Logging for security groups

« (config-lbaas.html) » (config-macvtap.html) (https://bugs.launchpad.net/neutron/+filebug?field.title=Logging%20for%20security%20groups%20in%20Neutron&field.comment=%0A%0A%0AThis bug tracker is for errors with the documentation, use the following as a template and remove or add fields as you see fit. Convert [ ] into [x] to check boxes:%0A%0A- [ ] This doc is inaccurate in this way: _____%0A- [ ] This is a doc addition request.%0A- [ ] I have a fix to the document that I can paste below including example: input and output. %0A%0AIf you have a troubleshooting or support issue, use the following resources:%0A%0A - Ask OpenStack: http://ask.openstack.org%0A - The mailing list: http://lists.openstack.org%0A - IRC: 'openstack' channel on Freenode%0A%0A---------%0ARelease:%2012.0.1.dev11%20on%202018-03-07%2021:05%0ASHA:%2043df2709acbdce86686a40b75fd34e96880427d0%0ASource:%20https://git.openstack.org/cgit/openstack/neutron/tree/doc/source/admin/config-logging.rst%0AURL: https://docs.openstack.org/neutron/queens/admin/config-logging.html&field.tags=doc)

UPDATED: 2018-03-07 21:05

Logging is designed as a service plug-in that captures events for relevant resources (for example, security groups or firewalls) when they occur.

Supported logging resource types¶

As of the Queens release, the **security_group** resource type is supported.

Configuration¶

To enable the service, follow the steps below.

1. On Neutron server node:

   a. Add the Logging service to the **service_plugins** setting in **/etc/neutron/neutron.conf**. For example:

   ```
   service_plugins = router,metering,log
   ```

   b. Add the Logging extension to the **extensions** setting in **/etc/neutron/plugins/ml2/ml2_conf.ini**. For example:

   ```
   [agent]
   extensions = log
   ```

2. On compute/network nodes:

   a. In **/etc/neutron/plugins/ml2/openvswitch_agent.ini**, add **log** to the **extensions** setting in the **[agent]** section. For example:

   ```
   [agent]
   extensions = log
   ```

   b. In **/etc/neutron/plugins/ml2/openvswitch_agent.ini**, add configuration options for logging feature in the **[network_log]** section. For example:

   ```
   [network_log]
   rate_limit = 100
   burst_limit = 25
   #local_output_log_base = <None>
   ```

   In which, **rate_limit** is used to configure the maximum number of packets to be logged per second (packets per second). When a high rate triggers **rate_limit**, logging queues packets to be logged. **burst_limit** is used to configure the maximum of queued packets. And logged data can be stored anywhere by using **local_output_log_base**.

> **Note**
>
> - Logging currently works with **openvswitch** firewall driver only.
> - It requires at least 100 for **rate_limit** and at least 25 for **burst_limit**.
> - If **rate_limit** is unset, logging will log unlimited.
> - If we don't specify **local_output_log_base**, logged data will be stored in system journal like **/var/log/syslog**.

Trusted projects policy.json configuration¶

With the default **/etc/neutron/policy.json**, administrators must set up resource logging on behalf of the cloud projects.

If projects are trusted to administer their own resource logging in your cloud, neutron's file **policy.json** can be modified to allow this.

Modify **/etc/neutron/policy.json** policy entries as follows:

```
"get_loggable_resources": "rule:regular_user",
"create_log": "rule:regular_user",
"update_log": "rule:regular_user",
"delete_log": "rule:regular_user",
"get_logs": "rule:regular_user",
"get_log": "rule:regular_user",
```

Operator workflow¶

1. Confirm logging resources are supported:

```
$ openstack network loggable resources list
+-----------------+
| Supported types |
+-----------------+
| security_group  |
+-----------------+
```

2. Create a logging resource with an appropriate resource type:

```
$ openstack network log create --resource-type security_group \
  --description "Collecting all security events in project demo" \
  --enable --event ALL Log_Created
+-----------------+-------------------------------------------------+
| Field           | Value                                           |
+-----------------+-------------------------------------------------+
| Description     | Collecting all security events in project demo |
| Enabled         | True                                            |
| Event           | ALL                                             |
| ID              | 8085c3e6-0fa2-4954-b5ce-ff6207931b6d            |
| Name            | Log_Created                                     |
| Project         | 02568bd62b414221956f15dbe9527d16                |
| Resource        | None                                            |
| Target          | None                                            |
| Type            | security_group                                  |
| created_at      | 2017-07-05T02:56:43Z                            |
| revision_number | 0                                               |
| tenant_id       | 02568bd62b414221956f15dbe9527d16                |
| updated_at      | 2017-07-05T02:56:43Z                            |
+-----------------+-------------------------------------------------+
```

> **Note**
>
> The **Enabled** field is set to **True** by default. If enabled, log information is written to the destination if configured in **local_output_log_base** or system journal like **/var/log/syslog**.

Enable/Disable log¶

We can enable or disable logging objects at runtime. It means that it will apply to all attached ports with the logging object immediately.

For example:

```
$ openstack network log set --disable Log_Created
$ openstack network log show Log_Created
 +-----------------+-------------------------------------------------+
 | Field           | Value                                           |
 +-----------------+-------------------------------------------------+
 | Description     | Collecting all security events in project demo |
 | Enabled         | False                                           |
 | Event           | ALL                                             |
 | ID              | 8085c3e6-0fa2-4954-b5ce-ff6207931b6d            |
 | Name            | Log_Created                                     |
 | Project         | 02568bd62b414221956f15dbe9527d16                |
 | Resource        | None                                            |
 | Target          | None                                            |
 | Type            | security_group                                  |
 | created_at      | 2017-07-05T02:56:43Z                            |
 | revision_number | 1                                               |
 | tenant_id       | 02568bd62b414221956f15dbe9527d16                |
 | updated_at      | 2017-07-05T03:12:01Z                            |
 +-----------------+-------------------------------------------------+
```

Events collected description¶

Logging will collect **ACCEPT** or **DROP** or both events related to security group, with the following general characteristics:

- Log every **DROP** event: Every **DROP** security event will be generated when an incoming or outgoing session is dropped, that is the new session is not allowed for the security group and because of that blocked.
- Log an **ACCEPT** event: An **ACCEPT** security event will be generated for each **NEW** incoming or outgoing session that is allowed by the ports security group. More details for the events follow below:
  - North/South **ACCEPT**: For a North/South session there would be a single **ACCEPT** event irrespective of direction.
  - East/West **ACCEPT/ACCEPT**: In an intra-project East/West session where the security group on the originating port allows the session and the security group on the destination port allows the session, i.e. the traffic is allowed, there would be two **ACCEPT** security events generated, one from the perspective of the originating port and one from the perspective of the destination port.
  - East/West **ACCEPT/DROP**: In an intra-project East/West session initiation where the security group on the originating port allows the session and the security group on the destination port does not allow the session there would be **ACCEPT** security events generated from the perspective of the originating port and **DROP** security events generated from the perspective of the destination port.

General data requirements: The security event should include:

- A status of the flow **ACCEPT/DROP**.
- An indication of the originator of the flow, e.g which project or log resource generated the event.
- A timestamp of the flow.
- An identifier of the associated instance interface (neutron port id).
- An identifier of the matching security group rule.
- A layer 3 and 4 information (address, port, protocol, etc).

> **Note**
>
> No other extraneous events are generated within the security event logs, e.g. no debugging data, etc.

- Security event record format:
  - Logged data of an **ACCEPT** event would look like:

```
May 5 09:05:07 action=ACCEPT project_id=736672c700cd43e1bd321aeaf940365c
log_resource_ids=['4522efdf-8d44-4e19-b237-64cafc49469b', '42332d89-df42-4588-a2bb-3ce50829ac51']
vm_port=e0259ade-86de-482e-a717-f58258f7173f
ethernet(dst='fa:16:3e:ec:36:32',ethertype=2048,src='fa:16:3e:50:aa:b5'),
ipv4(csum=62071,dst='10.0.0.4',flags=2,header_length=5,identification=36638,offset=0,
option=None,proto=6,src='172.24.4.10',tos=0,total_length=60,ttl=63,version=4),
tcp(ack=0,bits=2,csum=15097,dst_port=80,offset=10,option=[TCPOptionMaximumSegmentSize(kind=2,length=4,max_seg_size=1460),
TCPOptionSACKPermitted(kind=4,length=2), TCPOptionTimestamps(kind=8,length=10,ts_ecr=0,ts_val=196418896),
TCPOptionNoOperation(kind=1,length=1), TCPOptionWindowScale(kind=3,length=3,shift_cnt=3)],
seq=3284890090,src_port=47825,urgent=0,window_size=14600)
```

  - Logged data of a **DROP** event:

```
May 5 09:05:07 action=DROP project_id=736672c700cd43e1bd321aeaf940365c
log_resource_ids=['4522efdf-8d44-4e19-b237-64cafc49469b'] vm_port=e0259ade-86de-482e-a717-f58258f7173f
ethernet(dst='fa:16:3e:ec:36:32',ethertype=2048,src='fa:16:3e:50:aa:b5'),
ipv4(csum=62071,dst='10.0.0.4',flags=2,header_length=5,identification=36638,offset=0,
option=None,proto=6,src='172.24.4.10',tos=0,total_length=60,ttl=63,version=4),
tcp(ack=0,bits=2,csum=15097,dst_port=80,offset=10,option=[TCPOptionMaximumSegmentSize(kind=2,length=4,max_seg_size=1460),
TCPOptionSACKPermitted(kind=4,length=2), TCPOptionTimestamps(kind=8,length=10,ts_ecr=0,ts_val=196418896),
TCPOptionNoOperation(kind=1,length=1), TCPOptionWindowScale(kind=3,length=3,shift_cnt=3)],
seq=3284890090,src_port=47825,urgent=0,window_size=14600)
```

« (config-lbaas.html) » (config-macvtap.html) (https://bugs.launchpad.net/neutron/+filebug?field.title=Logging%20for%20security%20groups%20in%20Neutron&field.comment=%0A%0A%0AThis bug tracker is for errors with the documentation, use the following as a template and remove or add fields as you see fit. Convert [ ] into [x] to check boxes:%0A%0A- [ ] This doc is inaccurate in this way: _____%0A- [ ] This is a doc addition request.%0A- [ ] I have a fix to the document that I can paste below including example: input and output. %0A%0AIf you have a troubleshooting or support issue, use the following resources:%0A%0A - Ask OpenStack: http://ask.openstack.org%0A - The mailing list: http://lists.openstack.org%0A - IRC: 'openstack' channel on Freenode%0A%0A----------%0ARelease:%2012.0.1.dev11%20on%202018-03-07%2021:05%0ASHA:%2043df2709acbdce86686a40b75fd34e96880427d0%0ASource:%20https://git.openstack.org/cgit/openstack/neutron/tree/doc/source/admin/config-logging.rst%0AURL: https://docs.openstack.org/neutron/queens/admin/config-logging.html&field.tags=doc)

UPDATED: 2018-03-07 21:05

FOUND AN ERROR? REPORT A BUG (HTTPS://BUGS.LAUNCHPAD.NET/NEUTRON/+FILEBUG?FIELD.TITLE=LOGGING%20FOR%20SECURITY%20GROUPS%20IN%20NEUTRON&FIELD.COMMENT=%0A%0A%0ATHIS BUG TRACKER IS FOR ERRORS WITH THE DOCUMENTATION, USE THE FOLLOWING AS A TEMPLATE AND REMOVE OR ADD FIELDS AS YOU SEE FIT. CONVERT [ ] INTO [X] TO CHECK BOXES:%0A%0A- [ ] THIS DOC IS INACCURATE IN THIS WAY: _____%0A- [ ] THIS IS A DOC ADDITION REQUEST.%0A- [ ] I HAVE A FIX TO THE DOCUMENT THAT I CAN PASTE BELOW INCLUDING EXAMPLE: INPUT AND OUTPUT. %0A%0AIF YOU HAVE A TROUBLESHOOTING OR SUPPORT ISSUE, USE THE FOLLOWING RESOURCES:%0A%0A - ASK OPENSTACK: HTTP://ASK.OPENSTACK.ORG%0A - THE MAILING LIST: HTTP://LISTS.OPENSTACK.ORG%0A - IRC: 'OPENSTACK' CHANNEL ON FREENODE%0A%0A----------%0ARELEASE:%2012.0.1.DEV11%20ON%202018-03-07%2021:05%0ASHA:%2043DF2709ACBDCE86686A40B75FD34E96880427D0%0ASOURCE:%20HTTPS://GIT.OPENSTACK.ORG/CGIT/OPENSTACK/NEUTRON/TREE/DOC/SOURCE/ADMIN/CONFIG-LOGGING.RST%0AURL: HTTPS://DOCS.OPENSTACK.ORG/NEUTRON/QUEENS/ADMIN/CONFIG-LOGGING.HTML&FIELD.TAGS=DOC)

QUESTIONS? (HTTP://ASK.OPENSTACK.ORG)

Page Contents