark, and what dates DA is processing

**select \* from scm.message\_landing order by id;**

**select count(\*) from scm.message\_landing ;**

-> Get messages sent by DA

**select message -> 'Events' AS Events**

**from scm.message\_landing**

**where message @> '{"SourceIdentifier":"a020232:160eafd4914:-7fff"}'**

**and message @> '{"MessageType":"Events"}'**

**order by id;**

-> Get Events Json from inside message

**select message -> 'Events' ->> 'ElementChanges' AS Events**

**from scm.message\_landing**

**where message @> '{"SourceIdentifier":"a020232:160eafd4914:-7fff"}'**

**and message @> '{"MessageType":"Events"}'**

**and message -> 'Events' ->> 'ElementChanges' IS NOT NULL**

**order by id;**

-> Get ElementChanges Json from inside Events

-> Also filters messages that have attribute ElementChanges inside attribute Events

**select \* from scm.message\_landing**

**where is\_config\_message = false**

**and message @> '{"MessageType":"UnknownTestResults"}'**

**order by created\_timestamp desc;**

**select message -> 'Events' AS Events**

**from scm.message\_landing**

**where message @> '{"SourceIdentifier":"a020232:160eafd4914:-7fff"}'**

**and message @> '{"MessageType":"Events"}'**

**and message -> 'Events' -> 'ElementChanges' -> 0 ->> 'Content' IS NOT NULL**

**order by id;**

-> Gets Events with content

**select \* from scm.message\_landing where message ? ‘PartNo’**

-> Gets messages with attribute PartNo

**select \* from scm.message\_landing where message ?| array[‘PartNo’, ‘TotalParts’]**

-> Gets messages with either attribute PartNo or TotalParts

**select \* from scm.message\_landing where message ?& array[‘PartNo’, ‘TotalParts’]**

-> Gets messages with attributes PartNo and TotalParts

**select \* from scm.message\_landing where message ->> ‘PartNo’ > 1**

-> Gets messages with attribute PartNo value is greater than 1; or in case of arrays, has more than 1 element

**select \* from scm.message\_landing where message #> ‘{Statistics, AssetID}’ = '"-abc"';**

-> Gets messages where element Statistics has child object AssetID equal to “abc”

--

**delete from config.data\_source\_watermark;**

**delete from scm.message\_landing;**