

Stratus Cloud Solution



Stratus Cloud Solution Installation Guide

Notice

The information contained in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF STRATUS TECHNOLOGIES, STRATUS MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE.

Stratus Technologies assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. Software described in Stratus documents (a) is the property of Stratus Technologies Bermuda, Ltd. or the third party, (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

Stratus documentation describes all supported features of the user interfaces and the application programming interfaces (API) developed by Stratus. Any undocumented features of these interfaces are intended solely for use by Stratus personnel and are subject to change without warning.

This document is protected by copyright. All rights are reserved. Stratus Technologies grants you limited permission to download and print a reasonable number of copies of this document (or any portions thereof), without charge, for your internal use only, provided you retain all copyright notices and other restrictive legends and/or notices appearing in the copied document.

Copyrights

Stratus, the Stratus logo, everRun, and SplitSite are registered trademarks of Stratus Technologies Bermuda, Ltd. The Stratus Technologies logo, the Stratus 24 x 7 logo, and Automated Uptime are trademarks of Stratus Technologies Bermuda, Ltd.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Intel and the Intel Inside logo are registered trademarks and Xeon is a trademark of Intel Corporation or its subsidiaries in the United States and/or other countries/regions.

Microsoft, Windows, Windows Server, and Hyper-V are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries/regions.

VMware is a registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

The registered trademark Linux is used pursuant to a sublicense from the Linux Mark Institute, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Google and the Google logo are registered trademarks of Google Inc., used with permission. The Chrome browser is a trademarks of Google Inc., used with permission.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation.

Red Hat is a registered trademarks of Red Hat, Inc. in the United States and other countries.

Dell is a trademark of Dell Inc.

Hewlett-Packard and HP are registered trademarks of Hewlett-Packard Company.

All other trademarks and registered trademarks are the property of their respective holders.

Manual Name: Stratus Cloud Solution Installation Guide

Product Release Number: Stratus Cloud Solution Release 1.0.0.0

Publication Date: Monday, October 20, 2014

Stratus Technologies, Inc.

111 Powdermill Road

Maynard, Massachusetts 01754-3409

© 2014 Stratus Technologies Bermuda, Ltd. All rights reserved.

Table of Contents

Chapter 1: Stratus Cloud Solution Installation Guide	1
Stratus Cloud Solution Installation Overview	2
OpenStack Overview	2
Stratus Cloud Solution Hardware Overview	4
Stratus Cloud Solution Hardware Recommendations	4
Stratus Cloud Solution Hardware Requirements	5
Stratus Cloud Solution Software Overview	7
Required Software	7
Supported Internet Browsers	7
Supported Operating Systems	8
Required OpenStack Components	8
Network Design	11
OpenStack Installation and Configuration	13
Heat Installation Prerequisites and Processes	13
Installation Overview Flowcharts	14
Physical Connectivity	15
Storage Considerations	16
Configuring OpenStack for Evacuation and Migration	16
Supporting Instance Evacuations	19
Addressing Installation Errors	20
GRE Network Configuration	21
MySQL Connections	21
OpenStack Verification and Testing	23
OpenStack Verification	23
High Availability and Resiliency Testing	23
Debugging OpenStack	24
Installing the Stratus Cloud Solution	25
Installing CentOS	25
Installing the Stratus Cloud Solution	26
Setting Up Your Mail Server	29

1

Chapter 1: Stratus Cloud Solution Installation Guide

This installation guide does not intend to provide a one-stop solution to all the issues in a production-grade cloud, but serves as guide to be used as a baseline for building the production OpenStack Stratus Cloud Solution.

This guide also provides technically knowledgeable field engineers with an option to set up a production-grade OpenStack cloud with all the features that are required for and supported by the Stratus Cloud Solution. The architecture of this implementation can be extended or simplified to meet your requirements.

Related Topics

["Stratus Cloud Solution Installation Overview" on page 2](#)

["OpenStack Overview" on page 2](#)

["Stratus Cloud Solution Hardware Recommendations" on page 4](#)

["Stratus Cloud Solution Hardware Overview" on page 4](#)

["OpenStack Installation and Configuration" on page 13](#)

["OpenStack Verification and Testing" on page 23](#)

["Installing the Stratus Cloud Solution" on page 25](#)

Stratus Cloud Solution Installation Overview

The Stratus Cloud Solution (SCS) enables IT administrators to efficiently implement and manage a multiple availability level cloud, including support for highly available legacy applications. This allows IT administrators to provide an intuitive service catalog and application administration for end users.

OpenStack installation and configuration is not always an easy task. Each OpenStack installation is unique by virtue of the workload it intends to support, the differences in hardware and networking, and the security and compliance requirements. Note that SCS is deployed as a virtual appliance, which can be deployed as an instance (a virtual machine managed in the OpenStack cloud), or as a virtual machine, managed by a specific hypervisor.

Related Topics

["OpenStack Overview" on page 2](#)

OpenStack Overview

OpenStack is a group of interrelated open-source projects designed to provide massively scalable public and private clouds. The following services and projects are used throughout this document.

Service	Project Name	Description
Dashboard	Horizon	Allows you to interact with OpenStack services to launch an instance, assign IP addresses, set access controls, and other parameters.
Compute	Nova	Provisions and manages large networks of virtual machines on demand.
Networking	Neutron	Enables network connectivity as a service among interface devices managed by other OpenStack services; usually Compute. Allows you to create and attach interfaces to networks. Neutron features a plugable architecture that supports many popular networking vendors and technologies.
Object Storage	Swift	Stores and gets files. Does not mount directories like a file server.

Service	Project Name	Description
Block Storage	Cinder	Provides persistent block storage to guest virtual machines.
Identity service	Keystone	Provides authentication and authorization for the OpenStack services. Also provides a service catalog within a particular OpenStack cloud.
Image service	Glance	Provides a registry of virtual machine images; used by Compute to provision instances.
Telemetry service	Ceilometer	Monitors and meters the OpenStack cloud for billing, benchmarking, scalability, and statistics purposes.
Orchestration service	Heat	Orchestrates multiple composite cloud applications by using either the native HOT template format or the AWS CloudFormation template format, through both an OpenStack-native REST API and a CloudFormation-compatible query API.

Stratus Cloud Solution Hardware Overview

This section provides a general overview of hardware requirements and recommendations. Your exact hardware requirements should be calculated by the number of instances and resource needs of the workloads.

Related Topics

["Stratus Cloud Solution Hardware Requirements" on page 5](#)

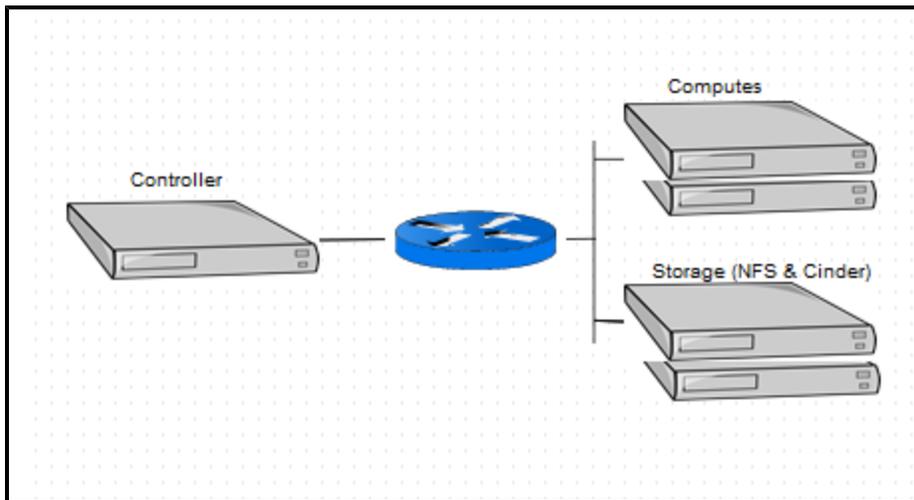
["Stratus Cloud Solution Hardware Recommendations" on page 4](#)

Stratus Cloud Solution Hardware Recommendations

The Stratus Cloud Solution does not impose any hardware requirements. The Stratus Cloud Solution works with any OpenStack cloud implementation. However, Stratus recommends configuring redundancy into the hardware to mitigate downtime.

The minimum suggested OpenStack hardware configuration consists of a controller node that runs the OpenStack core services, and at least two compute nodes which host the workloads. Two compute nodes are required for failover purposes in order to make the instances highly available.

Shared storage is provided by NFS storage, and cinder node provides the block storage. A deployment diagram is shown in the following illustration.



Hardware requirements for the Stratus Cloud Solution are shown in the following table.

Node or Switch	Quantity	CPU	Memory	Storage	Example
Controller node	1	Intel Xeon E5 2.6 GHz 6-core	8 x16 GB	6 x 1 TB SATA	Supermicro CSE-119XTQ-BR 700 WB
Compute node	2	Intel Xeon E5 2.6 GHz 6-core	8 x16 GB	6 x 1 TB SATA	Supermicro CSE-119XTQ-BR 700 WB
Storage node	2	Intel Xeon E5 2.6 GHz 6-core	4 x16 GB	24 x 1 TB SATA	216BE26-R1K28LPB
Network switch	2	n/a	n/a	n/a	DCS-7050T-36-F



Note: The hardware models and configurations shown in the table are suggestions. You can select any vendor and configuration, though 10G switches are recommended. Stratus does not provide a warranty on the hardware.

Stratus Cloud Solution Hardware Requirements

OpenStack Services on the Controller

OpenStack projects can be configured to run on separate nodes. However, for simplicity and maintainability, the core projects (namely Horizon, Keystone, and Glance) are deployed on a single node. Neutron typically is configured to run on a separate node and requires high bandwidth. This installation bundles Neutron services on the same controller node.

Block Storage or Cinder node

Block storage (Cinder) is configured on separate node clusters with expandable storage.

Compute nodes

Compute nodes:

- Provide CPU and memory for the instances
- Require many CPU cores and memory
- Can be horizontally scaled as your application needs grow

The following example shows typical calculations for determining your exact hardware requirements.

Application Requirements

Instances to run: 100

VCPUs/Instance: 2

Memory/Instance: 4 GB

Oversubscription: No

This translates to:

CPU Requirements

200 GHz of CPU capacity (100 virtual machines x 2 GHz/vCPU)

Approximate maximum: five cores (16 GHz / 2.4 GHz per core)

Based on:

E5 2640 sockets (200 GHz / 2.4 GHz per CPU / six cores per socket)

5 - 6 dual-core servers (11 sockets / two sockets per server)

17 virtual machines per server (100 virtual machines / six servers)

Memory Requirements

Approximately four 128 GB machines (400 GB / 128 GB; balanced with six machines for CPU)

To support 400 GB of total memory (100 virtual machines * 4 GB per virtual machine)

Cent OS 6.5 Image Requirements

The image used for the appliance installation must provide at least 150 GB of root space. To accomplish this, the QCOW2 file must have a virtual size of greater than or equal to 150 GB, and the flavor used to create the virtual machine must specify greater than or equal to 150 GB of root space.

Stratus Cloud Solution Software Overview

This section provides a general overview of software requirements, versioning, and recommendations.



Note: Without the recommended software minimums, node evacuation will not work.

Related Topics

["Required Software" on page 7](#)

["Required OpenStack Components" on page 8](#)

["Supported Internet Browsers" on page 7](#)

["Supported Operating Systems" on page 8](#)

Required Software

The following software with the specified version number is required for the proper installation and operation of Stratus Cloud Solution.

Software	Version
MySQL Server	5.1.73
Python	2.6.6
Apache	2.2.15
Openvswitch	1.11.0
Puppet	3.7.0
Rabbitmq-server	3.1.5
Memcached	1.4.4
Libvirt	0.10.2
Python mod_wsgi	3.2.6

Supported Internet Browsers

The following table lists the supported operating systems and browsers.

Browsers

Browser	Version
Firefox (on Linux only)	27
Internet Explorer (Windows)	10
Firefox (Windows; Technology Preview only)	27
Google Chrome (Windows and Linux; Technology Preview only)	32.0

Supported Operating Systems

The following operating systems have been tested for deployment into a Stratus-managed OpenStack environment.

Windows Operating Systems

Operating System	Version
Windows	7
Windows Server 2008	R2

Linux Operating Systems

Operating System	Version
CentOS 64-bit	6.5
RedHat Enterprise	6.5
Linux Ubuntu	12.04

Required OpenStack Components

The OpenStack components and the version number required for proper installation and operation of Stratus Cloud Solution are listed as follows.

To find the versions currently running on your system, use the following command: `rpm -qa | grep <component name>`; for example: `nova`

Nova

Component	Version
OpenStack-nova-cert	1.1-3.el6
OpenStack-nova-conductor	1.1-3.el6
OpenStack-nova-common	1.1-3.el6
OpenStack-nova-novncproxy	1.1-3.el6
OpenStack-nova-scheduler	1.1-3.el6
Python-nova	1.1-3.el6
OpenStack-nova-console	1.1-3.el6
Python-novaclient	2.17.0-2.el6
OpenStack-nova-api	1.1-3.el6

Glance

Component	Version
Python-glance-client	0.12.0-1.el6
Python-glance	1.1-1.el6
OpenStack-glance	1.1-1.el6

Heat

Component	Version
OpenStack-heat-api-cfn	1.2-1.0.el6
OpenStack-heat-common	1.2-1.0.el6
OpenStack-heat-engine	1.2-1.0.el6
OpenStack-heat-api	1.2-1.0.el6
Python-heatclient	0.2.9-1.el6

Neutron

Component	Version
OpenStack-neutron	1.2-1.el6
Python-neutronclient	2.3.4-1.el6
Python-neutron	1.2-1.el6
OpenStack-neutron-openvswitch	1.2-1.el6
OpenStack-neutron-ml2	1.2-1.el6

Horizon

Component	Version
Python-django-horizon	1.1-4.el6

Cinder

Component	Version
OpenStack-cinder	1.1-3.el6

Component	Version
Python-cinder	1.1-3.el6
Python-cinderclient	1.0.9-1.el6

Keystone

Component	Version
Python-keystone	1.1-1.el6
OpenStack-keystone	1.1-1.el6
Python-keystoneclient	0.9.0-1.el6

RabbitMQ

Component	Version
rabbitmq-server	3.3.1-1

Network Design

The following table shows the networks configured in this implementation. This installation further assumes that the networks are configured using VLANs on the bonded *eth1* interface, and that *eth0* is the administrative network.

Purpose	Is routed?	Network Name	Examples from MVPI
Provides IPMI and SSH connectivity. This network is only available within the data-center.	Yes	Admin net	192.168.81.0/24
Routed network to access OpenStack APIs.	Yes	API net	192.168.82.0/24

Purpose	Is routed?	Network Name	Examples from MVPI
Routed network that provides connectivity to the floating IPs assigned to the virtual machines.	Yes	External net	192.168.83.0/24
OpenStack internal messageQ communication non-routed network.	No	MGMT net	10.200.10.0/24
OpenStack virtual machine to virtual machine communication non-routed network.	No	Data net	10.10.1.0/24
OpenStack cinder and NFS storage non-routed network.	No	Cinder storage	10.200.11.0/24

OpenStack Installation and Configuration

This section provides information for installations and configurations required for your OpenStack and Stratus Cloud Solution systems.



Note: Stratus labs are currently using CentOS 6.5. Unless otherwise stated, assume CentOS 6.5 as the operating system running on the systems.

Related Topics

["Heat Installation Prerequisites and Processes" on page 13](#)

["Installation Overview Flowcharts" on page 14](#)

["Physical Connectivity" on page 15](#)

["Storage Considerations" on page 16](#)

["Configuring OpenStack for Evacuation and Migration" on page 16](#)

["Supporting Instance Evacuations" on page 19](#)

["Addressing Installation Errors" on page 20](#)

["GRE Network Configuration" on page 21](#)

["MySQL Connections" on page 21](#)

Heat Installation Prerequisites and Processes

The following customer requirements and Heat procedures are required for the installation of Stratus Cloud Solution.

Customer Site Requirements

For the installation of Stratus Cloud Solution, the customer must have:

- An installed and functioning Ice House version of OpenStack
- Heat enabled for cloud installation and operation
- A CentOS 6.5 image in Glance
- Internet access enabled from within the cloud

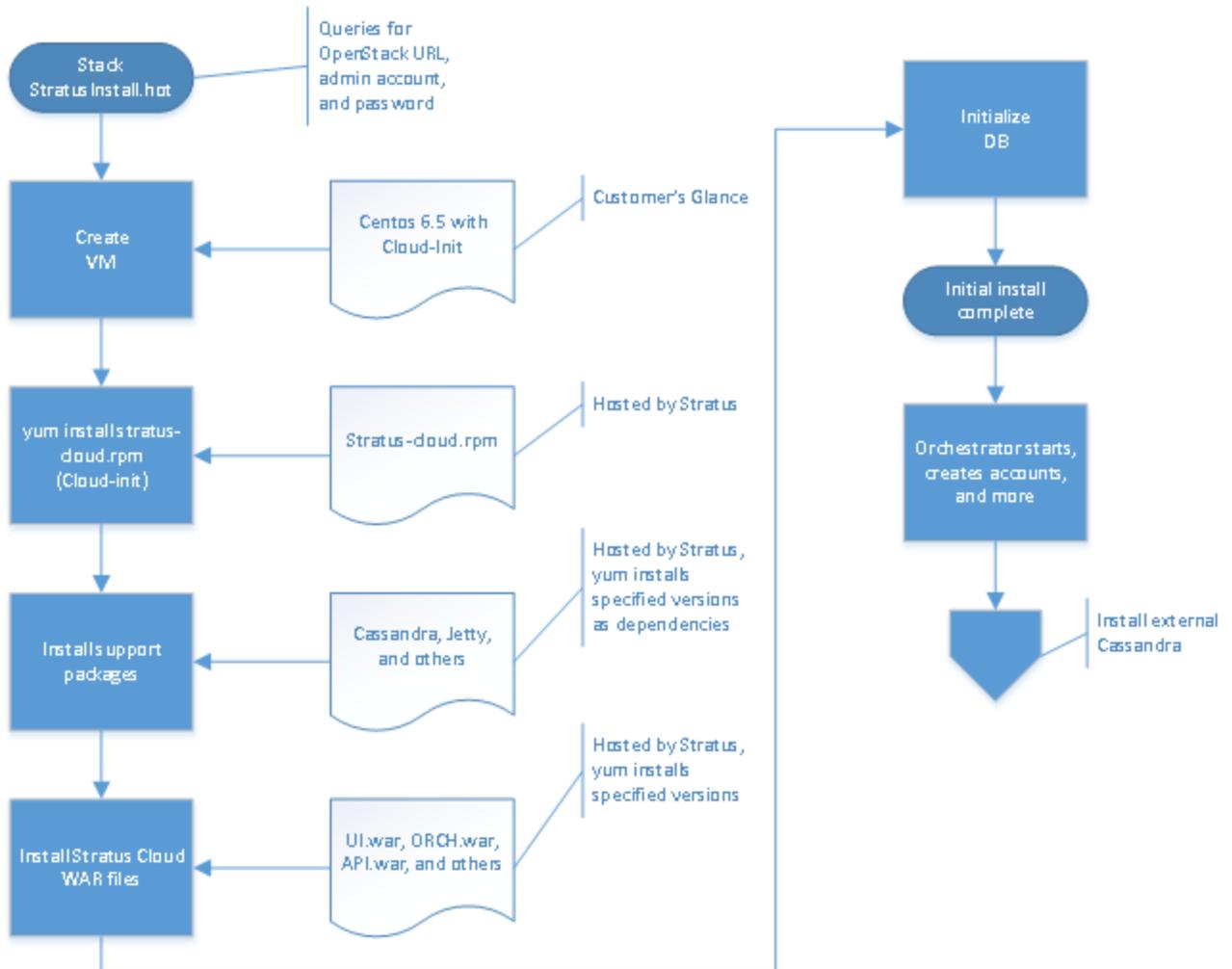
See also:

["Installation Overview Flowcharts" on page 14](#)

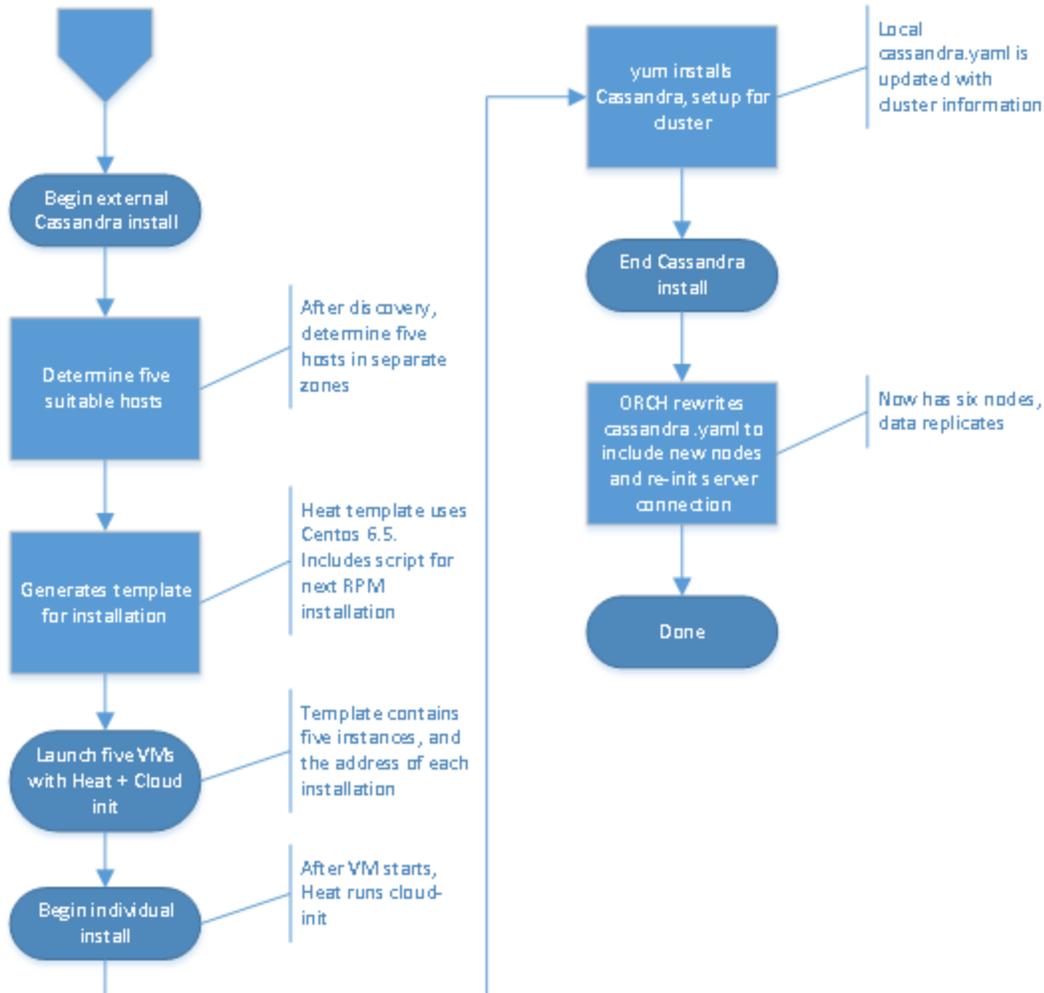
Installation Overview Flowcharts

Installing the Stratus Cloud Solution is a two-step process. The following flowcharts illustrate both steps of the Stratus Cloud Solution installation procedure.

Step 1:



Step 2:

**See also:**

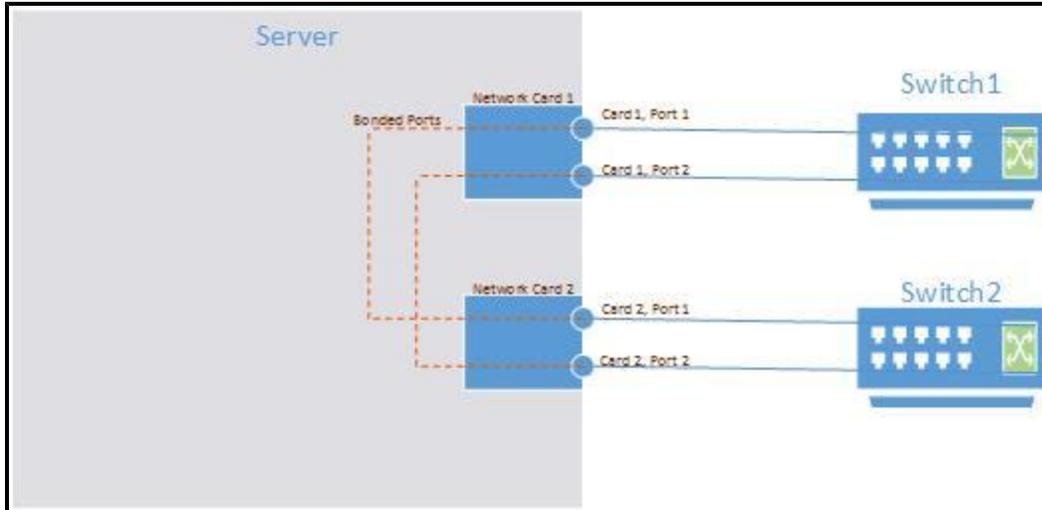
["Heat Installation Prerequisites and Processes" on page 13](#)

Physical Connectivity

In order to achieve highest level of availability, the physical network connectivity must be redundant. The following is a non-exhaustive list of suggestions recommended by Stratus:

- Hardware configuration should include at least two NICs, with enough ports in the card to support your networking requirements.
- Bond two ports from two different physical cards to protect against NIC port and NIC failure.
- Connect each port of the server bonded network to separate switches to protect against switch failures.

In the following diagram, the server contains two network cards; each card has two ports. The ports are marked as Card1Port1 through Card2Port2. Bond Card1Port1 and Card2Port1, and connect the ports to two separate switches.



For the switch configuration, configure VLANs on the switch matching the configuration in "[Network Design](#)" on page 11. Assign a temporary IP address, and verify network connectivity.

Storage Considerations

Stratus recommends the following considerations when setting up your storage environment.

- Protect the boot volume with either RAID 5 or RAID 6. A single disk boot volume can result in system failure (and failure of all instances) if the disk fails.
- Shared storage should be highly available, as all instances live on the shared storage.
- Cinder block shared storage should be highly available. Unless a high-end storage solution is used in the backend, the disks must at least be RAID 5 or 6 for physical disk failures protection.

Configuring OpenStack for Evacuation and Migration

Stratus strongly recommends the following OpenStack compute node configuration to ensure the correct operation for evacuations and migrations. If this configuration is not implemented, evacuations and migrations may fail.

To configure OpenStack for proper evacuation and migration:

1. On each compute node where NFS shared storage is used, add the following options to the NFS mount entry in `/etc/fstab`:

- `auto,lookupcache=none`
- Example: `/etc/fstab`:
- # NFS shared storage for instances:
 - `10.200.11.70:/KVMDataStore /var/lib/nova/instances
nfs auto,lookupcache=none 0 0`

2. Complete the following steps to ensure that your SSH keys are properly configured. For additional information, refer to the following websites:

- <https://lists.launchpad.net/openstack/msg24036.html>
- <https://ask.openstack.org/en/question/10335/ssh-resize/>
- <https://macnugget.org/projects/publickeys/>

3. Use an existing SSH key for `/root`, or create a new keypair using the following command:

- `ssh-keygen -t rsa`

4. Enter the file in which to save the key:

- `/root/.ssh/id_rsa`

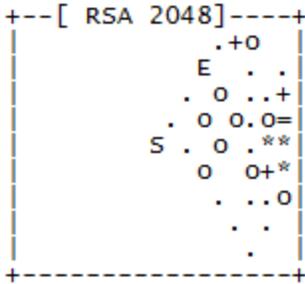
5. Enter the passphrase; leave the field blank for no passphrase.

6. Enter the same passphrase again.

- Your identification (private key) is saved in `/root/.ssh/id_rsa`.
- Your public key is saved in `/root/.ssh/id_rsa.pub`.

7. The key fingerprint is `55:45:fc:1f:2d:9b:f5:69:6d:03:5d:ef:2b:50:e8:11`
`root@<server_name>.<domain>.com`

8. The key's randomart image is:



9. A key pair is created, both public and private keys:

- The private root key is located at `/root/.ssh/id_rsa`.
- The public root key is located at `/root/.ssh/id_rsa.pub`.

10. Enable the Nova user for login using the command: `usermod -s /bin/bash nova`

11. Create the folder required by SSH, and move the private key from step 1 into the folder using the following commands:

- `mkdir -p /var/lib/nova/.ssh`
- `cp /root/.ssh/id_rsa /var/lib/nova/.ssh`
- `cat /root/.ssh/id_rsa.pub >> /var/lib/nova/.ssh/authorized_keys`
- Add these to `/var/lib/nova/.ssh/config`
- `Host *`
- `StrictHostKeyChecking no`
- `UserKnownHostsFile=/dev/null`
- `cd /var/lib/nova/.ssh`
- `chown nova *`
- `chgrp nova *`

12. Repeat steps 2 and 3 on each compute node.

13. All nodes share the same key pair; do not generate a new one for the other compute nodes. Instead, copy the key for the compute node on which it was created in step 1. For example:

- `(copy keys from compute-1 to compute-2) .. scp from compute-2`
- `scp root@compute-1:/root/.ssh/id_rsa* /root/.ssh`

14. Verify that the key is working properly, using the following commands:

- `su nova`
- **Example:** `ssh nova@compute-1 // you will log in to the node-another without a password`

15. Make sure that all libvirt user IDs and group IDs match across all nodes:

- For user ID:
 - `id -u qemu`
- For group ID:
 - `id -g qemu`
 - `id -u nova`
 - `id -g nova`

16. Modify `/etc/libvirt/qemu.conf`; uncomment and change these values:

- `dynamic_ownership=0`
- `user=root`
- `group=root`

17. Reboot the compute node.

Supporting Instance Evacuations

Stratus will supply a patch for your version of OpenStack Nova-Compute; however, you must specify your version. For instance evacuation support, the following procedure must be implemented on each compute node.



Note: After a YUM update on compute nodes that includes updates on the Nova compute service, `manager.py` is also updated. Therefore, `manager.py` must also be re-patched by executing the following process.

To support instance evacuations:

1. Navigate to `/usr/lib/python2.6/site-packages/nova/compute`.
2. In that directory, use the Vi editor to create a new file with the file name of: `evac-patch.txt`.
For example, `vi evac-patch.txt`.
3. In the `evac-patch.txt` file, paste in the following commands:

```
- /usr/lib/python2.6/site-pack-
ages/nova/compute/manager.py 2014-09-15
20:47:17.272501082 -0400

+++ /usr/lib/python2.6/site-pack-
ages/nova/compute/manager.py.new 2014-09-15
16:23:14.735380543 -0400

@@ -2502,6 +2502,7 @@

files = self._decode_files(injected_files)

kwargs = dict(
+ recreate=recreate,
context=context,
instance=instance,
image_meta=image_meta
```

4. Save and close the `evac-patch.txt` file.
5. From the directory `/usr/lib/python2.6/site-packages/nova/compute`, execute the following commands in this order:
 - For backup, execute the command: `cp manager.py ~/` .
 - Then, execute the patch command: `sudo patch < evac-patch.txt`.
6. Reboot the compute node.
7. Repeat this process on all compute nodes.

Addressing Installation Errors

If Errors are Encountered During Installation

When doing a clean installation of Stratus Cloud Solution, the installation script may fail if OpenStack cannot be verified. Should this occur and you attempt to run the install script again, it reports the installation is already complete. Address this issue using the following process.

To repair a failed Stratus Cloud Solution installation due to OpenStack verification issues:

1. Uninstall Stratus Cloud Solution using the command:

```
sudo sh clouds-0.1.0.19.5.sh uninstall.
```

2. Address any OpenStack issues identified in the installation error messages.

3. Re-install Stratus Cloud Solution using the command:

```
sudo sh clouds-0.1.0.19.5.sh install
http://192.168.91.50:5000/v2.0 admin admin.
```

See also:

["OpenStack Installation and Configuration" on page 13](#)

GRE Network Configuration

If you are using GRE networking, the maximum transmission unit (MTU) on the appliance must be set to 1400. If you are using VLAN networking, this configuration does not apply.

To configure GRE networking:

1. Edit the script located at `/etc/sysconfig/networking-scripts/ifcfg-eth0`.
2. In the script, change `MTU= "1500"` to `MTU="1400"`.
3. Save the changes in the script.

MySQL Connections

To prevent errors in Heat and Horizon, Stratus recommends setting the number of MySQL connections to 300.

To set MySQL connections:

1. Open the file `/etc/my.cnf`.
2. In the `/etc/my.cnf` file in the `[mysqld]` section, add the parameter: `max_connections = 300`. The following is an example of the the `/etc/my.cnf` file containing the correct MySQL connection settings:

```
[mysqld]
```

```
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql

# Disabling symbolic-links is recommended to prevent assorted
security risks

symbolic-links=0

default-storage-engine = innodb
innodb_file_per_table
collation-server = utf8_general_ci
init-connect = 'SET NAMES utf8'
character-set-server = utf8

bind-address = 0.0.0.0

max_connections = 300
```

3. Save and close the `/etc/my.cnf` file.
4. Restart `mysqld` using the command `service mysqld restart`.

OpenStack Verification and Testing

OpenStack verification and testing allows you to troubleshoot and resolve issues with your OpenStack and Stratus Cloud Solution configurations. You can identify and resolve issues in:

- Image upload
- Instance creation
- Floating IP configurations
- Security groups
- High Availability testing
- Resiliency testing
- Nodes
- Storage
- Debugging

Related Topics

["Debugging OpenStack" on page 24](#)

["OpenStack Verification" on page 23](#)

["High Availability and Resiliency Testing" on page 23](#)

OpenStack Verification

Use the following procedure for basic OpenStack testing:

1. Log in to horizon: `controller-1.<yourdomain>.stratus.com`.
2. Upload an image.
3. Create an instance.
4. Create a floating IP.
5. Assign a floating IP to the instance.
6. Create a security group to allow ssh and ping.
7. Verify that you can ping and ssh into the instance.

High Availability and Resiliency Testing

Use the following procedure for High Availability and resiliency testing.

1. Power down one of the switches; then run the OpenStack verification tests described in ["OpenStack Verification" on page 23](#).
2. Power on the switch and power down the other switch, then run the OpenStack verification tests described in ["OpenStack Verification" on page 23](#).
3. Reboot all the nodes in the cluster, then run the OpenStack verification tests described in ["OpenStack Verification" on page 23](#).
4. Storage tests: remove a disk from the RAID5 or RAID6 set. If you have RAID 5, then rebuilding the RAID array may be time-intensive.

See also:

["Debugging OpenStack" on page 24](#)

Debugging OpenStack

Use the following procedures to debug your OpenStack installation and configuration.

1. Start with the controller node to verify that all services are up:

```
$ nova-manage service list
```

```
$ neutron service list
```

```
$ cinder host list
```

2. Log files on the controller node are under `/var/log` directory:

```
Nova logs: /var/log/nova
```

```
Neutron logs: /var/log/neutron
```

```
http logs: /var/log/http
```

3. For compute nodes, the logs are under `/var/log/nova`.

Installing the Stratus Cloud Solution

Installing the Stratus Cloud Solution includes the CentOS installation and configuration, the Stratus Cloud Solution installation process, and configuring your email server to work with the Stratus Cloud Solution.

Related Topics

["Installing CentOS" on page 25](#)

["Installing the Stratus Cloud Solution" on page 26](#)

["Setting Up Your Mail Server" on page 29](#)

Installing CentOS

The first step in installing the Stratus Cloud Solution is installing the Cent Operating System.

To install CentOS for the Stratus Cloud Solution:

1. Upload a CentOS version 6.5 image with:
 - At least 160 GB or more of disk space /root space
 - 4v CPU
 - 8 GB RAM
2. Stratus recommends that you install *cloud-init*, and create an SSH key for your use.
3. If you do not have a CentOS version 6.5 *qcow2* image of the specified size located at `/root partition`, refer to the OpenStack instructions located at [OpenStack CentOS image guide](#).
4. When installing the CentOS, you must:
 - Use a custom disk
 - Delete the existing partitions
 - Create a `/root` 160 GB partition
 - And `/boot` using the remaining disk space, which is normally about 3 GB
5. To do this, run the command: `qemu-img create -f qcow2 /tmp/CentOS-6.5.qcow2 160G`
6. After the CentOS 6.5 *qcow2* file is created, upload this image to the OpenStack cloud using Horizon.

7. Create a special flavor for this instance with:
 - 4vCPU
 - 8192 MB RAM (no swap,no ephemeral)
 - 160 GB Root Disk
8. Using this new flavor, launch an instance using the new CentOS 6.5 image (optionally use an SSH key) on a network created off the external network. Stratus refers to this as a network application.

See also:

["Installing the Stratus Cloud Solution" on page 26](#)

Installing the Stratus Cloud Solution

After the CentOS installation is complete, install the Stratus Cloud Solution using the following procedure.

To install the Stratus Cloud Solution:

1. Navigate to the instance you created in the ["Installing CentOS" on page 25](#) procedure using the Horizon console by logging in as user *root* and use the password you assigned to *root* during installation. You may need to update the `/etc/udev/rules.d/70-persistent-net.rules` and remove the `eth0` entry, and rename `eth1` to `eth0`. This sometimes occurs when you deploy.
2. Update these files as follows:
 - `/etc/sysconfig/network` file with `HOSTNAME=YOUR HOST NAME`. Note that `**NOZEROCONF=yes` should already be there.
 - `/etc/hosts`: add an entry for `127.0.0.1` at the end for the hostname you just updated in the network file.
 - If you have not done so already, install the `cloud-init` using the OpenStack instructions in order to later use the SSH key. Cloud-init software allows an SSH key to be injected to the instance when you launch or deploy an instance. Without this, you cannot use an SSH key.
3. Reboot after these updates.
4. Assign this instance a floating IP address so that you can SSH to it using your key.
5. Login as *root* (`su - root`), navigate to `/opt`, and create a directory called `Release`.

6. Using SCP, securely copy your cloud install shell script to the `Release` directory.
7. Then: `CD /opt/Release.`
8. If you copied to your `/home/cloud-user` account, copy this account to `/opt/Release.`
9. Run the command `Chmod a+x cloud install script.sh.`
10. Find your end point for API access by going into Horizon Compute Access & Security, and click the API Access tab.
11. Use the identity service endpoint; for example, `http://192.168.100.50:5000/v2.0.`
You must know the admin user and the admin password for your OpenStack cloud.
12. Run the install script; for example, `./clouds-0.1.0.0, .sh install`
`http://192.168.11.50:5000/v2.0 admin admin.`
13. This begins the install process for the Stratus Cloud management software. The installation displays the following statuses:

```
./clouds-0.1.0.20.2.sh install http://192.168.100.5
0:5000/v2.0 admin admin

Verifying archive integrity... All good.
Uncompressing Stratus Clouds 0.1.0.20.2.....

--&gt; Checking current user...Ok
Error: No matching Packages to list

--&gt; @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
--&gt; Welcome to the Stratus-Clouds Installation
--&gt; Installing version 0.1.0.20.2
--&gt; @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
--&gt; A copy of this output will be located in:
--&gt; /opt/stratus/logs/install.log
--&gt; OpenStack Installation Location:
http://192.168.100.50:5000/v2.0
```

```
--&gt; OpenStack Admin Tenant: admin
--&gt; OpenStack Admin Password: admin
--&gt; Updating existing packages, may take a few minutes...
host-10-10-10-11.OpenStacklocal
--&gt; Local ip == 10.10.10.11
--&gt; Stopping necessary services...
--&gt; Installing packages
----&gt; ./apache-cassandra-2.0.8-0.fc14.noarch.rpm
----&gt; ./eclipse-jetty-9.2.1.v20140609-0.fc14.noarch.rpm
----&gt; ./elasticsearch-0.90.11-0.fc14.noarch.rpm
----&gt; ./logstash-1.4.2-1_2c0f5a1.noarch.rpm
----&gt; ./stratus-clouds-0.1.0.20.2-0.fc14.noarch.rpm
--&gt; Updating existing packages, may take a few minutes...Ok
-&gt; Installing rdo-release--&gt; Install nginx...Ok
--&gt; Updating firewall rules for 80, 443, 8080...
...add rule... INPUT -p tcp -m tcp --dport 80 -j ACCEPT
...add rule... INPUT -p tcp -m tcp --dport 443 -j ACCEPT
...add rule... INPUT -p tcp -m tcp --dport 9200 -j ACCEPT
...add rule... INPUT -p tcp -m tcp --dport 9300 -j ACCEPTOk
--&gt; Checking for novaclient program...Ok
--&gt; Checking for keystoneclient...Ok
--&gt; Verifying OpenStack information...
----&gt; Verifying OpenStack login...Ok
----&gt; Checking for ADMIN tenant...Ok
```

```
----&gt; Checking for ADMIN user...Ok
----&gt; Checking for ADMIN user role...Ok
----&gt; Checking for heat service...Ok
--&gt; Starting cassandra...
--&gt; Starting elasticsearch...
--&gt; Starting logstash...
--&gt; Starting nginx...
Updating /opt/jetty/resources/CloudMgmtExt.properties...Ok
--&gt; Installing an OpenStack rc file in /opt/stratus/osadmin.rc
--&gt; Starting jetty...
Wait for applications to start...
Initialized DB
Total Time : 0 hours, 6 minutes, 34 seconds17442..
--&gt; Completed database initialization
--&gt; Wait for application start
.--&gt; Installation complete
```

14. After a successful install, update the `/opt/jetty/resources/CloudMgmtExt.properties` file for the email specifics. For more information, refer to ["Setting Up Your Mail Server" on page 29](#).
15. You can now go to `https://ThisCentOSFloatingIP`, and begin using your Stratus Cloud.

See also:

["Setting Up Your Mail Server" on page 29](#)

Setting Up Your Mail Server

After setting up the appliance, you must set up your email server to coordinate with the new Stratus Cloud Solution installation. In the directory `/opt/jetty/resources`, edit your `CloudMgmtExt.properties` file as follows.



Note: Refer to your IT department for your specific mail server parameters, which are shown in red in the following example.

To set up your email server:

1. Add the following to your `CloudMgmtExt.properties` file:

```
## system mail properties ##  
  
# The system mail server host  
cloud.mgmt.mail.server.host=smtppmail.your_domain.com  
  
# The system mail server port (25 by default, generally 465  
for SSL and 587 for TLS)  
cloud.mgmt.mail.server.port=25  
  
# The email address that receiver can see in the header FROM  
cloud.mgmt.mail.sender.address=user_name@your_domain.com  
  
# Set to true if secure password authentication (SPA) is  
required by email server  
cloud.mgmt.mail.secure.password.authentication.required=false  
  
# The encryption type of the email server connection (DEFAULT,  
SSL or TLS)  
cloud.mgmt.mail.encryption.type=DEFAULT  
  
# The mail account username, required if the cloud.mg-  
mt.mail.secure.password.authentication.required set to true  
cloud.mgmt.mail.account.username=<change_on_setup>  
  
# The mail account password, required if the cloud.mg-  
mt.mail.secure.password.authentication.required set to true
```

```
cloud.mgmt.mail.account.password=<change_on_setup>
## password reset mail ##
# The callback URL pattern that sent via the forgot password
email. Change the host/ip if necessary
cloud.mgmt.mail.password.reset.url=https://your_cloud_serv-
er.your_domain.com/cloud/#login:passwordreset?useridentifier=
{0}&passwordresetcode={1}
## password initialize mail ##
# The callback URL pattern that sent via the initialize pass-
word email. Change the host/ip if necessary
cloud.mgmt.mail.password.initialize.url=https://your_cloud_
server.your_domain.com/cloud/#login:password?username={0}
```

2. Save and close the `CloudMgmtExt.properties` file.
3. Restart Jetty using the command `service jetty restart`.