

Installation manual for SUSE Cloud

This document describes how to bootstrap a full SUSE Cloud environment, by using Crowbar to provision OpenStack from bare metal servers. Currently it covers the SUSE Cloud Beta1 release, which is a technical preview.

Prerequisites

Hardware requirements

1. Crowbar admin node: x86_64 server with at least 2GB RAM and 40GB of disk.
2. OpenStack controller node: x86_64 server with at least 1GB RAM, and 4GB of disk **plus** however much extra you need for storing your VM images which will be launched on the compute nodes.
3. OpenStack compute nodes: x86_64 server with sufficient RAM and disk to run the hypervisor plus your VM images to your requirements.

N.B. the admin nodes *can* be run as VMs. This is not recommended for production installations, but should work nevertheless.

Network requirements

All nodes should be on a shared network segment, since the Crowbar admin node will act as a DHCP/TFTP/DNS/PXE server for the other nodes.

The Crowbar admin node wants to run on `192.168.124.10`. This means:

- If the admin node can route via `192.168.124.0/24` to get access to external software sources (YaST repos, etc.) you're fine. This may be the case if the Crowbar admin node is a VM guest, and routes via the VM host somehow.
- If you want to change the IP Address of the admin node you need to edit Crowbar's network proposal data in `/opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json`. For details on that see below.
- If this addressing scheme is otherwise incompatible with the rest of your network, it is possible to configure a second NIC (`eth1`) on the admin node which can see the rest of the world. This will require adjustments to `/opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json` as well. See below for an example. Note that this network will only be configured by Crowbar/Chef after the admin node is completely installed. Any existing configuration on that interface will be deleted and the interface will be shutdown during installation. Because of this it is essential that the admin node is able to access any external software repository that is configured on the admin node via the first NIC (`eth0`).

Note that if you configure `/etc/resolv.conf` on the admin node to point to upstream DNS nameservers, then the `bind` DNS software which automatically gets set up during the installation process will automatically be configured to forward requests for non-local records to those servers.

The [Crowbar Deployment Guide](#) (Section 4.2 and following) contains detailed information on how to adapt the network settings to your needs.

Shared storage requirements

There are no specific shared storage requirements for getting your cloud up and running; it is up to you to choose how to setup your block / object storage. Please see the [OpenStack documentation](#) for more information on these topics.

Software requirements

1. [SLES11 SP2 x86_64 installation media](#)
2. [SLE11 SP2 SMT installation media](#)
3. Access to SP2 Updates channel
4. SUSE Cloud ISO

Installation process

Please see the 'Trouble-shooting' section below if you run into problems.

Install Crowbar and Chef on the Crowbar admin node

- Install SLES11 SP2 on the Crowbar admin node. The 'Minimal' pattern or even a JeOS appliance should be sufficient to start with, but later you may need to install additional packages such as `yast2-network`, `rsync`, `nfs-client`, `screen` etc., depending on how you approach the below steps.
- Configure the network via YaST:
 - `eth0` (static IP):
 - IP Address: `192.168.124.10`
 - Subnet mask: `/24`
 - Hostname: `cb-sles-admin.example.com`
 - `hostname/dns`:
 - Hostname: `cb-sles-admin`
 - Domain Name: `example.com`
 - The above is an example - use whatever hostname is appropriate for your site, but note that `hostname -f` must give an FQDN, and you can't change the hostname later (doing so will break Chef, and the admin node will need to be reconfigured).

- Add SMT add-on and follow the install wizard, to configure SMT. (See the [SMT installation manual](#).) You can skip this step, if you have an SMT that offers the repositories mentioned below. It also needs to be reachable from the admin network.

Once SMT is set up, you need to mirror SLES 11 repositories (that will end up in `/srv/www/htdocs/repo/$RCE/`), using the following commands:

```
# smt repos SLES11-SP2-Core sle-11-x86_64 -e
# smt repos SLES11-SP2-Updates sle-11-x86_64 -e
# smt repos SLES11-SP1-Updates sle-11-x86_64 -e
# smt repos SLES11-SP1-Pool sle-11-x86_64 -e
# smt mirror # ... this will download ~ 13 GB of packages
```

- Disable the parts of SMT that we don't need for SUSE Cloud at this point:

```
# insserv -r smt
```

- Ensure that the install is fully patched to the latest SP2 updates:

```
# zypper up
```

- Add the SUSE Cloud ISO as an installation source via YaST (see "Handy Tips" below).

- Install Crowbar

- run `zypper install crowbar`

- Mirror the contents of the SLES11 SP2 x86_64 installation media into `/srv/tftpboot/suse-11.2/install/` on the Crowbar admin node. For example, if after inserting the DVD in the admin node:

```
# mount /dev/dvd /mnt
# rsync -avP /mnt/ /srv/tftpboot/suse-11.2/install/
# umount /mnt
```

or if the media is inserted on another machine on the network:

```
# mount /dev/dvd /mnt
# rsync -avPz /mnt/ 192.168.124.10:/srv/tftpboot/suse-11.2/install/
# umount /mnt
```

Note that in both cases, the trailing slash in `/mnt/` is crucial in order to ensure that `rsync` copies the *contents* of `/mnt` rather than the directory itself.

Rather than copying, you could also mount the media directly onto `/srv/tftpboot/suse-11.2/install`, or indirectly via `mount --bind`, or even via NFS if it is exported from elsewhere. However other approaches should be used with caution; for example, symlinking these directories to sources elsewhere may cause trouble for the TFTP server.

- Also mirror the SUSE Cloud installation media into `/srv/tftpboot/repos/Cloud/` using one of the techniques described for the previous step.
- Symlink SLES update channels to `/srv/tftpboot/repos`, to make them available to the Cloud nodes:

```
# ln -s /srv/www/htdocs/repo/$RCE/SLES11-SP1-Pool/sle-11-x86_64 \
    /srv/tftpboot/repos/SLES11-SP1-Pool
# ln -s /srv/www/htdocs/repo/$RCE/SLES11-SP1-Updates/sle-11-x86_64 \
    /srv/tftpboot/repos/SLES11-SP1-Updates
# ln -s /srv/www/htdocs/repo/$RCE/SLES11-SP2-Core/sle-11-x86_64 \
    /srv/tftpboot/repos/SLES11-SP2-Core
# ln -s /srv/www/htdocs/repo/$RCE/SLES11-SP2-Updates/sle-11-x86_64 \
    /srv/tftpboot/repos/SLES11-SP2-Updates
```

- *Alternatively* you can skip creating these symlinks (if you didn't set up SMT on the admin node) and edit `/opt/dell/barclamps/provisioner/chef/cookbooks/provisioner/templates/default/autoyast.xml.erb` instead, to point to external SMT instead of local repos -- this requires clients to resolve and route to that external SMT correctly!
- If you want to connect your admin node to an external network, you can do this by adapting `/opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json`. Here is a simple example for a bastion network config with a static IP for the admin node:

```

--- /opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json
+++ /opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json
@@ -90,6 +90,9 @@
    {
        "pattern": "single/./.*",
        "conduit_list": {
+         "bastion1": {
+         "if_list": [ "1g2" ]
+         },
        "intf0": {
            "if_list": [ "1g1" ]
        },
@@ -209,6 +212,20 @@
        "host": { "start": "192.168.124.161", "end": "192.168.124.161" }
    }
},
+ "bastion": {
+ "conduit": "bastion1",
+ "vlan": 50,
+ "use_vlan": false,
+ "add_bridge": false,
+ "subnet": "192.168.178.0",
+ "netmask": "255.255.255.0",
+ "broadcast": "192.168.178.255",
+ "router": "192.168.178.1",
+ "router_pref": 11,
+ "ranges": {
+ "admin": { "start": "192.168.178.39", "end": "192.168.178.39" }
+ }
+ },
+ "admin": {
+ "conduit": "intf0",
+ "vlan": 100,

```

- In case you want to change the IP of the admin node to some other network, and/or also change the networks configured by crowbar, you can do this by running the following command:

```

# sed -i.netbak -e 's/192.168.124/10.122.182/g' \
-e 's/192.168.125/10.122.187/g' \
-e 's/192.168.123/10.122.168/g' \
-e 's/192.168.122/10.122.172/g' \
/opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json

```

This will change the admin network to 10.122.182.0/24, and enable you to e.g. set the admin node IP to 10.122.182.10. It also changes the other networks used to different defaults. Make sure to review the **VLAN IDs** used in `/opt/dell/barclamps/network/chef/data_bags/crowbar/bc-template-network.json` and adapt them to your network. You might also want to add a `<router></router>` entry in the bmc network, otherwise your BMCs will not get a default gateway set and you'll likely only be able to access them from the admin node.

- As root on the admin node, run:

```

# zypper install screen
# screen -L /opt/dell/bin/install-chef-suse.sh

```

Running the script inside GNU screen in this manner is strongly recommended, since:

- the install process can make changes to the network configuration which could prematurely interrupt the script if it was run via the network (e.g. over `ssh`), and
 - all output will be captured to `./screenlog.0` which will greatly aid debugging if necessary. Of course `tmux` can be used instead of `screen` if you prefer :-)
- This command will install and configure chef, and use it to complete the installation of Crowbar and all required barclamps. It will take several minutes to complete.

- When it announces that the admin node has been deployed, you can then log into the Crowbar and Chef web interfaces:
 - Crowbar web UI on port 3000, i.e. <http://192.168.124.10:3000/> with username `crowbar` and password `crowbar`
 - Chef web UI on port 4040 i.e. <http://192.168.124.10:4040/> with username `admin` and password `password`
- In case you added a bastion network config via `bc-template-network.json`, you'll need to run

```
# crowbar network -U crowbar -P crowbar allocate_ip default <crowbar.example.com> bastion admin
# chef-client
```

Secure the services on the Crowbar admin node

- The first time you log into the Chef web UI on port 4040, it will prompt for a password change.
- To change the password for the Crowbar web UI on port 3000:
 - Click on `Barclamps` in the top right corner of the web UI.
 - Click on the arrow to the left of the Crowbar barclamp to expand it
 - Click the `Edit` button to edit the `Default` proposal.
 - Click on `Raw` to the right of `Attributes`.
 - Scroll through the attributes until you see something that looks like:

```
"users": {
  "machine-install": {
    "password": "0e7b02a8d2086009c1ff00cc26a827d981306cbd420b1862063e6df8534e0f6a13e45100b9
874d0a3fae5962c9ec2de12c0525b8c33685e8ee30406c4eee7133"
  },
  "crowbar": {
    "password": "crowbar"
  }
},
```

- Change the password.
- Click `Apply` and confirm you want to apply the changes.

Deploying Client Nodes

Base SLES Deployment

- PXE-boot another node on the same network as the Crowbar admin node (192.168.124.0/24).
- Once the client node comes up, it will appear in the Node Dashboard in the Crowbar web UI. It will be named for its MAC address, e.g.: `d52-54-00-47-7b-dc`.
- Click the node's name to view its details. It should be in State: Discovered.
- Click the `Edit` link.
- Click the `Allocate` button.
- A few seconds after allocating the node, it will reboot and commence SLES installation.
 - The node's status will update in the Crowbar web UI to `Installing`. Once it transitions to `Ready`, you have a new SLES client node.

OpenStack Component Deployment

- Make sure you have at least one client node running.
- In the Crowbar web UI, open the `Barclamps` menu and select `OpenStack`.
- Expand `Postgresql` and click `Create`. NOTE: do **not** use the `Mysql` barclamp; it's not supported and will potentially get removed later.
- One existing client node will be given the role `Postgresql-server`. Different nodes can be assigned by dragging them to the role, or clicking the `remove` button next to a role.
- Click `Apply`. **Some time will pass** (note: this action can take a couple of minutes to return), and PostgreSQL will be installed and configured on the client node. Success is indicated by the proposal's status indicator going green.
- Repeat the above three steps for each of the Keystone, Glance, Nova and Nova Dashboard barclamps. Various options can be set for each component when editing the proposal. In particular, note the default user accounts and passwords that are created - you should change these if you require a secure OpenStack deployment:
 - The admin user: `admin` with password `crowbar`.
 - The regular user: `crowbar` with password `crowbar`. This user is given its own project.

Using OpenStack

Uploading an Image and Launching an Instance

- After you have successfully deployed OpenStack using Crowbar, you'll want to use it. You can access it either using the Dashboard or the Nova API. You'll find a link to the Dashboard on the node that got the Nova Dashboard barclamp on the

overview page for that node in the Links section.

- Browse to the Dashboard and login using the user and password you specified in the keystone barclamp. (Default user: `crowbar`, password: `crowbar`)
- You'll find the `openrc.sh` (sometimes referred to as `NovaRC`) file by clicking on `Settings` in the top-right hand corner of the webpage. Download this file and source it in your shell, to set the access details for the Nova API. Note that this file is automatically provided by Chef on the OpenStack controller node as `/root/.openrc`.
 - If you are uncertain which node is the controller, open the `Barclamps` menu, select `OpenStack`, and click the `Nova` proposal you created earlier. Down the bottom of this screen the controller node will be listed with the `nova-multi-controller` role.
- To interact with the API, you should use the `python-novaclient` that provides the `nova` command from the `SUSE Cloud ISO`.
- Preparing images for OpenStack is easy using [SUSE Studio](#).
 - Make sure the network is set to DHCP, you don't use YaST2 Firstboot or any EULA dialogs, and you install `suse-ami-tools`. `suse-ami-tools` talks to the metadata-api and is used for pulling keypairs into the VM.
- Just build raw images and convert them to compressed `qcow2` images, after downloading them from Studio, using the following command (make sure to have `virt-utils` installed):

```
qemu-img convert -c -f raw -O qcow2 <image file> <final image file>
```

- To upload an image to glance, use this command:

```
glance add name="my-cloud-image" \
  is_public=True \
  container_format=bare \
  disk_format=qcow2 \
  < <final image file>
```

- To launch the instance, click the `Project` tab at the top-left, then `Images & Snapshot`, then click the `Launch` button to the right of your instance.

OpenStack CLI Commands

- As mentioned above, be sure to source the `openrc.sh` or `/root/.openrc` file in your shell before running these.
- Open ssh port in default security group:

```
nova secgroup-add-rule default tcp 22 22 0.0.0.0/0
nova secgroup-list-rules default
```

- Launch a new instance (this is the CLI equivalent of using the dashboard to launch an instance):

```
nova boot --flavor <flavor> --image <image> <name>
```

- Create volume (10GB):

```
nova volume-create --display_name="my volume" 10
```

- Attach volume to instance:

```
nova volume-attach <server> <volume> <device>
```

- List running services (in the cluster):

```
nova-manage service list
```

- Describe resource usage per node:

```
nova-manage service describe_resource <nodename>
```

- Refer to `nova help` and `nova help <command>` for more details.

Handy Tips

- The default root password for Crowbar-deployed client nodes is `root`.
- As copies of the SLES 11 SP2 DVD and SUSE Cloud media are present on the Crowbar admin node, the Crowbar admin node can also use those same directories as software sources, e.g.:

```
# zypper ar /srv/tftpboot/suse-11.2/install/ SLES-11-SP2
# zypper ar /srv/tftpboot/repos/Cloud/ SUSE-Cloud
```

- If you really want to know, in excruciating detail, exactly what the install script does, try:

```
# screen -L bash -ex /opt/dell/bin/install-chef-suse.sh
```

- While testing it can be useful to set `UseDNS No` in `/etc/ssh/sshd_config` on all nodes. This will eliminate login delays when SSHing to cloud nodes from hosts elsewhere that might not be resolvable by the Crowbar admin node's DNS server.
- If testing Crowbar in a VM, create a separate network for the admin node and deployed clients, e.g. a suitable libvirt network definition would be similar to the following. Bonus: If you use `yast firewall` to flag `virbr1` as internal, `eth0` as external, and enable masquerading, the admin node will be able to see the rest of the world (although only the VM host will be able to ssh *in* to the admin node and deployed clients on this network).

```
<network>
  <name>crowbar</name>
  <uuid>381dea14-8a34-ec60-8568-9a0d454c07cc</uuid>
  <forward mode='nat' />
  <bridge name='virbr1' stp='on' delay='0' />
  <mac address='52:54:00:D4:0A:6F' />
  <ip address='192.168.124.1' netmask='255.255.255.0'>
  </ip>
</network>
```

Trouble-shooting

Common pitfalls / gotchas, and suggested solutions

- Crowbar:
 - A Crowbar node hangs at `Unpacking initramfs` during PXE boot:
 - Your node probably does not have enough RAM. Try increasing to 2GB.
 - A Crowbar node which is a libvirt VM shuts down during the discovery/allocation phase and does not restart:
 - Check the VM's `<on_reboot>` setting via `virsh dumpxml $domainname` - it should be `restart`, not `destroy`.
 - If necessary, edit the setting via `virsh edit $domainname`
 - Crowbar node hangs at `Executing AutoYast script: /var/adm/autoinstall/init.d/crowbar_join`:
 - Find the IP address via the Crowbar web UI
 - ssh as `root` to that IP
 - Check the `/var/log/crowbar-join*` log files for errors
 - The Nova barclamp proposal fails to apply on a VM node:
 - Make sure you are not trying to run KVM within KVM. In the proposal, hypervisor should be set to `qemu`.
 - Browsing to the Chef web UI gives a `Tampered with cookie` error:
 - You probably have an old cookie in your browser from a previous Chef installation on the same IP. Remove the cookie and try again.
- OpenStack
 - Unable to connect to VM:
 - Check security groups.
 - Don't use YaST2 Firstboot or any EULA dialog.
 - Ensure network is set to DHCP.
 - Ensure suse-ami-tools is installed.
 - Slow VM performance?
 - Is your VM running on btrfs? This is not recommended, see http://www.linux-kvm.org/page/Tuning_KVM for more details.

Known issues

You can check bugzilla for [open issues with SUSE Cloud 1.0](#). In particular, check for [open issues in the Deployment component](#) which could affect the installation process.

Other known issues include the following:

- No 32-bit support; currently x86_64 architecture is required everywhere.
- [Crowbar is not yet FHS-compliant](#) due to use of the following paths:
 - `/tftpboot`
 - `/opt/dell/crowbar_framework/log`
- Cannot reuse existing HTTP install server.
- Removal of barclamps from a node do not necessarily shut down associated services or remove associated packages. This may have to be done manually.
- Crowbar is not yet always very good at reporting progress or explaining errors. See the "Debugging" section below.
- Sometimes Crowbar may report a node as `Ready` while it's actually rebooting. Applying a proposal to a node in this state will fail. Once the node is up again, click `Apply` on the failed proposal again to make it succeed.

Debugging

Crowbar and its components have a number of log files which can be checked. They are all listed below for completeness, but here are some suggestions for particular scenarios:

- If applying a barclamp proposal fails, you could check the Chef client logs on the node(s) affected by the proposal, and also the Crowbar web UI logs.

Log files

- On the Crowbar admin node:
 - Crowbar web UI: `/opt/dell/crowbar_framework/log/production.log`
 - Chef web UI: `/var/log/chef/webui.log`
 - Chef server: `/var/log/chef/server.log`
 - Chef expander: `/var/log/chef/expander.log`
 - Chef client (for the admin node only): `/var/log/chef/client.log`
 - Apache SOLR (Chef's search server): `/var/log/chef/solr.log`
 - HTTP (autoyast) install server for `provisioner` barclamp: `/var/log/apache2/provisioner-
{access,error}_log`
 - All the usual SUSE logs: `/var/log/messages`, `/var/log/zypper.log` etc.
 - syslogs for all Crowbar nodes: `/var/log/nodes/*.log` - these are collected via remote syslogging
 - Other Crowbar client node logs saved on admin node:
 - `/install-logs/h*.log` - Initial chef-client run on PXE-booted nodes prior to discovery by Crowbar.
 - `/opt/dell/crowbar_framework/log/d*.log` - Output from chef-client when proposals are applied to nodes. This is the first place to look if a barclamp proposal fails to apply.
- On all other Crowbar nodes:
 - Logs for when the node registers with the Crowbar admin node:
 - `/var/log/crowbar-join.errlog`
 - `/var/log/crowbar-join-$TOPIC.{log,err}` - STDOUT/STDERR from running commands associated with `$TOPIC` when the node joins the Crowbar cluster. `$TOPIC` can be:
 - `zypper` - package management activity
 - `ifup` - network configuration activity
 - `chef` - chef-client activity
 - `time` - starting of `ntp` client
 - Chef client log: `/var/log/chef/client.log`
 - All the usual SUSE logs: `/var/log/messages`, `/var/log/zypper.log` etc.
- On the Openstack controller node:
 - `/var/log/keystone/keystone.log` - OpenStack authentication etc.
 - `/var/log/rabbitmq/*` - logs for RabbitMQ, used by OpenStack for handling message queues
 - `/var/log/nova/` - various logs relating to Nova services:
 - `api.log`
 - `consoleauth.log`
 - `network.log`
 - `nova-manage.log`
 - `scheduler.log`
 - `volume.log`
- On Openstack compute nodes:
 - `/var/log/nova/` - various logs relating to Nova services:
 - `compute.log`
 - `nova-manage.log`

Who to contact for support

For this beta1 technical preview release:

- if you are internal to SUSE: please submit any issues to cloud@suse.de
- if you are a SUSE customer or partner: please submit any issues to cloud-beta@suse.de

Feedback is very welcome!

Glossary

Deployment Architecture

- **Node** -- A server which is managed by Crowbar.
- **Admin Node** -- Node which the Crowbar/Chef servers run on
- **Compute Node** -- a node which has an [OpenStack Compute \(Nova\)](#) Role.
- **Controller Node** -- Has the Nova-Controller/Keystone/... Role
 - Controller Nodes -- can be one or many (ie Keystone Controller, Swift-Proxy Controller, ...)

Crowbar UI & Chef Items

- **barclamp** -- A set of Chef cookbooks, templates and other necessary logic for applying a particular role to a node, or to some set of nodes.
- **proposal** -- Specific configuration for a barclamp, including barclamp-specific settings and the list of nodes to which the proposal should be applied.
- **role** -- An instance of a proposal that is active on a node

- **node** -- An instance of a proposal that is active on a node.
- **chef** -- an automated configuration management platform.
- **cookbook** -- A collection of chef recipes which deploy a software stack or technology. It is the unit of distribution for chef.
- **recipe** -- a group of chef scripts (written in Chef/Ruby) and templates used by chef to deploy a unit of functionality.

Generated from git revision 9342184 at Fri Jun 1 14:04:06 CEST 2012