CentOS 7 and Chef

CentOS 7 is centrally supported at SLAC for the following platforms:

- VMware virtual machines
- Bare metal server with devctl for remote console (IPMI / BMC)

For desktops or laptops, Ubuntu LTS is the supported choice.

Although RHEL 7 is also available if required by your application for support, CentOS 7 is preferred and recommended instead. Any instructions below for CentOS 7 also apply for RHEL 7.

Note: RHEL 8 and Rocky Linux 8 support will be available soon (in 2022).

Step-by-step guide

These are the steps to install and configure CentOS 7 with Chef at SLAC for a headless bare metal server.
To request a CentOS 7 virtual machine (VM) in VMware, please email unix-admin@slac.stanford.edu .

1. Install CentOS 7 using either the Minimal or the DVD ISO available here (available on the SLAC network or VPN). The ISO image can also be used for a USB key install.

   http://yum.slac.stanford.edu/iso/centos/

   N.B. some systems may have gpt labeled drives which enable larger than 2.2TB drives, these require an entry in the kickstart script like: part biosboot --fstype=biosboot --size=1

   Without this entry, the kickstart will halt telling you that you need to create a 1MB biosboot partition.

2. Log into your new CentOS 7 host.
   Become root by using sudo or /bin/su.
   Install Chef on bare metal or a VM by running this command (get a root prompt, or use sudo as shown below):

   ```
   curl -s http://yum.slac.stanford.edu/go-chef | sudo /bin/sh
   ```

   If you want to only configure yum, and not run any of the other Chef recipes, then don't run the above command, run this instead:

   ```
   curl -s http://yum.slac.stanford.edu/go-chef-yum-only | sudo /bin/sh
   ```

3. After you have run one of the above curl commands, you can optionally install the YFS client to get access to AFS. Do not install the YFS client unless you have to. Access to AFS is optional for CentOS 7 and it is not required for a centrally manged CentOS 7 host. SLAC is making an effort to not introduce additional dependencies on AFS. We do understand there are some current workflows which require AFS. The default SLAC CentOS 7 host will not have YFS installed, but it is available if you require it.

   You may need to run "yum upgrade" and then "reboot" before doing the following steps, if you installed an older version of CentOS 7 (eg, installed 7.0, when the current version is at 7.9)

   Use this command, after the above "go-chef" script completes:

   ```
   # /usr/bin/knife-node-add-role yfs-client
   ```

   Then run "chef-client" again:

   ```
   # chef-client
   ```

   The install of the YFS kernel module can take some time. The YFS client will start automatically. Future updates to the YFS kernel module will occur through yum. You will not automatically get an AFS token when logging in. Run the following command to get an afs token from your Kerberos ticket:

   ```
   $ aklog
   ```

   If you want to leave your home directory alone (ie, keep it on the local disk) then you are done. But if you want to have your AFS home directory as your home directory on this machine when you login, here are the steps to do that:

Edit this file: /etc/sssd/sssd.conf

comment out the line that says:
override_homedir = /home/%u
Run this command:
systemctl restart sssd

Create a symlink by running this command:
ln -s /afs/slac.stanford.edu/u /u

You should now have this symlink:
/u -> /afs/slac.stanford.edu/u

logout and login - and you should be in your AFS home directory, but you still need to run 'aklog' to get an AFS token after logging in.

> Note, if you decide to use AFS, then one should also set the following attribute "override_homedir=no" for your node so your edits to /etc/sssd/sssd.conf don't get overwritten with a chef run.
>
> "override_homedir=no" means don't change the setting in /etc/sssd/sssd.conf
>
> (Yes that value setting is bit odd, and we have it on the short-term list
>
> https://confluence.slac.stanford.edu/display/CHEF/Chef+short-term+todo+list
>
> to consider renaming.)
>
> The "override_homedir" attribute, and others, are describe at:
>
> https://confluence.slac.stanford.edu/pages/viewpage.action?pageId=232068309
>
> The above page also describes how to set that for the node.

4. Note, a Cheffed node by default does not limit login to the node, anyone at SLAC would be able to login to the node. If you want to limit login to the node please contact unix-admin@slac.stanford.edu with the name of the node and how you would like access to be restricted.
5. And still before you exit your root prompt, create a sudoers entry for yourself inside the /etc/sudoers.d directory.
   If you do not want or need sudo access, you can skip this step.

   You can copy and paste the following (replace 'ksa' with your username):
   cat > /etc/sudoers.d/user-ksa << EOF
   ksa ALL=ALL
   EOF

   Be sure to read and fill out the sudo request form. This is required for auditing purposes:
   https://www.slac.stanford.edu/comp/unix/auth/superuser-req.shtml

6. If you would like a Kerberos host keytab installed on your CentOS 7 host, send an email to unix-admin@slac.stanford.edu .

   UPDATE (2022-Jan): The installation of the CentoS/RHEL Kerberos keytab should be completely automated with chef-client. It can take up to 24 hours, but there should not be a need to email unix-admin anymore to request the key installation. If the automatic installation of the keytab does not work, please let unix-admin know.

   The subject line of the email to unix-admin for a host keytab request should be "please update whitelist for kerberos host keytab to include 'your_node_name_here'"

   e.g "just cheffed node, please update whitelist for kerberos host keytab to include lsst-aio02"

   Without a Kerberos host keytab, you will need to enter your SLAC password when connecting via ssh, even when you already have a Kerberos ticket granting ticket (TGT). If you have unix-admin install a Kerberos host keytab, then you can use passwordless GSSPAI via ssh to connect without a password when you already have a Kerberos TGT.

   automation of putting a keytab on the host, is part of the chef short-term goals (Chef short-term todo list) 'automate method of putting node on whitelist, or putting node in system.info with chef.lastrun data which auto keytab install could use to determine if keytab can be installed'

After you install Chef using the go-chef script, your CentOS 7 host will be configured for central authentication using Unix Kerberos.

In addition, here is an incomplete list of the configuration items that will be configured by Chef (just to give you an idea):

- cron

- logrotate
- rsyslog
- /etc/motd
- root password
- kerberos
- ssh
- shells
- sssd
- ntp
- yum
- yum-cron
- sudo for unix-admin
- login access for unix-admin

Scope of Support for CentOS 7 on the Desktop

Update (2022-Jan): CentOS 7 is no longer a supported choice for personal productivity desktops or laptops. SLAC IT offers full support for Ubuntu LTS on both the desktop and laptop. Please open a Service Now ticket for any assistance. Note, the "go-chef" script works on Ubuntu desktops. Use the "go-chef-laptop" script for laptops (the go-chef-laptop script is intended for roaming machines that move on and off the SLAC network).

CentOS 7 on the desktop should be thought of as a personal productivity machine, not a development or server. Development machines and servers can be hosted in virtual machines or bare metal machines in servers rooms. Virtualization platforms available include VMware, and (in the future) Amazon Web Services public cloud. AWS for SLAC use is currently being tested.

List of supported personal productivity applications. The following are the applications supported by the Help Desk IT Desktop Support (ITDS) team. These are standard RPM packages supported by Red Hat, or else standard supported applications (such as Outlook Web Access email web client).

Application Name	Description	RPM name(s)	Notes
Firefox	web browser	firefox	
LibreOffice	office suite	libreoffice, libreoffice-*	
Outlook Web Access	email client	N/A	https://email.slac.stanford.edu/owa/
SSH	ssh client	openssh-clients	ssh, scp, sftp
FastX	remote linux display	N/A	FastX

Graphics Card Support

CentOS 7 includes supported drivers for proprietary graphics cards such as nVidia and ATI. These supported drivers are included with each kernel update, so when you reboot into a new kernel, an updated graphics kernel module is available and your graphics will work.

ITDS specifically does not support graphics drivers that are not part of the standard operating system. If you want to replace the CentOS 7 support noveau driver with the proprietary Nvidia driver (for example), you are now responsible for any graphics configuration on your machine. ITDS is not responsible for supporting non-standard graphics drivers. When you replace the noveau driver with the Nvidia driver, special steps are required to verify the noveau driver gets blacklisted. Also, each kernel update will require you to rebuild the Nvidia kernel module. This is a non-standard configuration and is not covered under central support, because of the relationship between updated kernels and patching policy, the manual process of rebuilding the Nvidia kernel module with each kernel update, and the reboot policy. If you wish to install the Nvidia driver, you need to have a documented procedure in place regarding how often you update the kernel, when you reboot the kernel, and when you rebuild the Nvidia kernel module after you reboot into a new kernel.

Yum (RPM) Repositories

This is a list of the recommended yum repositories for CentOS 7 and RHEL 7. Some of these will be enabled by default, and others can be enabled if you require them.

CentOS	RHEL	Repository Name	Description	Part of Distribution	Recommendation Level	More information
	x	rhel-7-server-rpms	RHEL 7 Base	yes	high	
	x	rhel-7-server-extras-rpms	RHEL 7 Extra	yes	high	
	x	rhel-7-server-optional-rpms	RHEL 7 Optional	yes	high	
	x	rhel-7-server-rh-common-rpms	RHEL 7 Common	yes	high	

	x	rhel-7-server-supplementary-rpms	RHEL 7 Supplementary	yes	high	
	x	rhel-7-server-thirdparty-oracle-java-rpms	RHEL 7 Oracle Java	yes	high	
	x	rhel-server-rhscl-7-rpms	Software Collections, Developer Toolset	yes	high	http://developers.redhat.com/products/softwarecollections/overview/
x		base	CentOS-7 - Base	yes	high	
x		extras	CentOS-7 - Extras	yes	high	
x		updates	CentOS-7 - Updates	yes	high	
x	x	epel	Extra Packages for Enterprise Linux	no	medium	https://fedoraproject.org/wiki/EPEL
x	x	ius	IUS Community Packages for Enterprise Linux 7	no	medium	https://ius.io/
x	x	nux-dextop-release	Nux.Ro RPMs for general desktop use	no	medium	http://li.nux.ro/repos.html

We do **not** recommend these repositories: ATrpms, RPMForge, RepoForge. Those repositories do not play well with RHEL or CentOS. You can easily break your system due to distribution RPMs being replaced by the third party RPMs, and therefore causing rpm dependency problems that prevent routine security patches from being applied. If you need RPMs or software that you cannot find in the recommended repositories above, email unix-admin@slac.stanford.edu for advice.

Frequently Asked Questions:

Question	Answer
Why does ssh prompt me for a password?	If you don't have a Kerberos host keytab, password-less ssh will not work. Send a request to unix-admin (with your hostname) to install a Kerberos host keytab.
Where is /nfs?	Client NFS access is on our to-do list. We have switched from NIS to LDAP, and the automounter maps are not in LDAP yet. In the mean time, you can use scp (or possibly git). The rhel7.slac.stanford.edu login host was installed and configured before we started using Chef, and it is using NIS with NFS client access, but it will eventually be reinstalled and configured using Chef once we have client NFS support in Chef.
Where is /afs?	OpenAFS will be an option in CentOS 7, but not a requirement. We are currently developing a Chef cookbook to automatically install and configure OpenAFS. If you need /afs before the cookbook is ready, you can send a request to unix-admin and we can install and configure it manually. The rhel7.slac.stanford.edu login host has /afs installed and configured.
How do I get an AFS token?	Run the command 'aklog'. Then run the command 'tokens' to view your token. Then cd to /afs/slac/... to access afs space.
What is the difference between CentOS 7 and RHEL 7?	CentOS announced the official joining with Red Hat in January 2014. Although independent from Red Hat Enterprise Linux, the joining of CentOS and Red Hat strengthens the CentOS community and facilitates the CentOS build process since Red Hat is directly involved in supporting it. Scientific Computing Services (SCS) can offer a centrally managed CentOS 7 OS distribution because of the flexibility of the Chef configuration management tool. This provides SLAC the choice to pay for vendor support where required and appropriate, and also leverage the High Energy Physics Unix Information Exchange (HEPiX, https://www.hepix.org) and CentOS community for many use cases. SLAC has benefited from Red Hat Enterprise Linux (RHEL) vendor support since 2004 starting with RHEL 3. SLAC will continue to leverage vendor support from Red Hat, however it will be beneficial to for SCS to manage CentOS 7, and only use RHEL 7 where appropriate (ERP business systems and IBM GPFS servers, for example).
How do I install a machine that does not have a CD drive?	You can install using a USB thumb drive. See https://wiki.centos.org/HowTos/InstallFromUSBkey If you have a server that has a connection to SLAC's out of band devctl (Device Control) subnet, then SCS can PXE boot your server and install it over the network.
Grub2	Centos7 and RHEL7 use grub2 which don't do the automatic setup of console as grub legacy did.

Please send any questions to unix-admin@slac.stanford.edu