



Monitoring OpenStack

OpenStack PowerPack version 100

Table of Contents

Introduction	3
What is OpenStack?	3
What Does the OpenStack PowerPack Monitor?	4
Installing the OpenStack PowerPack	4
Configuration and Credentials	6
Configuring OpenStack for Monitoring	6
Prerequisites for Monitoring OpenStack	6
Assigning a Role to a User	7
Adding the User Role to API Policy Endpoints	7
Policy Permissions for Administrators	8
Policy Permissions for Non-Administrator Users	10
Creating a SOAP/XML Credential for OpenStack	12
Discovery	14
Creating an OpenStack Virtual Device	14
Discovering OpenStack Component Devices	15
Viewing OpenStack Component Devices	15
Relationships Between Component Devices	15

Chapter

1

Introduction

Overview

This manual describes how to monitor OpenStack resources in SL1 using the *OpenStack PowerPack*.

The following sections provide an overview of OpenStack and the *OpenStack PowerPack*:

This chapter covers the following topics:

<i>What is OpenStack?</i>	3
<i>What Does the OpenStack PowerPack Monitor?</i>	4
<i>Installing the OpenStack PowerPack</i>	4

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is OpenStack?

OpenStack is an open-source software platform for cloud computing. It uses numerous interrelated components to control large pools of compute, storage, and networking resources throughout a data center. Users can manage their OpenStack resources through the OpenStack portal, the OpenStack API, or the OpenStackClient (OSC) command line interface.

What Does the OpenStack PowerPack Monitor?

To monitor OpenStack resources using SL1, you must install the *OpenStack PowerPack*. This PowerPack enables you to discover, model, and collect data about OpenStack devices.

The *OpenStack PowerPack* includes:

- Two example Credentials you can use as templates to create SOAP/XML credentials to connect to the OpenStack domain you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for OpenStack resources
- Device Classes for each of the OpenStack component devices that SL1 monitors
- Event Policies and corresponding alerts that are triggered when OpenStack component devices meet certain status criteria

NOTE: The *OpenStack PowerPack* supports OpenStack.org distribution.

Installing the OpenStack PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *OpenStack PowerPack*.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the **Enable Selective PowerPack Field Protection** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the **System Administration** manual.)

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the [ScienceLogic Support Site](#).
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter

2

Configuration and Credentials

Overview

The following sections describe how to configure OpenStack resources for monitoring by SL1 using the OpenStack PowerPack:

This chapter covers the following topics:

Configuring OpenStack for Monitoring	6
Creating a SOAP/XML Credential for OpenStack	12

Configuring OpenStack for Monitoring

To discover OpenStack resources for monitoring by SL1, you must create a SOAP/XML credential that includes authentication information for an OpenStack user.

The user whose information is used in this credential can be either an administrator or a regular (non-administrator) user. Administrator credentials enable SL1 to discover an OpenStack domain and resource pool; regular user credentials enable SL1 to discover only a single project within a specified domain and those components that the user has permissions for in the policy files. The recommended policy edits described in the [Adding the User Role to API Policy Endpoints](#) section will enable non-administrator users to discover resource pools.

The following sections describe how to assign a role to an OpenStack user and then add that user role to the appropriate API policy endpoints.

Prerequisites for Monitoring OpenStack

Before completing the following sections, you must have already created the OpenStack domain and projects you want to monitor, the user whose information you will include in the SOAP/XML credential, and the role you want to assign to that user.

TIP: ScienceLogic recommends that you create a new user role that will be used only for ScienceLogic monitoring and then add this ScienceLogic-specific user role to the policy endpoints described in the [Adding the User Role to API Policy Endpoints](#) section. Having a ScienceLogic-specific user role makes it easier to manage the role's policy permissions without having to change any of your existing user roles.

Assigning a Role to a User

After you have created the user whose information you will include in the SOAP/XML credential, you must assign that user a role in a specific project. This can be done either in the OpenStack portal or using the OpenStackClient command line interface. Both methods are described in this section.

Method 1: OpenStack Portal

To assign the user a role using the OpenStack portal:

1. Log in to the OpenStack portal and navigate to the **Projects** page (Identity > Projects).
2. Locate the project you want to monitor. In the **Actions** column, click **[Manage Members]**.
3. If the user whose information you will include in the SOAP/XML credential does not already appear in the **Project Members** list, locate the user in the **All Users** list and click the plus (+) icon for that user.
4. Locate the user in the **Project Members** list and use the drop-down menu next to the user's name to select the user's role.
5. Click **[Save]**.

Method 2: Command Line Interface

To add a role to the user in a project using the OpenStackClient (OSC) command line interface, SSH into OSC and then use the following command format:

```
openstack role add <role name> --project <project name> user <username>
```

Adding the User Role to API Policy Endpoints

After you have assigned the user a role, you must add the user's assigned role to endpoints in the following OpenStack API policies:

- Keystone (identity services)
- Nova (compute services)
- Neutron (networking services)
- Cinder (block storage services)

For example, to allow a user to list OpenStack projects, Keystone's policy.json file needs to include the following rule:

```
"identity:list_projects" : "role: <user-role>"
```

A rule can also contain multiple roles by using the "or" syntax. For example:

```
"identity:list_projects" : "role: <user-role-1> or role: <user-role-2>"
```

By default, a role can be any of the following:

- admin
- user
- member

Policy Permissions for Administrators

For administrator users, you must update the following policies:

Keystone Policy

An administrator user defined in the SOAP/XML credential needs permissions to the following endpoints defined in `/etc/keystone/policy.json`:

- `identity:get_region`
- `identity:list_regions`
- `identity:get_endpoint`
- `identity:list_endpoints`
- `identity:get_domain`
- `identity:list_domains`
- `identity:get_project`
- `identity:list_projects`

Nova Policy

An administrator user defined in the SOAP/XML credential needs permissions to the following endpoints defined in `/etc/nova/policy.json`:

- `os_compute_api:os-aggregates:index`
- `os_compute_api:os-aggregates:show`
- `os_compute_api:os-extended-server-attributes`
- `os_compute_api:flavors`
- `os_compute_api:os-hosts`
- `os_compute_api:os-hypervisors`
- `os_compute_api:limits`
- `os_compute_api:os-networks`
- `os_compute_api:os-networks:view`
- `os_compute_api:os-networks-associate`
- `os_compute_api:os-security-group-default-rules`
- `os_compute_api:os-security-groups`
- `os_compute_api:os-server-diagnostics`
- `os_compute_api:os-server-groups`

- os_compute_api:os-server-usage
- os_compute_api:servers:detail
- os_compute_api:servers:index:get_all_tenants
- os_compute_api:servers:detail:get_all_tenants
- os_compute_api:servers:show
- os_compute_api:servers:show:host_status
- os_compute_api:os-services
- os_compute_api:os-simple-tenant-usage:show
- os_compute_api:os-simple-tenant-usage:list
- os_compute_api:os-tenant-networks
- os_compute_api:os-virtual-interfaces
- os_compute_api:os-volumes
- os_compute_api:os-volumes-attachments:show

Neutron Policy

An administrator user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/neutron/policy.json:

- get_subnet
- get_subnet:segment_id
- get_subnetpool
- get_address_scope
- get_network
- get_network:router:external
- get_network:segments
- get_network:provider:network_type
- get_network:provider:physical_network
- get_network:provider:segmentation_id
- get_network:queue_id
- get_network_ip_availabilities
- get_network_ip_availability
- get_segment
- get_port
- get_port:queue_id
- get_router
- get_router:distributed
- get_router:ha

- get_dhcp-networks
- get_l3-routers
- get_network_profiles
- get_network_profile
- get_flavors
- get_flavor

Cinder Policy

An administrator user defined in the SOAP/XML credential needs permission to the following endpoint defined in /etc/cinder/policy.json:

- volume_extension:services:index

Policy Permissions for Non-Administrator Users

For regular (non-administrator) users, you must update the following policies:

Keystone Policy

A regular user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/keystone/policy.json:

- identity:get_region
- identity:list_regions
- identity:get_endpoint
- identity:list_endpoints
- identity:get_domain
- identity:list_domains
- identity:get_project
- identity:list_projects

Nova Policy

A regular user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/nova/policy.json:

- os_compute_api:os-aggregates:index
- os_compute_api:os-aggregates:show
- os_compute_api:os-extended-server-attributes
- os_compute_api:flavors
- os_compute_api:os-hosts
- os_compute_api:os-hypervisors
- os_compute_api:limits
- os_compute_api:os-networks

- os_compute_api:os-networks:view
- os_compute_api:os-networks-associate
- os_compute_api:os-security-group-default-rules
- os_compute_api:os-security-groups
- os_compute_api:os-server-diagnostics
- os_compute_api:os-server-groups
- os_compute_api:os-server-usage
- os_compute_api:servers:detail
- os_compute_api:servers:index:get_all_tenants
- os_compute_api:servers:detail:get_all_tenants
- os_compute_api:servers:show
- os_compute_api:servers:show:host_status
- os_compute_api:os-services
- os_compute_api:os-simple-tenant-usage:show
- os_compute_api:os-simple-tenant-usage:list
- os_compute_api:os-tenant-networks
- os_compute_api:os-virtual-interfaces
- os_compute_api:os-volumes
- os_compute_api:os-volumes-attachments:show

Neutron Policy

A regular user defined in the SOAP/XML credential needs permissions to the following endpoints defined in /etc/neutron/policy.json:

- get_subnet
- get_subnet:segment_id
- get_subnetpool
- get_address_scope
- get_network
- get_network:router:external
- get_network:segments
- get_network:provider:network_type
- get_network:provider:physical_network
- get_network:provider:segmentation_id
- get_network:queue_id
- get_network_ip_availabilities
- get_network_ip_availability

- get_segment
- get_port
- get_port:queue_id
- get_router
- get_router:distributed
- get_router:ha
- get_dhcp-networks
- get_l3-routers
- get_network_profiles
- get_network_profile
- get_flavors
- get_flavor

Creating a SOAP/XML Credential for OpenStack

To configure SL1 to monitor OpenStack, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *OpenStack* PowerPack to communicate with your OpenStack domain.

The PowerPack includes two example SOAP/XML credentials that you can edit for your own use:

- **OpenStack Admin - Example.** This credential is for administrators and will discover all projects contained within the specified domain.
- **OpenStack User - Example.** This credential is for regular (non-administrator) users and will discover a single project within a specified domain and those components that the user has permissions for in the policy files.

NOTE: During discovery, SL1 discovers only those OpenStack components within the single domain that is specified in the SOAP/XML credential, regardless of whether the credential is for an administrator or a regular user. To discover multiple domains, you must create a separate credential for each domain, which results in each domain being discovered with its own separate dynamic component map. To load-balance multiple domains, ScienceLogic recommends discovering different domains on different Data Collectors or All-In-One Appliances.

To configure a SOAP/XML credential to access OpenStack:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **OpenStack Admin - Example** or **OpenStack User - Example** credential, then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears.

3. Complete the following fields:

Basic Settings

- **Profile Name.** Type a name for the OpenStack credential.
- **Content Encoding.** Select *text/xml*.
- **Method.** Select POST.
- **HTTP Version.** Select HTTP/1.1.
- **URL.** Type "http://<IP Address>:<Port>", replacing <IP address> with the IP address or hostname of the OpenStack domain and replacing <Port> with the appropriate port number.
- **HTTP Auth User.** Type the OpenStack username.
- **HTTP Auth Password.** Type the OpenStack user's password.
- **Timeout (seconds).** Type "120".

Proxy Settings

- **Hostname/IP.** Leave this field blank.
- **Port.** Type "0".
- **User.** Leave this field blank.
- **Password.** Leave this field blank.

CURL Options

- **CURL Options.** Do not make any selections in this field.

SOAP Options

- **Embedded Password [%P].** Leave this field blank.
- **Embed Value [%1].** Type the OpenStack domain ID.
- **Embed Value [%2].** If you are creating a credential for a regular (non-administrator) user, type the OpenStack project name. Otherwise, leave this field blank.
- **Embed Value [%3].** Leave this field blank.
- **Embed Value [%4].** Leave this field blank.

HTTP Headers

- **HTTP Headers.** Do not make any selections in this field.

4. Click the [Save As] button.

Chapter

3

Discovery

Overview

The following sections describe how to discover OpenStack resources for monitoring by SL1 using the OpenStack PowerPack:

This chapter covers the following topics:

Creating an OpenStack Virtual Device	14
Discovering OpenStack Component Devices	15
Viewing OpenStack Component Devices	15

Creating an OpenStack Virtual Device

To discover OpenStack resources, you must first create a **virtual device** that represents the root device for the OpenStack domain. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your OpenStack root device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Complete the following fields:
 - **Device Name**. Type a name for the device.

- **Organization.** Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- **Device Class.** Select *OpenStack | Cloud Virtual Service*.
- **Collector.** Select the collector group that will monitor the device.

4. Click the **[Add]** button to create the virtual device.

Discovering OpenStack Component Devices

To discover and model the components of your OpenStack domain, you must manually align the "OpenStack: Account Discovery" Dynamic Application with the OpenStack virtual device. When you do so, the "OpenStack: Account Discovery" Dynamic Application uses the virtual device as the root component device representing the OpenStack account and creates child component devices for all of the resources used by that account.

To align the "OpenStack: Account Discovery" Dynamic Application to your OpenStack virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon () for your OpenStack virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Action]** button and select *Add Dynamic Application* from the menu.
5. On the **Dynamic Application Alignment** modal page:
 - In the **Dynamic Applications** field, select *OpenStack: Account Discovery*.
 - In the **Credentials** field, select the credential you created for OpenStack.
6. Click the **[Save]** button to align the Dynamic Application with the OpenStack virtual device and discover the OpenStack domain and resources.

Viewing OpenStack Component Devices

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can also view OpenStack component devices in the following place in the user interface:

- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an OpenStack service, find the OpenStack cloud virtual service device and click its plus icon (+).

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between the following component devices:

- Virtual machines and hypervisors
- Virtual machines and networks

© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see <https://sciencelogic.com/company/legal>.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010