

记录安全组

[« \(config-lbaas.html\)](#)
[» \(config-macvtap.html\)](#)

更新日期：2018-03-07 21:05

日志记录被设计为一个服务插件，用于在相关资源（例如，安全组或防火墙）发生时捕获事件。

支持的日志资源类型

在Queens发行版中，**security_group**支持资源类型。

配置

要启用该服务，请按照以下步骤操作。

1. 在Neutron服务器节点上：

a. 将记录服务添加到中的**service_plugins**设置 **/etc/neutron/neutron.conf**。例如：

```
service_plugins = 路由器, 计量, 日志
```

b. 将记录扩展添加到中的**extensions**设置 **/etc/neutron/plugins/ml2/ml2_conf.ini**。例如：

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

2. 在计算/网络节点上：

a. 在**/etc/neutron/plugins/ml2/openvswitch_agent.ini**，添加**log**到**extensions**该**[agent]**部分中的设置。例如：

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

b. 在**/etc/neutron/plugins/ml2/openvswitch_agent.ini**该**[network_log]**部分添加日志记录功能的配置选项。例如：

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

其中，**rate_limit**用于配置每秒记录的最大数据包数（每秒数据包数）。当高速率触发时 **rate_limit**，日志队列记录数据包。**burst_limit**用于配置排队数据包的最大数量。记录的数据可以通过使用存储在任意地方**local_output_log_base**。

注意

- 日志记录目前**openvswitch**仅适用于防火墙驱动程序。
- 它至少需要100 **rate_limit**，至少需要25 **burst_limit**。
- 如果**rate_limit**未设置，日志记录将无限制地登录。
- 如果我们没有指定**local_output_log_base**，记录的数据将被存储在系统日志中**/var/log/syslog**。

可信项目policy.json配置

在默认情况下**/etc/neutron/policy.json**，管理员必须代表云项目设置资源日志记录。

如果项目被信任在您的云中管理他们自己的资源日志记录，**policy.json**可以修改neutron的文件以允许这样做。

修改**/etc/neutron/policy.json**策略条目如下：

```
“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”,
```

操作员的工作流程

1. 确认日志资源是否受支持：

```
$ openstack网络可登录资源列表
+ -----+
| 支持的类型 |
+ -----+
| security_group |
+ -----+
```

2. 使用适当的资源类型创建一个日志记录资源：

```
$ openstack网络日志创建 - 资源类型security_group \
--description “收集项目演示中的所有安全事件” \
--enable --event ALL Log_Created
+ -----+
| 字段 | 值 |
+ -----+
| 说明 | 收集项目演示 | 中的所有安全事件
| 已启用 | True |
| 活动 | ALL |
| ID | 8085c3e6-0fa2-4954-b5ce-ff6207931b6d |
| 名称 | Log_Created |
| 项目 | 02568bd62b414221956f15dbe9527d16 |
| 资源 | 无 |
| 目标 | 无 |
| 类型 | security_group |
| created_at | 2017-07-05T02: 56: 43Z |
| revision_number | 0 |
| tenant_id | 02568bd62b414221956f15dbe9527d16 |
| updated_at | 2017-07-05T02: 56: 43Z |
+ -----+
+ -----+
+ -----+
```

注意

该Enabled字段True默认设置为。如果启用，则将日志信息写入目标（如果配置为 local_output_log_base或系统日志类似）/var/log/syslog。

启用/禁用日志

我们可以在运行时启用或禁用日志记录对象。这意味着它将立即应用于所有与日志记录对象相连的端口。

例如：

```
$ openstack网络日志集 --disable Log_Created
$ openstack网络日志显示Log_Created
+ -----+
| 字段 | 值 |
+ -----+
| 说明 | 收集项目演示 | 中的所有安全事件
| 已启用 | False |
| 活动 | ALL |
| ID | 8085c3e6-0fa2-4954-b5ce-ff6207931b6d |
| 名称 | Log_Created |
| 项目 | 02568bd62b414221956f15dbe9527d16 |
| 资源 | 无 |
| 目标 | 无 |
| 类型 | security_group |
| created_at | 2017-07-05T02: 56: 43Z |
| revision_number | 1 |
| tenant_id | 02568bd62b414221956f15dbe9527d16 |
| updated_at | 2017-07-05T03: 12: 01Z |
+ -----+
+ -----+
+ -----+
```

事件收集描述

日志记录将收集ACCEPT或DROP两个与安全组相关的事件，具有以下一般特征：

- 记录每个DROP事件：DROP丢弃传入或传出会话时会生成每个安全事件，即安全组不允许新会话并因此被阻止。
- 记录ACCEPT事件：ACCEPT将为端口安全组允许的每个新传入或传出会话生成安全事件。以下是该活动的更多详情：

- 南北方向**ACCEPT**：对于北/南方会议，**ACCEPT** 不管方向如何，都会有单个事件。
- East / West **ACCEPT** / **ACCEPT**：在项目内部的East / West会话中，始发端口上的安全组允许会话和目标端口上的安全组允许会话（即允许通信），则会**ACCEPT**生成两个安全事件一个是始发端口的角度来看，另一个是从目的端口的角度来看。
- East / West **ACCEPT** / **DROP**：在项目内东/西会话启动中，始发端口上的安全组允许会话和目标端口上的安全组不允许会话，则会从**ACCEPT**安全事件的角度生成安全事件源端口和**DROP**从目标端口角度生成的安全事件。

一般数据要求：安全事件应包括：

- 流量状态**ACCEPT** / **DROP**。
- 流的发起者的指示，例如哪个项目或日志资源产生事件。
- 流的时间戳。
- 相关实例接口的标识符（neutron端口标识）。
- 匹配的安全组规则的标识符。
- 第3层和第4层信息（地址，端口，协议等）。

注意

安全事件日志中不会生成其他无关的事件，例如没有调试数据等。

- 安全事件记录格式：
 - 记录的**ACCEPT**事件数据如下所示：

```
May 5 09:05:07 action = ACCEPT project_id = 736672c700cd43e1bd321aef940365c
log_resource_ids = ['4522efdf-8d44-4e19-b237-64cafc49469b', '42332d89-df42-4588-a2bb-3ce50829ac51']
vm_port = e0259ade-86de-482e-a717-f58258f7173f
以太网 (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
TCPOptionSACKPermitted (kind = 4, length = 2), TCPOptionTimestamps (种类= 8, 长度= 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)
```

- 记录**DROP**事件的数据：

```
May 5 09:05:07 action = DROP project_id = 736672c700cd43e1bd321aef940365c
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, 标识= 36638, 偏移= 0,
选项=无, 原型= 6, src = '172.24.4.10', tos = 0, total_length = 60, ttl = 63, 版本= 4),
tcp (ack = 0, bits = 2, TCPOptionSACKPermitted
(kind = 4, length = 2), TCPOptionTimestamps (kind = 8, length = 1)
, csum = 15097, dst_port = 80, offset = 10, option = [TCPOptionMaximumSegmentSize (kind = 2, length = 4, max_seg_size = 1460) 10, ts_ecr =
SEQ = 3284890090, src_port = 47825, 迫切= 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/cgiit/openstack/neutron/tree/doc/source/admin/config-logging.rst%0AURL: https://docs.openstack.org/neutron/queens/admin/config-logging.html&field.tags=doc)

更新日期：2018-03-07 21:05



(<https://creativecommons.org/licenses/by/3.0/>)

除另有说明外，本文档受 [Creative Commons Attribution 3.0](https://creativecommons.org/licenses/by/3.0/) 许可的授权 (<https://creativecommons.org/licenses/by/3.0/>)。查看所有 [OpenStack 法律文件](http://www.openstack.org/legal) (<http://www.openstack.org/legal>)。

🐛 发现错误？报告错误 ([https://bugs.launchpad.net/neutron/+filebug?](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/cgiit/openstack/neutron/tree/doc/source/admin/config-logging.rst%0AURL: https://docs.openstack.org/neutron/queens/admin/config-logging.html&field.tags=doc)

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:%2043DF2709ACBDC86686A40B75FD34E96880427D0%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)

🔗 问题吗？ (<http://ask.openstack.org>)



- Neutron 12.0.1
 - (../index.html)
 - 安装指南 (../install/index.html)
 - OpenStack网络指南 (index.html)
 - 介绍 (intro.html)
 - 组态 (config.html)
 - 部署示例 (deploy.html)
 - 操作 (ops.html)
 - 移民 (migration.html)
 - 杂 (misc.html)
 - 存档的内容 (archives/index.html)
 - 中子配置选项 (../configuration/index.html)
 - 命令行界面参考 (../cli/index.html)
 - 中子特征分类 (../feature_classification/index.html)
 - 贡献者指南 (../contributor/index.html)

页面内容

- 支持的日志资源类型
- 组态
 - 可信项目policy.json配置
- 操作员工作流
 - 启用/禁用日志
- 事件收集描述

OpenStack的

- 项目 (<http://openstack.org/projects/>)
- OpenStack安全 (<http://openstack.org/projects/openstack-security/>)
- 常见问题 (<http://openstack.org/projects/openstack-faq/>)
- 博客 (<http://openstack.org/blog/>)
- 新闻 (<http://openstack.org/news/>)

社区

- 用户组 (<http://openstack.org/community/>)
- 活动 (<http://openstack.org/community/events/>)
- 工作 (<http://openstack.org/community/jobs/>)
- 公司 (<http://openstack.org/foundation/companies/>)
- 有助于 (<http://docs.openstack.org/infra/manual/developers.html>)

文档

- OpenStack手册 (<http://docs.openstack.org>)
- 入门 (<http://openstack.org/software/start/>)
- API文档 (<http://developer.openstack.org>)
- 维基 (<https://wiki.openstack.org>)

品牌与法律

- 标志和指南 (<http://openstack.org/brand/>)
- 商标政策 (<http://openstack.org/brand/openstack-trademark-policy/>)
- 隐私政策 (<http://openstack.org/privacy/>)
- OpenStack CLA (https://wiki.openstack.org/wiki/How_To_Contribute#Contributor_License_Agreement)

保持联系

(<https://twitter.com/OpenStack>) (<https://www.youtube.com/user/OpenStackFoundation>)

OpenStack项目是在Apache 2.0许可 (<http://www.apache.org/licenses/LICENSE-2.0>)下提供的。Openstack.org由 [Rackspace云计算提供支持 \(http://rackspace.com\)](http://rackspace.com)。