CloudVision Custom Events

Using the EOS Syslog function, and CVP Custom Events, CVP users can trigger custom events of any severity. Since EOS streams its state to CVP by way of the TerminAttr agent, this includes all of the system log messages.

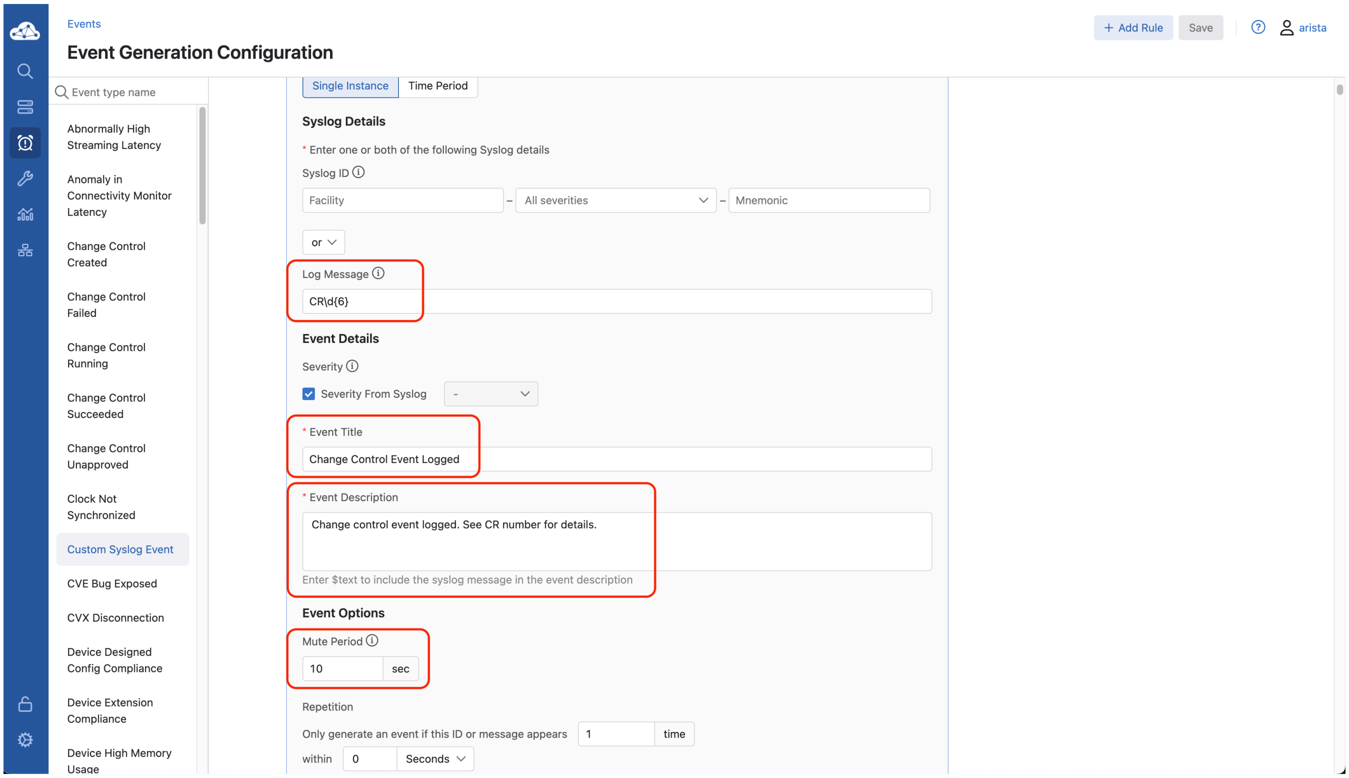
A custom event based on a specific syslog entry can be created with little more than a regular expression (aka regex) to detect and match an occurring log message. Or this log could be triggered by an EOS Event-Handler as part of the action. In this lab we will use the EOS CLI to send log messages that CVP will detect and create an Event accordingly.

Creating a Custom Event

1. Start by selecting **Events** from the navigation menu. Then select **Event Generation**.
2. After selecting **Event Generation** choose and select **Custom Syslog Event** from the event types.
3. Select **Add Rule**.
4. Under **Syslog Details** set the fields to the values listed:
5. In the **Log Message** field add the following Regular Expression:

   ```
   CR\d{6}
   ```

6. The **Event Title** field should be set to **Change Control Event Logged**.
7. The **Description** field should be set to **Change Control Event Logged. See CR number for details**.
8. The **Mute Period** field should be **10 sec**.



Syslog Details

* Enter one or both of the following Syslog details

Syslog ID: Facility – All severities – Mnemonic

or

Log Message: CR\d{6}

Event Details

Severity: ☑ Severity From Syslog -

* Event Title: Change Control Event Logged

* Event Description: Change control event logged. See CR number for details.

Enter $text to include the syslog message in the event description

Event Options

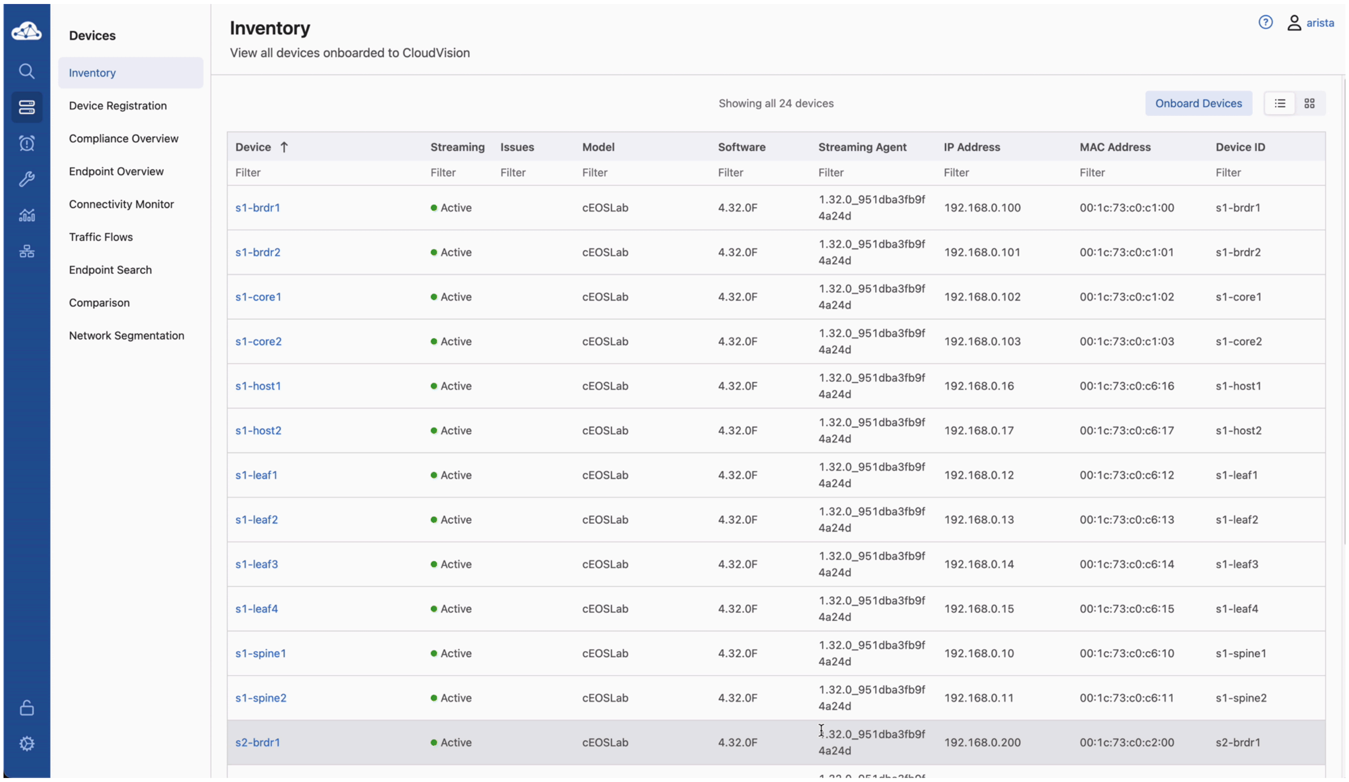
Mute Period: 10 sec

Repetition

Only generate an event if this ID or message appears 1 time within 0 Seconds

(_images/cvp_custom_event_1.png)

9. Select **Save Changes** to finish creating the Custom Syslog Event.



Inventory

View all devices onboarded to CloudVision

Showing all 24 devices

Device ↑	Streaming	Issues	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
s1-brdr1	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.100	00:1c:73:c0:c1:00	s1-brdr1
s1-brdr2	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.101	00:1c:73:c0:c1:01	s1-brdr2
s1-core1	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.102	00:1c:73:c0:c1:02	s1-core1
s1-core2	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.103	00:1c:73:c0:c1:03	s1-core2
s1-host1	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.16	00:1c:73:c0:c6:16	s1-host1
s1-host2	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.17	00:1c:73:c0:c6:17	s1-host2
s1-leaf1	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.12	00:1c:73:c0:c6:12	s1-leaf1
s1-leaf2	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.13	00:1c:73:c0:c6:13	s1-leaf2
s1-leaf3	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.14	00:1c:73:c0:c6:14	s1-leaf3
s1-leaf4	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.15	00:1c:73:c0:c6:15	s1-leaf4
s1-spine1	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.10	00:1c:73:c0:c6:10	s1-spine1
s1-spine2	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.11	00:1c:73:c0:c6:11	s1-spine2
s2-brdr1	● Active		cEOSLab	4.32.0F	1.32.0_951dba3fb9f4a24d	192.168.0.200	00:1c:73:c0:c2:00	s2-brdr1

(_images/cvp_custom_event_2.gif)

Tip

This Regular expression will match when the log message contains a string beginning with "CR" followed by exactly 6 numeric digits. In this example CR means **Change Record**. This will give the NOC the change record to review when an event is logged.

Generating the Syslog Message

1. Log in to the CLI of leaf switch **s1-leaf1**.
2. Type the following EOS CLI command:

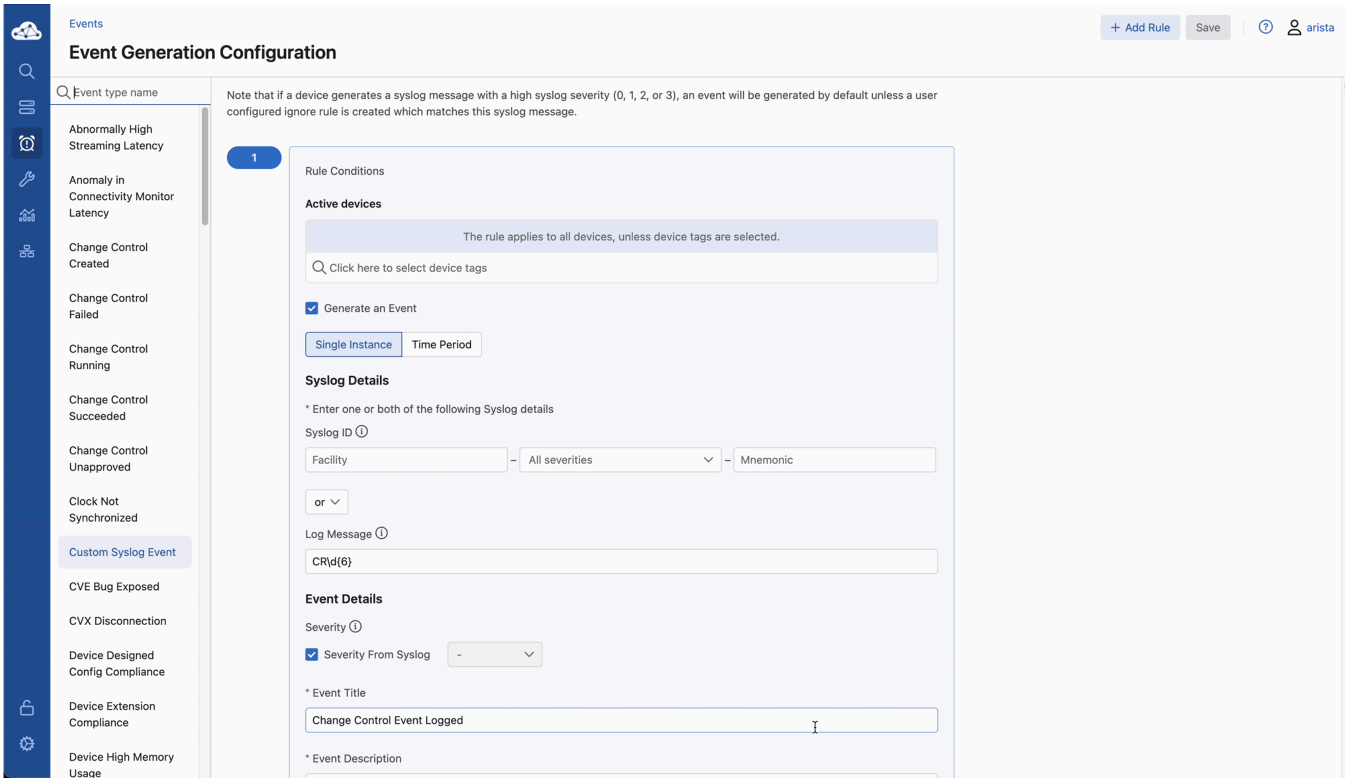
```
s1-leaf1# send log level alerts message CR123456 starting now!
```

```
Last login: Wed Jun  5 15:41:52 2024 from 192.168.0.1
s1-leaf1#
s1-leaf1#
```

(_images/cvp_custom_event_3.gif)

Reviewing the Events in Cloudvision

1. Select **Events** from the navigation menu.
2. You should see an event similar to the one below:



Event Generation Configuration

Note that if a device generates a syslog message with a high syslog severity (0, 1, 2, or 3), an event will be generated by default unless a user configured ignore rule is created which matches this syslog message.

Rule Conditions

Active devices

The rule applies to all devices, unless device tags are selected.

Click here to select device tags

☑ Generate an Event

Single Instance | Time Period

Syslog Details

* Enter one or both of the following Syslog details

Syslog ID

Facility – All severities – Mnemonic

or

Log Message

CR\d{6}

Event Details

Severity

☑ Severity From Syslog -

* Event Title

Change Control Event Logged

* Event Description

(_images/cvp_custom_event_4.gif)

Tip

- Experiment by sending messages with different severity levels, and modify the **CR123456** example using only 5 digits, or 7 digits. Does the event still trigger when using 5 or 7 digits?
- Experiment with different regular expressions, perhaps try to build a match for other logs happening on **s1-leaf1**

LAB COMPLETE

Created using Sphinx (http://sphinx-doc.org/) 6.1.3.

Back to top