



Control Center Installation Guide

Release 1.2.0

Zenoss, Inc.

www.zenoss.com

Control Center Installation Guide

Copyright © 2016 Zenoss, Inc. All rights reserved.

Zenoss and the Zenoss logo are trademarks or registered trademarks of Zenoss, Inc., in the United States and other countries. All other trademarks, logos, and service marks are the property of Zenoss or other third parties. Use of these marks is prohibited without the express written consent of Zenoss, Inc., or the third-party owner.

Linux is a registered trademark of Linus Torvalds.

All other companies and products mentioned are trademarks and property of their respective owners.

Part Number: 1321.16.296

Zenoss, Inc.
11305 Four Points Drive
Bldg 1 - Suite 300
Austin, Texas 78726

Contents

About this guide.....	5
Chapter 1: Installing a master host.....	6
Verifying candidate host resources.....	6
Master host storage requirements.....	8
Disabling consistent network device naming.....	10
Preparing the master host operating system.....	11
Installing Docker Engine.....	13
Installing Control Center.....	13
Configuring Docker Engine.....	15
Optional: Loading image files.....	17
Creating the application data thin pool.....	18
Chapter 2: Configuring and starting the master host.....	19
Control Center maintenance scripts on the master host.....	19
User access control.....	19
Configuring the base size device for tenant data storage.....	21
Setting the host role to master.....	22
Optional: Configuring offline use.....	23
Master host configuration variables.....	23
Universal configuration variables.....	27
Starting Control Center for the first time.....	28
Adding the master host to a resource pool.....	29
Chapter 3: Installing delegate hosts.....	30
Verifying candidate host resources.....	30
Delegate host storage requirements.....	32
Disabling consistent network device naming.....	32
Preparing a delegate host.....	33
Installing Docker Engine.....	35
Installing Control Center.....	36
Configuring Docker.....	36
Chapter 4: Configuring and starting delegate hosts.....	39
Control Center maintenance scripts on delegate hosts.....	39
Enabling use of the command-line interface.....	39
Setting the host role to delegate.....	40
Setting internal services endpoints.....	40
Optional: Configuring offline use.....	41
Delegate host configuration variables.....	42
Universal configuration variables.....	44
Starting Control Center.....	45
Delegate host authentication.....	45
Chapter 5: Configuring a ZooKeeper ensemble.....	48

ZooKeeper and Control Center.....	48
Understanding the configuration process.....	48
Configuring the master host as a ZooKeeper node.....	50
Configuring delegate host A as a ZooKeeper node.....	51
Configuring delegate host B as a ZooKeeper node.....	53
Starting a ZooKeeper ensemble.....	55
Updating delegate hosts.....	55
 Appendix A: Starting and stopping Control Center deployments.....	57
Stopping Control Center (single-host deployment).....	57
Starting Control Center (single-host deployment).....	58
Stopping Control Center (multi-host deployment).....	58
Starting Control Center (multi-host deployment).....	62
 Appendix B: Storage management utility.....	64
serviced-storage.....	64
 Appendix C: Control Center configuration variables.....	68
Best practices for configuration files.....	68
Control Center configuration file.....	68
 Appendix D: Preparing to install without internet access.....	78
Downloading repository and image files.....	78
Installing the repository mirror.....	79
Staging Docker image archive files.....	79
 Appendix E: Configuring a private master NTP server.....	80
Configuring an NTP master server.....	80
Configuring NTP clients.....	81

About this guide

Control Center Installation Guide provides detailed procedures for installing and configuring a Control Center cluster. Please review the *Control Center Planning Guide* carefully before using this guide.

Related publications

Title	Description
<i>Control Center Planning Guide</i>	Provides both general and specific information about preparing to deploy a Control Center cluster.
<i>Control Center Installation Guide</i>	Provides detailed procedures for installing and configuring a Control Center cluster.
<i>Control Center Reference Guide</i>	Provides information and procedures for managing Control Center. This information is also available as online help in the Control Center browser interface.
<i>Control Center Release Notes</i>	Describes known issues, fixed issues, and late-breaking information not included in other publications.

Documentation feedback

To provide feedback about this document, or to report an error or omission, please send an email to docs@controlcenter.io. In the email, please include the document title and part number, and as much information as possible about the context of your feedback. The part number appears at the end of the list of trademarks, at the front of this guide.

Supported clients and browsers

The following table identifies the client operating systems and web browser combinations supported in this release.

Client OS	Supported Browsers
Windows 7 and 8.1	Internet Explorer 11 (enterprise mode is supported, but compatibility mode is not)
	Internet Explorer 10 (compatibility mode not supported)
	Firefox 30 and above
	Chrome 30 and above
Windows Server 2012 R2	Firefox 30
	Chrome 36
Macintosh OS/X 10.9	Firefox 30 and above
	Chrome 36 and above
Ubuntu 14.04 LTS	Firefox 30 and above
	Chrome 37 and above
Red Hat Enterprise Linux 6.5, CentOS 6.5	Firefox 30 and above
	Chrome 37 and above

1

Installing a master host

This chapter describes how to install Control Center on a Red Hat Enterprise Linux (RHEL) or CentOS 7.1 or 7.2 host. The candidate host must have the CPU, RAM, and storage resources required to serve as the master host in a Control Center cluster.

For more information about master host requirements, refer to the *Control Center Planning Guide*.

Verifying candidate host resources

Use this procedure to determine whether the hardware resources and installed operating system of a host are sufficient to serve as a Control Center master host.

- 1 Log in to the candidate host as `root`, or as a user with superuser privileges.
- 2 Verify that the host implements the 64-bit version of the x86 instruction set.

```
uname -m
```

- If the output is `x86_64`, the architecture is 64-bit. Proceed to the next step
 - If the output is `i386/i486/i586/i686`, the architecture is 32-bit. Stop this procedure and select a different host.
- 3 Determine whether the CPU resources are sufficient.
 - a Display the total number of CPU cores.

```
cat /proc/cpuinfo | grep -Ec '^core id'
```

- b Compare the available resources with the requirements for a Control Center master host.

For more information, refer to the *Control Center Planning Guide*.
- 4 Determine whether the CPU resources support the AES instruction set.

```
cat /proc/cpuinfo | grep -Ec '^flags.*aes'
```

For optimal performance, the result of the preceding commands must match the total number of CPU resources available on the host. If the result is 0, performance is severely degraded.

If the result is 0 and the candidate host is a virtual machine, the managing hypervisor may be configured in Hyper-V compatibility mode. Check the setting and disable it, if possible, or select a different host.

- 5 Determine whether the available memory and swap is sufficient.

- a Display the available memory.

```
free -h
```

- b Compare the available memory with the amount required for a master host in your deployment.

For more information, refer to the *Control Center Planning Guide*.

- 6 Ensure the host has a persistent numeric ID.

Skip this step if you are installing a single-host deployment.

Each host in a Control Center cluster must have a unique host ID, and the ID must be persistent (not change when the host reboots).

```
test -f /etc/hostid || genhostid
hostid
```

Record the ID for comparison with other hosts in the cluster.

- 7 Verify that name resolution works on this host.

```
hostname -i
```

If the result is not a valid IPv4 address, add an entry for the host to the network nameserver, or to `/etc/hosts`.

- 8 Add an entry to `/etc/hosts` for localhost, if necessary.

- a Determine whether `127.0.0.1` is mapped to localhost.

```
grep 127.0.0.1 /etc/hosts | grep localhost
```

If the preceding commands return no result, perform the following substep.

- b Add an entry to `/etc/hosts` for localhost.

```
echo "127.0.0.1 localhost" >> /etc/hosts
```

- 9 Update the operating system, if necessary.

- a Determine which release is installed.

```
cat /etc/redhat-release
```

If the result includes `7.0`, perform the following substeps.

- b Update the operating system and then restart the host.

The following commands require internet access or a local mirror of operating system packages.

```
yum makecache fast && yum update -y && reboot
```

- 10 Update the Linux kernel, if necessary.

- a Determine which kernel version is installed.

```
uname -r
```

If the result is lower than `3.10.0-327.22.2.el7.x86_64`, perform the following substeps.

- b Update the kernel or the operating system, and then restart the host.

The following commands require internet access or a local mirror of operating system packages.

Update only the kernel:

```
yum makecache fast && yum update -y kernel && reboot
```

Update the operating system, including the kernel:

```
yum makecache fast && yum update -y && reboot
```

Master host storage requirements

This section provides a quick reference for the minimum storage requirements of a Control Center master host. These requirements are in addition to the storage required for the host's operating system. For more information, refer to the *Control Center Planning Guide*.

Control Center cluster hosts need either unformatted block storage devices or partitions, or free space in one or more LVM volume groups.

- Enter the following command to display information about block storage:

```
lsblk -ap --output=NAME,SIZE,TYPE,FSTYPE,MOUNTPOINT
```

- Enter the following command to display information about LVM volume groups:

```
vgdisplay
```

Compare the output with the information in the following table.

Purpose	Minimum size	Description
Docker data	50GB (required)	Local, high-performance storage.
Control Center internal services data	50GB (required)	Local, high-performance storage formatted as an XFS filesystem.
Application data	200GB (suggested)	Local, high-performance storage.
Application data backups	150GB (suggested)	A remote file server compatible with XFS or a local storage formatted as an XFS filesystem. If the storage is local, ensure that it does not cause contention with the storage for Control Center internal services.

The storage for Docker data and application data is configured as LVM thin pools in subsequent procedures.

The suggested minimum sizes for application data and application data backups should be replaced with sizes that meet your application requirements. To calculate the appropriate sizes for these storage areas, use the following guidelines:

- Application data storage includes space for both data and snapshots. The default base size for data is 100GB, and the recommended space for snapshots is 100% of the base size. Adding the two yields the suggested minimum size of 200GB.
- For application data backups, the recommended space is 150% of the base size for data.

The following sections provide procedures for formatting and mounting local storage as XFS filesystems for Control Center internal services data and application data backups.

Creating a filesystem for Control Center internal services

This procedure requires one unused device or partition.

Use this procedure to create an XFS filesystem on an unused device or partition.

- 1 Log in to the target host as `root`, or as a user with superuser privileges.
- 2 Identify the target device or partition for the filesystem to create.

```
lsblk -ap --output=NAME,SIZE,TYPE,FSTYPE,MOUNTPOINT
```

- 3 Create an XFS filesystem.
Replace *Storage* with the path of the target device or partition:

```
mkfs.xfs Storage
```

- 4 Enter the following command to add an entry to the `/etc/fstab` file.
Replace *Storage* with the path of the device or partition used in the previous step:

```
echo "Storage /opt/serviced/var/iscvs xfs defaults 0 0" >> /etc/fstab
```

- 5 Create the mount point for internal services data.

```
mkdir -p /opt/serviced/var/iscvs
```

- 6 Mount the filesystem, and then verify it mounted correctly.

```
mount -a && mount | grep iscvs
```

Example result:

```
/dev/xvdb1 on /opt/serviced/var/iscvs type xfs
(rw,relatime,attr2,inode64,noquota)
```

Creating a filesystem for application data backups

This procedure requires one unused device or partition, or a remote file server that is compatible with XFS.

Use this procedure create an XFS filesystem on a device or partition, or to mount a remote filesystem, for application data backups.

Note If you are using a partition on a local device for backups, ensure that the storage for Control Center internal services data is not on the same device.

- 1 Log in to the target host as `root`, or as a user with superuser privileges.
- 2 Optional: Identify the target device or partition for the filesystem to create, if necessary.
Skip this step if you are using a remote file server.

```
lsblk -ap --output=NAME,SIZE,TYPE,FSTYPE,MOUNTPOINT
```

- 3 Optional: Create an XFS filesystem, if necessary.
Skip this step if you are using a remote file server.
Replace *Storage* with the path of the target device or partition:

```
mkfs.xfs Storage
```

- 4 Create an entry in the `/etc/fstab` file.

Replace *File-System-Specification* with one of the following values:

- the path of the device or partition used in the previous step

- the remote server specification

```
echo "File-System-Specification \
/opt/serviced/var/backups xfs defaults 0 0" >> /etc/fstab
```

- 5 Create the mount point for backup data.

```
mkdir -p /opt/serviced/var/backups
```

- 6 Mount the filesystem, and then verify it mounted correctly.

```
mount -a && mount | grep backups
```

Example result:

```
/dev/sdb3 on /opt/serviced/var/backups type xfs
(rw,relatime,seclabel,attr2,inode64,noquota)
```

Disabling consistent network device naming

The consistent network device naming feature can create device names that are too long for use with virtual IPs. This step disables the feature so that all network device names are `eth` followed by an integer.

- 1 Log in as `root`, or as a user with superuser privileges.
- 2 Edit the GRUB 2 general settings file.

- a Create a backup copy of the settings file.

```
cp /etc/default/grub /etc/default/grub.bak
```

- b Open `/etc/default/grub` with a text editor.

- c Add kernel boot arguments to the value of the `GRUB_CMDLINE_LINUX` variable.

The arguments to add are `biosdevname=0` and `net.ifnames=0`. Make sure the arguments are between the delimiter characters (`"`).

- d Save the file, and then close the text editor.

- 3 Determine whether the host is configured for UEFI or legacy boot mode.

```
find /boot -maxdepth 1 -type d
```

- If the output includes `/boot/efi`, the host is configured for UEFI boot mode.
- If the output does not include `/boot/efi`, the host is configured for legacy boot mode.

- 4 Recreate the GRUB 2 boot configuration file.

For UEFI boot mode:

```
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

For legacy boot mode:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- 5 Create an override for the default rules policy of the dynamic device management daemon.

```
ln -s /dev/null /etc/udev/rules.d/80-net-name-slot.rules
```

- 6 Change network device configurations.

- a Change directory to `/etc/sysconfig/network-scripts`.

```
cd /etc/sysconfig/network-scripts
```

- b List the network device configuration files.

```
ls ifcfg-* | grep -v ifcfg-lo
```

The `ifcfg-lo` file is excluded because it does not need to be changed.

- c Rename and edit device files.

For example, if you have a device file named `ifcfg-enol6777736`, use the `mv` command rename it to `ifcfg-eth0`, and then change the values of the *NAME* and *DEVICE* variables inside the file to `eth0`.

- 7 Reboot the host.

Preparing the master host operating system

Note **Zenoss customers:** If you are creating a deployment without internet access, perform the steps in [Preparing to install without internet access](#) on page 78, before performing this procedure.

Use this procedure to prepare a RHEL/CentOS 7.1 or 7.2 host as a Control Center master host.

- 1 Log in to the candidate master host as `root`, or as a user with superuser privileges.
- 2 Disable the firewall, if necessary.

This step is required for installation but not for deployment. For more information, refer to the *Control Center Planning Guide*.

- a Determine whether the `firewalld` service is enabled.

```
systemctl status firewalld.service
```

- If the result includes `Active: inactive (dead)`, the service is disabled. Proceed to the next step.
- If the result includes `Active: active (running)`, the service is enabled. Perform the following substep.

- b Disable the `firewalld` service.

```
systemctl stop firewalld && systemctl disable firewalld
```

On success, the preceding commands display messages similar to the following example:

```
rm '/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service'
rm '/etc/systemd/system/basic.target.wants/firewalld.service'
```

- 3 Optional: Enable persistent storage for log files, if desired.

By default, RHEL/CentOS systems store log data only in memory or in a ring buffer in the `/run/log/journal` directory. By performing this step, log data persists and can be saved indefinitely, if you implement log file rotation practices. For more information, refer to your operating system documentation.

```
mkdir -p /var/log/journal && systemctl restart systemd-journald
```

- 4 Disable Security-Enhanced Linux (SELinux), if installed.

- a Determine whether SELinux is installed.

```
test -f /etc/selinux/config && grep '^SELINUX=' /etc/selinux/config
```

If the preceding commands return a result, SELinux is installed.

- b Set the operating mode to disabled.
Open `/etc/selinux/config` in a text editor, and change the value of the `SELINUX` variable to `disabled`.
- c Confirm the new setting.

```
grep '^SELINUX=' /etc/selinux/config
```

- 5 Enable and start the Dnsmasq package.

The package facilitates networking among Docker containers.

```
systemctl enable dnsmasq && systemctl start dnsmasq
```

- 6 Install and configure the NTP package.

Note This procedure assumes the host has internet access. To install and configure NTP on a host that does not have internet access, see [Configuring a private master NTP server](#) on page 80.

- a Install the package.

```
yum install -y ntp
```

- b Set the system time.

```
ntpd -gq
```

- c Enable the `ntpd` daemon.

```
systemctl enable ntpd
```

- d Configure `ntpd` to start when the system starts.

Currently, an unresolved issue associated with NTP prevents `ntpd` from restarting correctly after a reboot. The following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local  
chmod +x /etc/rc.d/rc.local
```

- 7 Add the Zenoss repositories to the host's repository list.

- a Install the repository package.

The package adds the Zenoss stable, unstable, and testing repositories to `/etc/yum.repos.d`. All three repositories are disabled.

```
rpm -ivh http://get.zenoss.io/yum/zenoss-repo-1-1.x86_64.rpm
```

- b Clean out the yum cache directory.

```
yum clean all
```

- 8 Reboot the host.

```
reboot
```

Installing Docker Engine

Use one of the procedures in this section to install Docker Engine.

Installing Docker Engine with internet access

Use this procedure to install Docker Engine on a host that has internet access.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Install Docker Engine 1.12.1, and then disable accidental upgrades.
 - a Add the Docker repository to the host's repository list.

```
cat <<EOF > /etc/yum.repos.d/docker.repo
[dockerrepo]
name=Docker Repository
baseurl=https://yum.dockerproject.org/repo/main/centos/7/
enabled=1
gpgcheck=1
gpgkey=https://yum.dockerproject.org/gpg
EOF
```

- b Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- c Install Docker Engine from the remote repository.

```
yum install -y docker-engine-1.12.1
```

- d Open `/etc/yum.repos.d/docker.repo` with a text editor.
 - e Change the value of the `enabled` key from 1 to 0.
 - f Save the file, and then close the text editor.

Optional: Installing Docker Engine without internet access

Zenoss customers: If you are installing Docker Engine without internet access, perform the steps in [Preparing to install without internet access](#) on page 78 before performing this procedure.

Use this procedure to install Docker Engine on a host that does not have internet access.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Install Docker Engine 1.12.1 from the local repository mirror.
 - a Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- b Install Docker Engine.

```
yum install --enablerepo=zenoss-mirror -y docker-engine-1.12.1
```

Installing Control Center

Use one of the procedures in this section to install Control Center.

Installing Control Center with internet access

Use this procedure to install Control Center on a host that has internet access.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Install Control Center 1.2.0.
 - a Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- b Install Control Center from the remote repository.

```
yum --enablerepo=zenoss-stable install -y serviced-1.2.0
```

- 3 Make a backup copy of the Control Center configuration file.

- a Make a copy of `/etc/default/serviced`.

```
cp /etc/default/serviced /etc/default/serviced-1.2.0-orig
```

- b Set the backup file permissions to read-only.

```
chmod 0440 /etc/default/serviced-1.2.0-orig
```

- 4 Add a drop-in file for the NFS service.

This step is a workaround for an [an unresolved issue](#).

- a Create a directory for the drop-in file.

```
mkdir -p /etc/systemd/system/nfs-server.service.d
```

- b Create the drop-in file.

```
cat <<EOF > /etc/systemd/system/nfs-server.service.d/nfs-server.conf
[Unit]
Requires=
Requires= network.target proc-fs-nfsd.mount rpcbind.service
Requires= nfs-mountd.service
EOF
```

- c Reload the systemd manager configuration.

```
systemctl daemon-reload
```

Optional: Installing Control Center without internet access

Zenoss customers: Perform the steps in [Preparing to install without internet access](#) on page 78 before performing this procedure.

Use this procedure to install Control Center on a host that does not have internet access.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Install Control Center 1.2.0 from the local repository mirror.
 - a Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- b** Install Control Center.

```
yum install --enablerepo=zenoss-mirror -y serviced-1.2.0
```

- 3** Make a backup copy of the Control Center configuration file.

- a** Make a copy of `/etc/default/serviced`.

```
cp /etc/default/serviced /etc/default/serviced-1.2.0-orig
```

- b** Set the backup file permissions to read-only.

```
chmod 0440 /etc/default/serviced-1.2.0-orig
```

- 4** Add a drop-in file for the NFS service.

This step is a workaround for an [an unresolved issue](#).

- a** Create a directory for the drop-in file.

```
mkdir -p /etc/systemd/system/nfs-server.service.d
```

- b** Create the drop-in file.

```
cat <<EOF > /etc/systemd/system/nfs-server.service.d/nfs-server.conf
[Unit]
Requires=
Requires= network.target proc-fs-nfsd.mount rpcbind.service
Requires= nfs-mountd.service
EOF
```

- c** Reload the systemd manager configuration.

```
systemctl daemon-reload
```

Configuring Docker Engine

Use this procedure to configure Docker Engine.

- 1** Log in to the master host as `root`, or as a user with superuser privileges.
- 2** Create a symbolic link for the Docker temporary directory.

Docker uses its temporary directory to spool images. The default directory is `/var/lib/docker/tmp`. The following command specifies the same directory that Control Center uses, `/tmp`. You can specify any directory that has a minimum of 10GB of unused space.

- a** Create the `docker` directory in `/var/lib`.

```
mkdir /var/lib/docker
```

- b** Create the link to `/tmp`.

```
ln -s /tmp /var/lib/docker/tmp
```

- 3** Create a systemd drop-in file for Docker Engine.

- a** Create the override directory.

```
mkdir -p /etc/systemd/system/docker.service.d
```

- b** Create the unit drop-in file.

```
cat <<EOF > /etc/systemd/system/docker.service.d/docker.conf
[Service]
TimeoutSec=300
EnvironmentFile=-/etc/sysconfig/docker
ExecStart=
ExecStart=/usr/bin/dockerd \${OPTIONS}
TasksMax=infinity
EOF
```

- c** Reload the systemd manager configuration.

```
systemctl daemon-reload
```

- 4** Create an LVM thin pool for Docker data.

For more information about the `serviced-storage` command, see [serviced-storage](#) on page 64.

Replace *Storage* with the paths of one or more block devices or partitions, or the name of an LVM volume group:

```
serviced-storage create-thin-pool --size=50G docker Storage
```

On success, the result is the device mapper name of the thin pool, which always starts with `/dev/mapper.`

- 5** Configure and start the Docker service.

- a** Create a variable for the name of the Docker thin pool.

Replace *Thin-Pool-Device* with the name of the thin pool device created in the previous step:

```
myPool="Thin-Pool-Device"
```

- b** Create a variable for the IPv4 address of the master host.

Replace *Master-Host* with the hostname or IPv4 address of the master host:

```
masterIP="Master-Host"
```

- c** Create variables for adding arguments to the Docker configuration file. The `--exec-opt` argument is a workaround for [a Docker issue](#) on RHEL/CentOS 7.x systems.

```
myDriver="--storage-driver devicemapper"
myLog="--log-level=error"
myFix="--exec-opt native.cgroupdriver=cgroupfs"
myMount="--storage-opt dm.mountopt=discard"
myFlag="--storage-opt dm.thinpooldev=$myPool"
myReg="--insecure-registry=$masterIP:5000"
```

- d** Add the arguments to the Docker configuration file.

```
echo 'OPTIONS="'$myLog $myDriver $myFix $myMount $myFlag $myReg'"' \
>> /etc/sysconfig/docker
```

- e** Start or restart Docker.

```
systemctl restart docker
```

The startup may take up to a minute, and may fail. If startup fails, repeat the `restart` command.

- 6** Configure name resolution in containers.

Each time it starts, `docker` selects an IPv4 subnet for its virtual Ethernet bridge. The selection can change; this step ensures consistency.

- a Identify the IPv4 subnet and netmask `docker` has selected for its virtual Ethernet bridge.

```
ip addr show docker0 | grep inet
```

- b Open `/etc/sysconfig/docker` in a text editor.
- c Add the following flags to the end of the *OPTIONS* declaration.

Replace *Bridge-Subnet* with the IPv4 subnet `docker` selected for its virtual bridge:

```
--dns=Bridge-Subnet --bip=Bridge-Subnet/16
```

For example, if the bridge subnet is 172.17.0.1, add the following flags:

```
--dns=172.17.0.1 --bip=172.17.0.1/16
```

Note Use a space character () to separate flags, and make sure the double quote character (") delimits the declaration of *OPTIONS*.

- d Restart the Docker service.

```
systemctl restart docker
```

Optional: Loading image files

Zenoss customers: Perform the steps in [Preparing to install without internet access](#) on page 78 before performing this procedure.

Use this procedure to load images into the local repository on a host that does not have internet access.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Change directory to `/root`.

```
cd /root
```

- 3 Extract the images.

```
for image in install-*.run
do
echo -n "$image: "
eval ./ $image
done
```

Image extraction begins when you press the **y** key. If you press the **y** key and then **Return** key, the current image is extracted, but the next one is not.

- 4 List the images in the registry.

```
docker images
```

The result should show one image for each archive file.

- 5 Optional: Delete the archive files, if desired.

```
rm -i ./install-*.run
```

Creating the application data thin pool

Use this procedure to create a thin pool for application data storage.

The following Control Center configuration variables are used to specify application data thin pools:

SERVICED_FS_TYPE

Default: `devicemapper`

The driver to manage application data storage on the `serviced` master host. Only `devicemapper` is supported in production deployments.

The only supported storage layout for the `devicemapper` driver is an LVM thin pool. To create a thin pool, use the `serviced-storage` utility. To specify the name of the thin pool device, use the `SERVICED_DM_THINPOOLDEV` variable.

SERVICED_DM_THINPOOLDEV

Default: (none)

The name of the thin pool device to use with the `devicemapper` storage driver.

Note This procedure does not include a specific value for the size of the thin pool. For more information about sizing this resource, refer to the documentation for your application. Or, use the suggested minimum value, 200GB. You can add storage to an LVM thin pool at any time.

Perform these steps:

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Create an LVM thin pool for application data.

For more information about the `serviced-storage` command, see [serviced-storage](#) on page 64.

Replace *Value* with the fixed or relative amount of space to use for the thin pool; and replace *Storage* with the paths of one or more block devices or partitions, or the name of an LVM volume group:

```
serviced-storage create-thin-pool --size=Value serviced Storage
```

On success, the result is the device mapper name of the thin pool, which always starts with `/dev/mapper`. Record the name for use in the next step.

- 3 Edit storage variables in the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Locate the line for the `SERVICED_FS_TYPE` variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (`#`) from the beginning of the line.
 - d Add `SERVICED_DM_THINPOOLDEV` immediately after `SERVICED_FS_TYPE`, and set its value. Replace *Thin-Pool-Name* with the device mapper name of the thin pool for application data:

```
SERVICED_DM_THINPOOLDEV=Thin-Pool-Name
```

- e Save the file, and then close the editor.

Proceed to the next chapter and configure the host.

2

Configuring and starting the master host

This chapter includes the procedures for configuring Control Center on the master host, describes the configuration options that apply to the master host, and includes steps for starting the master host for the first time. Perform the procedures in this chapter before installing Control Center on delegate hosts.

Many configuration choices depend on application requirements. Please review your application documentation before configuring Control Center on the master host.

This chapter includes synopses of the configuration variables that affect the master host. For more information about a variable, see [Control Center configuration variables](#) on page 68.

Control Center maintenance scripts on the master host

The scripts in the following list are installed when Control Center is installed, and are started either daily or weekly by `anacron`.

`/etc/cron.daily/serviced`

This script invokes `logrotate` daily, to manage the `/var/log/serviced.access.log` file.

This script is required on the master host and on all delegate hosts.

`/etc/cron.weekly/serviced-fstrim`

This script invokes `fstrim` weekly, to reclaim unused blocks in the application data thin pool.

The life span of a solid-state drive (SSD) degrades when `fstrim` is run too frequently. If the block storage of the application data thin pool is an SSD, you can reduce the frequency at which this script is invoked, as long as the thin pool never runs out of free space. An identical copy of this script is located in `/opt/serviced/bin`.

This script is required on the master host only.

`/etc/cron.weekly/serviced-zenosssdbpack`

This script invokes a `serviced` command weekly, which in turn invokes the database maintenance script for a Zenoss application. If the application is not installed or is offline, the command fails.

This script is required on the master host only.

User access control

Control Center provides a browser interface and a command-line interface.

To gain access to the Control Center browser interface, users must have login accounts on the Control Center master host. In addition, users must be members of the Control Center administrative group, which by default is

the system group, `wheel`. To enhance security, you may change the administrative group from `wheel` to any non-system group.

To use the Control Center command-line interface (CLI) on a Control Center cluster host, a user must have login account on the host, and the account must be a member of the `docker` group. Members of the `wheel` group, including `root`, are members of the `docker` group.

Pluggable Authentication Modules (PAM) is supported and recommended for enabling access to both the browser interface and the command-line interface.

Adding users to the default administrative group

Use this procedure to add users to the default administrative group of Control Center, `wheel`. Performing this procedure enables users to gain access to the Control Center browser interface.

Note Perform this procedure or the next procedure, but not both.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Add a user to the system group.

Replace *User* with the name of a login account on the master host.

```
usermod -aG wheel User
```

Repeat the preceding command for each user to add.

Configuring a regular group as the Control Center administrative group

Use this procedure to change the default administrative group of Control Center from `wheel` to a non-system group.

The following Control Center variables are used in this procedure:

SERVICED_ADMIN_GROUP

Default: `wheel`

The name of the Linux group on the `serviced` master host whose members are authorized to use the `serviced` browser interface. You may replace the default group with a group that does not have superuser privileges.

SERVICED_ALLOW_ROOT_LOGIN

Default: `1` (true)

Determines whether the `root` user account on the `serviced` master host may be used to gain access to the `serviced` browser interface.

Note Perform this procedure or the previous procedure, but not both.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Create a variable for the group to designate as the administrative group.
In this example, the name of group to create is `serviced`. You may choose any name or use an existing group.

```
GROUP=serviced
```

- 3 Create a new group, if necessary.

```
groupadd $GROUP
```

- 4 Add one or more existing users to the new administrative group.

Replace *User* with the name of a login account on the host:

```
usermod -aG $GROUP User
```

Repeat the preceding command for each user to add.

- 5 Specify the new administrative group in the `serviced` configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Locate the line for the `SERVICED_ADMIN_GROUP` variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (`#`) from the beginning of the line.
 - d Change the value from `wheel` to the name of the group you chose earlier.
 - e Save the file, and then close the editor.
- 6 Optional: Prevent the `root` user from gaining access to the Control Center browser interface, if desired.
 - a Open `/etc/default/serviced` in a text editor.
 - b Locate the line for the `SERVICED_ALLOW_ROOT_LOGIN` variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (`#`) from the beginning of the line.
 - d Change the value from `1` to `0`.
 - e Save the file, and then close the editor.

Enabling use of the command-line interface

Use this procedure to enable a user to perform administrative tasks with the Control Center command-line interface.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Add a user to the `Docker` group.

Replace *User* with the name of a login account on the host.

```
usermod -aG docker User
```

Repeat the preceding command for each user to add.

Configuring the base size device for tenant data storage

Use this procedure to configure the base size of virtual storage devices for tenants in the application data thin pool. The base size is used each time a tenant device is created. In particular, the first time `serviced` starts, it creates the base size device and then creates a tenant device from the base size device.

The following Control Center configuration variable is used to specify the base size device:

`SERVICED_DM_BASESIZE`

Default: 100G

The base size of virtual storage devices for tenants in the application data thin pool, in gigabytes. The units symbol (G) is required. This variable is used when `serviced` starts for the first time, to set the initial size of tenant devices, and when a backup is restored, to set the size of the restored tenant device.

The base size device is sparse device that occupies at most 1MB of space in the application data thin pool; its size has no immediate practical impact. However, the application data thin pool should have enough space for twice the size of each tenant device it supports, to store both the data itself and snapshots of the data. Since the application data thin pool is an LVM logical volume, its size can be increased at any time.

Likewise, the size of a tenant device can be increased, as long as the available space in the thin pool can support the larger tenant device plus snapshots.

Perform these steps:

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Identify the size of the thin pool for application data.

The size is required to set an accurate value for the `SERVICED_DM_BASESIZE` variable.

```
lvs --options=lv_name,lv_size | grep serviced-pool
```

- 3 Edit storage variables in the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Add `SERVICED_DM_BASESIZE` immediately after `SERVICED_DM_THINPOOLDEV`, and set its value.

Replace *Fifty-Percent* with the value that is less than or equal to 50% of the size of the thin pool for application data. Include the symbol for gigabytes, G:

```
SERVICED_DM_BASESIZE=Fifty-PercentG
```

- c Save the file, and then close the editor.
- 4 Verify the settings.

```
grep -E '^\\b*SERVICED' /etc/default/serviced
```

Setting the host role to master

Use this procedure to configure a host as the master host. The following configuration variable assigns the host role:

SERVICED_MASTER

Default: 1 (true)

Assigns the role of a `serviced` instance, either master or delegate. The master runs the application services scheduler and other internal services. Delegates run the application services assigned to the resource pool to which they belong.

Only one `serviced` instance can be the master; all other instances must be delegates. The default value assigns the master role. To assign the delegate role, set the value to 0 (false). This variable must be explicitly set on all Control Center cluster hosts.

Perform these steps:

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Edit the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Locate the line for the `SERVICED_MASTER` variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (#) from the beginning of the line.
 - d Save the file, and then close the editor.
- 3 Verify the settings.

```
grep -E '^\\b*SERVICED' /etc/default/serviced
```

Optional: Configuring offline use

Zenoss customers: If you are creating a deployment without internet access, perform this procedure.

Use this procedure to configure a host to operate without internet access. The following configuration variable informs `serviced` that internet access is not available:

SERVICED_OUTBOUND_IP

Default: (none)

The default startup routines of `serviced` include attempting to ping `google.com`. When a value is set for this variable, `serviced` does not attempt the ping and assumes it does not have internet access.

Use this variable to specify the IP address of a network interface other than the default, or to prevent `serviced` from assuming it has internet access.

Note Setting the Docker `HTTP_PROXY` or `HTTPS_PROXY` environment variables prevents access to the IP address defined with this variable. To enable access, unset the Docker variables, and then reboot the host.

Perform these steps:

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Identify the IPv4 address of the host.

```
hostname -i
```

- 3 Edit the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Locate the line for the `SERVICED_OUTBOUND_IP` variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (`#`) from the beginning of the line.
 - d Change the value to the IPv4 address identified in the previous step.
 - e Save the file, and then close the editor.
- 4 Verify the settings.

```
grep -E '^\b*SERVICED' /etc/default/serviced
```

Master host configuration variables

The tables in this section provide an overview of the `serviced` configuration variables that apply to the Control Center master host. Set these variables as required for your environment or applications.

Best practices for configuration files

The Control Center configuration file, `/etc/default/serviced`, contains Bash environment variables that are read by the `serviced` daemon startup script. The following list describes recommended best practices for its use and maintenance:

- 1 When in doubt, make a backup. Making a backup copy of the configuration file before editing it is always the safest choice.
- 2 Copy a variable, then edit the copy. If you need to revert a variable to its default value, you don't have to leave the file to look it up.
- 3 Put the first character of the variable declaration in the first column of its line. It's easier to `grep` for settings when each one starts a line.

- 4 Add customizations to the top of the file. Customizations at the end of the file or scattered throughout the file can be overlooked.

Storage variables

The variables in the following table are set only on the master host.

- Use one of the first two groups of variables but not both.
- The defaults of the third group may need to be changed before starting the master host for the first time.
- Typically, the defaults of the last two groups of variables are not changed until Control Center has managed an application for a while and a need arises.

The `SERVICED_STORAGE_STATS_UPDATE_INTERVAL` variable sets the interval for collecting kernel statistics about the application data thin pool. Its default value is unlikely to require a change until a need arises.

Variable	Description	Purpose
<code>SERVICED_FS_TYPE</code> <code>SERVICED_DM_ARGS</code> <code>SERVICED_DM_BASESIZE</code> <code>SERVICED_DM_THINPOOLDEV</code>	The specifications of a devicemapper-based application data storage resource for production use.	Provide basic information about the data storage resource.
<code>SERVICED_FS_TYPE</code> <code>SERVICED_DM_LOOPDATASIZE</code> <code>SERVICED_DM_LOOPMETADATASIZE</code> <code>SERVICED_ALLOW_LOOP_BACK</code>	The specifications of a devicemapper-based application data storage resource for development use.	Provide basic information about the data storage resource.
<code>SERVICED_ISVCS_PATH</code> <code>SERVICED_VOLUMES_PATH</code> <code>SERVICED_BACKUPS_PATH</code>	The data storage paths of separate functional components of Control Center internal services.	Enable separate storage areas for one or more components. The default installation process puts all three components on the same device.
<code>SERVICED_SNAPSHOT_TTL</code> <code>SERVICED_SNAPSHOT_USE_PERCENT</code> <code>SERVICED_MAX_DFS_TIMEOUT</code>	The snapshot retention interval, the percentage of the data storage thin pool that is unused, and the snapshot attempt timeout interval.	Prevent the creation of snapshots that are too large to fit the thin pool.
<code>SERVICED_LOGSTASH_MAX_DAYS</code> <code>SERVICED_LOGSTASH_MAX_SIZE</code> <code>SERVICED_LOGSTASH_CYCLE_TIME</code>	The variables that manage the amount of space used by the application log storage service.	Prevent application logs from filling the storage device that logstash uses.

Internal services endpoint variables

The variables in the following table must be set identically on all Control Center delegate hosts. On the master host, the default values of these variables do not need to be changed, unless the Docker registry is hosted on a system other than the master. In that case, `SERVICED_DOCKER_REGISTRY` must be set explicitly on the master host, too.

The `SERVICED_AUTH_TOKEN_EXPIRATION` variable affects RPC, mux, and internal services endpoint traffic.

Variable	Endpoint	Description
<i>SERVICED_DOCKER_REGISTRY</i>	<i>Master-Host</i> : 9100	The local Docker registry for Control Center internal services images and application images.
<i>SERVICED_ENDPOINT</i>	<i>Master-Host</i> : 4979	The serviced RPC server. The endpoint port number must match the value of <i>SERVICED_RPC_PORT</i> .
<i>SERVICED_LOG_ADDRESS</i>	<i>Master-Host</i> : 5042	The <i>logstash</i> service.
<i>SERVICED_LOGSTASH_ES</i>	<i>Master-Host</i> : 9100	The Elasticsearch service.
<i>SERVICED_STATS_PORT</i>	<i>Master-Host</i> : 8443	The serviced metrics consumer service.
<i>SERVICED_AUTH_TOKEN_EXPIRATION</i>	(none)	The length of time a delegate authentication token is valid.

RPC service variables

The variables in the following table must be set identically on all Control Center cluster hosts, except:

- *SERVICED_RPC_PORT*, set only on the master
- *SERVICED_MAX_RPC_CLIENTS*, set only on delegates

By default, *serviced* uses TLS to encrypt all RPC traffic. The *SERVICED_KEY_FILE* and *SERVICED_CERT_FILE* variables identify the digital certificate used for RPC, mux, and HTTP traffic.

The *SERVICED_AUTH_TOKEN_EXPIRATION* variable affects RPC, mux, and internal services endpoint traffic.

Variable	Where to set
<i>SERVICED_ENDPOINT</i>	Master, delegates
<i>SERVICED_MAX_RPC_CLIENTS</i>	Delegates
<i>SERVICED_RPC_PORT</i>	Master
<i>SERVICED_RPC_CERT_VERIFY</i>	Master, delegates
<i>SERVICED_RPC_DISABLE_TLS</i>	Master, delegates
<i>SERVICED_RPC_TLS_MIN_VERSION</i>	Master, delegates
<i>SERVICED_RPC_TLS_CIPHERS</i>	Master, delegates
<i>SERVICED_KEY_FILE</i>	Master
<i>SERVICED_CERT_FILE</i>	Master
<i>SERVICED_RPC_DIAL_TIMEOUT</i>	Master, delegates
<i>SERVICED_AUTH_TOKEN_EXPIRATION</i>	Master

Multiplexer variables

The variables in the following table must be set identically on all Control Center cluster hosts.

By default, `serviced` uses TLS to encrypt all mux traffic. The `SERVICED_KEY_FILE` and `SERVICED_CERT_FILE` variables identify the digital certificate used for RPC, mux, and HTTP traffic.

The `SERVICED_AUTH_TOKEN_EXPIRATION` variable affects RPC, mux, and internal services endpoint traffic.

Variable	Where to set
<code>SERVICED_MUX_PORT</code>	Master, delegates
<code>SERVICED_MUX_DISABLE_TLS</code>	Master, delegates
<code>SERVICED_MUX_TLS_MIN_VERSION</code>	Master, delegates
<code>SERVICED_MUX_TLS_CIPHERS</code>	Master, delegates
<code>SERVICED_KEY_FILE</code>	Master
<code>SERVICED_CERT_FILE</code>	Master
<code>SERVICED_AUTH_TOKEN_EXPIRATION</code>	Master

HTTP server variables

The variables in the following table are set only on the master host, except the `SERVICED_UI_PORT` variable, which must be set identically on all cluster hosts.

By default, `serviced` uses TLS to encrypt all HTTP traffic. The `SERVICED_KEY_FILE` and `SERVICED_CERT_FILE` variables identify the digital certificate used for RPC, mux, and HTTP traffic.

Variable	Description
<code>SERVICED_UI_PORT</code>	The port on which the HTTP server listens for requests.
<code>SERVICED_TLS_MIN_VERSION</code>	The minimum version of TLS that <code>serviced</code> accepts for HTTP traffic.
<code>SERVICED_TLS_CIPHERS</code>	The list TLS ciphers that <code>serviced</code> accepts for HTTP traffic.
<code>SERVICED_KEY_FILE</code>	The path of a digital certificate key file.
<code>SERVICED_CERT_FILE</code>	The path of a digital certificate file.

Browser interface variables (master host only)

The variables in the following table are set only on the master host.

Variable	Description
<code>SERVICED_UI_POLL_FREQUENCY</code>	The number of seconds between polls from browser interface clients.
<code>SERVICED_SVCSTATS_CACHE_TIMEOUT</code>	The number of seconds to cache statistics about services.
<code>SERVICED_ADMIN_GROUP</code>	The group on the master host whose members can use the browser interface.

Variable	Description
<i>SERVICED_ALLOW_ROOT_LOGIN</i>	Determines whether <code>root</code> on the master host can use the browser interface.

Tuning variables (master host only)

Variable	Description
<i>SERVICED_ES_STARTUP_TIMEOUT</i>	The number of seconds to wait for the Elasticsearch service to start.
<i>SERVICED_MASTER_POOLID</i>	The name of the default resource pool. This variable is only used the first time <code>serviced</code> is started.

Universal configuration variables

The tables in this section provide an overview of the `serviced` configuration variables that apply to all hosts in a Control Center cluster. Set these variables as required for your environment or applications.

Role variable

Variable	Description
<i>SERVICED_MASTER</i>	Assigns the role of a <code>serviced</code> instance, either master or delegate. The master runs the application services scheduler and other internal services. Delegates run the application services assigned to the resource pool to which they belong.

Browser interface variable (all hosts)

Variable	Description
<i>SERVICED_UI_PORT</i>	The port on which the HTTP server listens for requests.

Networking variables

Variable	Description
<i>SERVICED_STATIC_IPS</i>	A list of one or more static IP addresses for IP assignment.
<i>SERVICED_OUTBOUND_IP</i>	The IP address of the network interface for <code>serviced</code> to use. When this variable is not set, <code>serviced</code> uses the IP address of the default network interface and assumes it has internet access. To prevent <code>serviced</code> from assuming it has internet access, set this variable.
<i>SERVICED_VIRTUAL_ADDRESS_SUBNET</i>	The private network for containers that use virtual IP addresses. The default is <code>10.3.0.0/16</code> , and the network can be unique on each host. A <code>/29</code> network is sufficient.
<i>SERVICED_DOCKER_DNS</i>	A list of one or more DNS servers. The list is injected into all Docker Engine containers.

Debugging variables

Variable	Description
<i>SERVICED_LOG_LEVEL</i>	The log level <code>serviced</code> uses when writing to the system log.
<i>SERVICED_DEBUG_PORT</i>	The port on which <code>serviced</code> listens for HTTP requests for the Go profiler .
<i>SERVICED_DOCKER_LOG_DRIVER</i>	The log driver for all Docker container logs.
<i>SERVICED_DOCKER_LOG_CONFIG</i>	Docker <code>--log-opt</code> options.

Tuning variables (all cluster hosts)

Variable	Description
<i>GOMAXPROCS</i>	The maximum number of CPU cores that <code>serviced</code> uses.
<i>SERVICED_MAX_CONTAINER_AGE</i>	The number of seconds <code>serviced</code> waits before removing a stopped container.
<i>SERVICED_ISVCS_ENV_[0-9]+</i>	Startup arguments to pass to specific internal services.
<i>SERVICED_SERVICE_MIGRATION_TAG</i>	Overrides the default value for the service migration image.
<i>SERVICED_OPTS</i>	Startup arguments for <code>serviced</code> .
<i>SERVICED_CONTROLLER_BINARY</i>	The path of the <code>serviced-controller</code> binary.
<i>SERVICED_HOME</i>	The path of the home directory for <code>serviced</code> .
<i>SERVICED_ETC_PATH</i>	The path of the directory for <code>serviced</code> configuration files.
<i>SERVICED_VHOST_ALIASES</i>	A list of hostname aliases for a host; for example, <code>localhost</code> .

Starting Control Center for the first time

Use this procedure to start the Control Center service (`serviced`) on a master host after installing and configuring it. This procedure is valid for single-host and multi-host deployments, whether the deployment has internet access or not, and is only performed once.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Verify the configuration settings.

```
grep -E '^b*SERVICED' /etc/default/serviced
```

- 3 Start the Control Center service.

```
systemctl start serviced
```

To monitor progress, enter the following command:

```
journalctl -flu serviced -o cat
```

On hosts with internet access, the `serviced` daemon invokes `docker` to pull its internal services images from Docker Hub. The Control Center browser and command-line interfaces are unavailable until the images are installed and tagged, and the services are started. The process takes about 5 minutes.

On hosts without internet access, the `serviced` daemon tags images in the local registry and starts its internal services. The Control Center browser and command-line interfaces are unavailable for about 3 minutes.

When the message `Host Master successfully started` is displayed, Control Center is ready for the next procedure.

Adding the master host to a resource pool

Perform one of the procedures in this section.

Adding the master host to a resource pool (single-host deployments)

Use this procedure to add the master host to a resource pool. For single-host deployments, the master host is added to the `default` pool.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Add the master host to the `default` resource pool.
Replace *Hostname-Or-IP* with the hostname or IP address of the Control Center master host:

```
serviced host add --register Hostname-Or-IP:4979 default
```

If you use a hostname, all of the hosts in your Control Center cluster must be able to resolve the name, either through an entry in `/etc/hosts` or through a nameserver on the network.

Adding the master host to a resource pool (multi-host deployments)

Use this procedure to add the master host to a resource pool. For multi-host deployments, the master host is added to its own, separate pool.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Create a new resource pool named `master`.

```
serviced pool add master
```

- 3 Assign administrative and distributed file system (DFS) permissions to the new resource pool.

```
serviced pool set-permission --admin --dfs master
```

- 4 Add the master host to the new resource pool.
Replace *Hostname-Or-IP* with the hostname or IP address of the Control Center master host:

```
serviced host add --register Hostname-Or-IP:4979 master
```

If you use a hostname, all of the hosts in your Control Center cluster must be able to resolve the name, either through an entry in `/etc/hosts` or through a nameserver on the network.

3

Installing delegate hosts

This chapter describes how to install Control Center on a Red Hat Enterprise Linux (RHEL) or CentOS 7.1 or 7.2 host. The candidate host must have the CPU, RAM, and storage resources required to serve as a delegate host in a Control Center cluster.

For more information about delegate host requirements, refer to the *Control Center Planning Guide*.

Note If you are installing a single-host deployment, skip this chapter.

Repeat the procedures in this chapter on each host to add to a cluster.

Verifying candidate host resources

Use this procedure to determine whether a host's hardware resources and operating system are sufficient to serve as a Control Center delegate host. Perform this procedure on each candidate delegate host in your deployment.

- 1 Log in to the candidate host as `root`, or as a user with superuser privileges.
- 2 Verify that the host implements the 64-bit version of the x86 instruction set.

```
uname -m
```

- If the output is `x86_64`, the architecture is 64-bit. Proceed to the next step
 - If the output is `i386/i486/i586/i686`, the architecture is 32-bit. Stop this procedure and select a different host.
- 3 Determine whether the CPU resources are sufficient.
 - a Display the total number of CPU cores.

```
cat /proc/cpuinfo | grep -Ec '^core id'
```

- b Compare the available resources with the requirements for a Control Center master host.

For more information, refer to the *Control Center Planning Guide*.
- 4 Determine whether the CPU resources support the AES instruction set.

```
cat /proc/cpuinfo | grep -Ec '^flags.*aes'
```

For optimal performance, the result of the preceding commands must match the total number of CPU resources available on the host. If the result is 0, performance is severely degraded.

If the result is 0 and the candidate host is a virtual machine, the managing hypervisor may be configured in Hyper-V compatibility mode. Check the setting and disable it, if possible, or select a different host.

- 5 Determine whether the available memory and swap is sufficient.

- a Display the available memory.

```
free -h
```

- b Compare the available memory with the amount required for a delegate host in your deployment.

For more information, refer to the *Control Center Planning Guide*.

- 6 Ensure the host has a persistent numeric ID.

Each host in a Control Center cluster must have a unique host ID, and the ID must be persistent (not change when the host reboots).

```
test -f /etc/hostid || genhostid
hostid
```

Record the ID for comparison with other hosts in the cluster.

- 7 Verify that name resolution works on this host.

```
hostname -i
```

If the result is not a valid IPv4 address, add an entry for the host to the network nameserver, or to `/etc/hosts`.

- 8 Add an entry to `/etc/hosts` for localhost, if necessary.

- a Determine whether 127.0.0.1 is mapped to localhost.

```
grep 127.0.0.1 /etc/hosts | grep localhost
```

If the preceding commands return no result, perform the following substep.

- b Add an entry to `/etc/hosts` for localhost.

```
echo "127.0.0.1 localhost" >> /etc/hosts
```

- 9 Update the operating system, if necessary.

- a Determine which release is installed.

```
cat /etc/redhat-release
```

If the result includes 7.0, perform the following substeps.

- b Update the operating system and then restart the host.

The following commands require internet access or a local mirror of operating system packages.

```
yum makecache fast && yum update -y && reboot
```

- 10 Update the Linux kernel, if necessary.

- a Determine which kernel version is installed.

```
uname -r
```

If the result is lower than 3.10.0-327.22.2.el7.x86_64, perform the following substeps.

- b Update the kernel or the operating system, and then restart the host.

The following commands require internet access or a local mirror of operating system packages.

Update only the kernel:

```
yum makecache fast && yum update -y kernel && reboot
```

Update the operating system, including the kernel:

```
yum makecache fast && yum update -y && reboot
```

Delegate host storage requirements

This section provides a quick reference to the block storage requirements of Control Center delegate hosts. For more information, refer to the *Control Center Planning Guide*.

Control Center cluster hosts need either unformatted block storage devices or partitions, or free space in one or more LVM volume groups.

- Enter the following command to display information about block storage:

```
lsblk -ap --output=NAME,SIZE,TYPE,FSTYPE,MOUNTPOINT
```

- Enter the following command to display information about LVM volume groups:

```
vgdisplay
```

The following storage configuration is recommended for delegate hosts:

- One local, high-performance device or partition with a minimum of 35GB of storage, formatted with XFS, for the root filesystem.
- One local, unformatted, high-performance device or partition with 50GB of storage. A step in this chapter configures the space as an LVM thin pool for Docker data.

Disabling consistent network device naming

The consistent network device naming feature can create device names that are too long for use with virtual IPs. This step disables the feature so that all network device names are `eth` followed by an integer.

- 1 Log in as `root`, or as a user with superuser privileges.
- 2 Edit the GRUB 2 general settings file.
 - a Create a backup copy of the settings file.

```
cp /etc/default/grub /etc/default/grub.bak
```

- b Open `/etc/default/grub` with a text editor.
 - c Add kernel boot arguments to the value of the `GRUB_CMDLINE_LINUX` variable.
The arguments to add are `biosdevname=0` and `net.ifnames=0`. Make sure the arguments are between the delimiter characters (`"`).
 - d Save the file, and then close the text editor.
- 3 Determine whether the host is configured for UEFI or legacy boot mode.

```
find /boot -maxdepth 1 -type d
```

- If the output includes `/boot/efi`, the host is configured for UEFI boot mode.
- If the output does not include `/boot/efi`, the host is configured for legacy boot mode.

- 4 Recreate the GRUB 2 boot configuration file.

For UEFI boot mode:

```
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

For legacy boot mode:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- 5 Create an override for the default rules policy of the dynamic device management daemon.

```
ln -s /dev/null /etc/udev/rules.d/80-net-name-slot.rules
```

- 6 Change network device configurations.

- a Change directory to /etc/sysconfig/network-scripts.

```
cd /etc/sysconfig/network-scripts
```

- b List the network device configuration files.

```
ls ifcfg-* | grep -v ifcfg-lo
```

The `ifcfg-lo` file is excluded because it does not need to be changed.

- c Rename and edit device files.

For example, if you have a device file named `ifcfg-enol6777736`, use the `mv` command rename it to `ifcfg-eth0`, and then change the values of the *NAME* and *DEVICE* variables inside the file to `eth0`.

- 7 Reboot the host.

Preparing a delegate host

Zenoss customers: If you are creating a deployment without internet access, perform the steps in [Preparing to install without internet access](#) on page 78, before performing this procedure.

Use this procedure to prepare a RHEL/CentOS 7.1 or 7.2 host as a Control Center delegate host.

- 1 Log in to the candidate delegate host as `root`, or as a user with superuser privileges.
- 2 Disable the firewall, if necessary.

This step is required for installation but not for deployment. For more information, refer to the *Control Center Planning Guide*.

- a Determine whether the `firewalld` service is enabled.

```
systemctl status firewalld.service
```

- If the result includes `Active: inactive (dead)`, the service is disabled. Proceed to the next step.
- If the result includes `Active: active (running)`, the service is enabled. Perform the following substep.

- b Disable the `firewalld` service.

```
systemctl stop firewalld && systemctl disable firewalld
```

On success, the preceding commands display messages similar to the following example:

```
rm '/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service'
rm '/etc/systemd/system/basic.target.wants/firewalld.service'
```

3 Optional: Enable persistent storage for log files, if desired.

By default, RHEL/CentOS systems store log data only in memory or in a ring buffer in the `/run/log/journal` directory. By performing this step, log data persists and can be saved indefinitely, if you implement log file rotation practices. For more information, refer to your operating system documentation.

```
mkdir -p /var/log/journal && systemctl restart systemd-journald
```

4 Disable Security-Enhanced Linux (SELinux), if installed.

a Determine whether SELinux is installed.

```
test -f /etc/selinux/config && grep '^SELINUX=' /etc/selinux/config
```

If the preceding commands return a result, SELinux is installed.

b Set the operating mode to disabled.

Open `/etc/selinux/config` in a text editor, and change the value of the `SELINUX` variable to `disabled`.

c Confirm the new setting.

```
grep '^SELINUX=' /etc/selinux/config
```

5 Enable and start the Dnsmasq package.

The package facilitates networking among Docker containers.

```
systemctl enable dnsmasq && systemctl start dnsmasq
```

6 Install and configure the NTP package.

Note This procedure assumes the host has internet access. To install and configure NTP on a host that does not have internet access, see [Configuring a private master NTP server](#) on page 80.

a Install the package.

```
yum install -y ntp
```

b Set the system time.

```
ntpd -gq
```

c Enable the `ntpd` daemon.

```
systemctl enable ntpd
```

d Configure `ntpd` to start when the system starts.

Currently, an unresolved issue associated with NTP prevents `ntpd` from restarting correctly after a reboot. The following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
```

7 Add the Zenoss repositories to the host's repository list.

a Install the repository package.

The package adds the Zenoss stable, unstable, and testing repositories to `/etc/yum.repos.d`. All three repositories are disabled.

```
rpm -ivh http://get.zenoss.io/yum/zenoss-repo-1-1.x86_64.rpm
```

- b** Clean out the yum cache directory.

```
yum clean all
```

- 8** Reboot the host.

```
reboot
```

Installing Docker Engine

Use one of the procedures in this section to install Docker Engine.

Installing Docker Engine with internet access

Use this procedure to install Docker Engine on a host that has internet access.

- 1** Log in to the host as `root`, or as a user with superuser privileges.
- 2** Install Docker Engine 1.12.1, and then disable accidental upgrades.
 - a** Add the Docker repository to the host's repository list.

```
cat <<EOF > /etc/yum.repos.d/docker.repo
[dockerrepo]
name=Docker Repository
baseurl=https://yum.dockerproject.org/repo/main/centos/7/
enabled=1
gpgcheck=1
gpgkey=https://yum.dockerproject.org/gpg
EOF
```

- b** Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- c** Install Docker Engine from the remote repository.

```
yum install -y docker-engine-1.12.1
```

- d** Open `/etc/yum.repos.d/docker.repo` with a text editor.
- e** Change the value of the `enabled` key from 1 to 0.
- f** Save the file, and then close the text editor.

Optional: Installing Docker Engine without internet access

Zenoss customers: If you are installing Docker Engine without internet access, perform the steps in [Preparing to install without internet access](#) on page 78 before performing this procedure.

Use this procedure to install Docker Engine on a host that does not have internet access.

- 1** Log in to the host as `root`, or as a user with superuser privileges.
- 2** Install Docker Engine 1.12.1 from the local repository mirror.

- a Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- b Install Docker Engine.

```
yum install --enablerepo=zenoss-mirror -y docker-engine-1.12.1
```

Installing Control Center

Use one of the procedures in this section to install Control Center.

Installing Control Center with internet access

Use this procedure to install Control Center on a host that has internet access.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Install Control Center 1.2.0.

- a Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- b Install Control Center from the remote repository.

```
yum --enablerepo=zenoss-stable install -y serviced-1.2.0
```

Optional: Installing Control Center without internet access

Zenoss customers: Perform the steps in [Preparing to install without internet access](#) on page 78 before performing this procedure.

Use this procedure to install Control Center on a host that does not have internet access.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Install Control Center 1.2.0 from the local repository mirror.

- a Clean the yum cache and update repository metadata.

```
yum clean all && yum makecache fast
```

- b Install Control Center.

```
yum install --enablerepo=zenoss-mirror -y serviced-1.2.0
```

Configuring Docker

Use this procedure to configure Docker.

- 1 Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2 Create a symbolic link for the Docker temporary directory.

Docker uses its temporary directory to spool images. The default directory is `/var/lib/docker/tmp`. The following command specifies the same directory that Control Center uses, `/tmp`. You can specify any directory that has a minimum of 10GB of unused space.

- a** Create the `docker` directory in `/var/lib`.

```
mkdir /var/lib/docker
```

- b** Create the link to `/tmp`.

```
ln -s /tmp /var/lib/docker/tmp
```

- 3** Create a `systemd` drop-in file for Docker Engine.

- a** Create the override directory.

```
mkdir -p /etc/systemd/system/docker.service.d
```

- b** Create the unit drop-in file.

```
cat <<EOF > /etc/systemd/system/docker.service.d/docker.conf
[Service]
TimeoutSec=300
EnvironmentFile=-/etc/sysconfig/docker
ExecStart=
ExecStart=/usr/bin/dockerd $OPTIONS
TasksMax=infinity
EOF
```

- c** Reload the `systemd` manager configuration.

```
systemctl daemon-reload
```

- 4** Create an LVM thin pool for Docker data.

For more information about the `serviced-storage` command, see [serviced-storage](#) on page 64.

Replace *Storage* with the paths of one or more block devices or partitions, or the name of an LVM volume group:

```
serviced-storage create-thin-pool --size=50G docker Storage
```

On success, the result is the device mapper name of the thin pool, which always starts with `/dev/mapper`.

- 5** Configure and start the Docker service.

- a** Create a variable for the name of the Docker thin pool.

Replace *Thin-Pool-Device* with the name of the thin pool device created in the previous step:

```
myPool="Thin-Pool-Device"
```

- b** Create a variable for the IPv4 address of the master host.

Replace *Master-Host* with the hostname or IPv4 address of the master host:

```
masterIP="Master-Host"
```

- c** Create variables for adding arguments to the Docker configuration file. The `--exec-opt` argument is a workaround for [a Docker issue](#) on RHEL/CentOS 7.x systems.

```
myDriver="--storage-driver devicemapper"
myLog="--log-level=error"
myFix="--exec-opt native.cgroupdriver=cgroupfs"
myMount="--storage-opt dm.mountopt=discard"
myFlag="--storage-opt dm.thinpooldev=$myPool"
```

```
myReg="--insecure-registry=$masterIP:5000"
```

- d** Add the arguments to the Docker configuration file.

```
echo 'OPTIONS="'$myLog $myDriver $myFix $myMount $myFlag $myReg'"' \
>> /etc/sysconfig/docker
```

- e** Start or restart Docker.

```
systemctl restart docker
```

The startup may take up to a minute, and may fail. If startup fails, repeat the `restart` command.

6 Configure name resolution in containers.

Each time it starts, `docker` selects an IPv4 subnet for its virtual Ethernet bridge. The selection can change; this step ensures consistency.

- a** Identify the IPv4 subnet and netmask `docker` has selected for its virtual Ethernet bridge.

```
ip addr show docker0 | grep inet
```

- b** Open `/etc/sysconfig/docker` in a text editor.

- c** Add the following flags to the end of the `OPTIONS` declaration.

Replace *Bridge-Subnet* with the IPv4 subnet `docker` selected for its virtual bridge:

```
--dns=Bridge-Subnet --bip=Bridge-Subnet/16
```

For example, if the bridge subnet is 172.17.0.1, add the following flags:

```
--dns=172.17.0.1 --bip=172.17.0.1/16
```

Note Use a space character () to separate flags, and make sure the double quote character (") delimits the declaration of `OPTIONS`.

- d** Restart the Docker service.

```
systemctl restart docker
```

Proceed to the next chapter and configure the host.

4

Configuring and starting delegate hosts

This chapter provides the procedures that are required to configure a delegate host, describes the configuration options that apply to delegate hosts, and includes steps for starting a delegate for the first time. Perform the procedures in this chapter on each delegate host in a Control Center cluster.

Note If you are installing a single-host deployment, skip this chapter.

This chapter includes synopses of the configuration variables that affect delegate hosts. For more information about a variable, see [Control Center configuration variables](#) on page 68.

Control Center maintenance scripts on delegate hosts

The scripts in the following list are installed when Control Center is installed, and are started either daily or weekly by `anacron`.

Of these scripts, only the first is required on delegate hosts. The others can be removed.

/etc/cron.daily/serviced

This script invokes `logrotate` daily, to manage the `/var/log/serviced.access.log` file.

This script is required on the master host and on all delegate hosts.

/etc/cron.weekly/serviced-fstrim

This script can be removed from delegate hosts.

/etc/cron.weekly/serviced-zenossdbpack

This script can be removed from delegate hosts.

Enabling use of the command-line interface

Use this procedure to enable a user to perform administrative tasks with the Control Center command-line interface.

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Add a user to the Docker group.

Replace *User* with the name of a login account on the host.

```
usermod -aG docker User
```

Repeat the preceding command for each user to add.

Setting the host role to delegate

Use this procedure to configure a host as a delegate host. The following configuration variable assigns the host role:

SERVICED_MASTER

Default: 1 (true)

Assigns the role of a `serviced` instance, either master or delegate. The master runs the application services scheduler and other internal services. Delegates run the application services assigned to the resource pool to which they belong.

Only one `serviced` instance can be the master; all other instances must be delegates. The default value assigns the master role. To assign the delegate role, set the value to 0 (false). This variable must be explicitly set on all Control Center cluster hosts.

Perform these steps:

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Edit the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Locate the line for the `SERVICED_MASTER` variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (`#`) from the beginning of the line.
 - d Change the value from 1 to 0.
 - e Save the file, and then close the editor.
- 3 Verify the settings.

```
grep -E '^b*SERVICED' /etc/default/serviced
```

Setting internal services endpoints

Use this procedure to configure a delegate host with the endpoints of the Control Center internal services.

Although Control Center relies on ZooKeeper for coordination, it is not a Control Center internal service. The instructions for setting the ZooKeeper endpoint are included in the next chapter.

The following configuration variables identify the internal services endpoints:

SERVICED_DOCKER_REGISTRY

Default: `{{SERVICED_MASTER_IP}}:5000`

The endpoint of the `serviced` Docker registry host. On delegate hosts, replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the registry host, which by default is the `serviced` master host.

SERVICED_ENDPOINT

Default: `{{SERVICED_MASTER_IP}}:4979`

The endpoint of the `serviced` RPC server. Replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the `serviced` master host. The port number of this endpoint must match the value of the `SERVICED_RPC_PORT` variable defined on the `serviced` master host.

SERVICED_LOG_ADDRESS

Default: `{{SERVICED_MASTER_IP}}:5042`

The endpoint of the logstash service. Replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the `serviced` master host.

SERVICED_LOGSTASH_ES**Default:** `{{SERVICED_MASTER_IP}}:9100`

The endpoint of the logstash Elasticsearch service. On delegate hosts, replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the Elasticsearch host, which by default is the `serviced` master host.

SERVICED_STATS_PORT**Default:** `{{SERVICED_MASTER_IP}}:8443`

The endpoint of the `serviced` metrics consumer service. Replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the `serviced` master host.

Perform these steps:

- 1 Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2 Edit the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b For each endpoint variable, locate the line that sets the variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (`#`) from the beginning of the line.
 - d Replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the master host.
 - e Save the file, and then close the editor.
- 3 Verify the settings.

```
grep -E '^b*SERVICED' /etc/default/serviced
```

Optional: Configuring offline use

Zenoss customers: If you are creating a deployment without internet access, perform this procedure.

Use this procedure to configure a host to operate without internet access. The following configuration variable informs `serviced` that internet access is not available:

SERVICED_OUTBOUND_IP**Default:** (none)

The default startup routines of `serviced` include attempting to ping `google.com`. When a value is set for this variable, `serviced` does not attempt the ping and assumes it does not have internet access.

Use this variable to specify the IP address of a network interface other than the default, or to prevent `serviced` from assuming it has internet access.

Note Setting the Docker `HTTP_PROXY` or `HTTPS_PROXY` environment variables prevents access to the IP address defined with this variable. To enable access, unset the Docker variables, and then reboot the host.

Perform these steps:

- 1 Log in to the host as `root`, or as a user with superuser privileges.
- 2 Identify the IPv4 address of the host.

```
hostname -i
```

- 3 Edit the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.

- b Locate the line for the *SERVICED_OUTBOUND_IP* variable, and then make a copy of the line, immediately below the original.
 - c Remove the number sign character (#) from the beginning of the line.
 - d Change the value to the IPv4 address identified in the previous step.
 - e Save the file, and then close the editor.
- 4 Verify the settings.

```
grep -E '^\\b*SERVICED' /etc/default/serviced
```

Delegate host configuration variables

The tables in this section provide an overview of the *serviced* configuration variables that apply to Control Center delegate hosts. Set these variables as required for your environment or applications.

Delegate variables

The following miscellaneous variables apply only to delegate hosts.

Variable	Description
<i>SERVICED_STATS_PERIOD</i>	The frequency at which delegates gather metrics to send to the master host.
<i>SERVICED_IPTABLES_MAX_CONNECTIONS</i>	The maximum number of open connections to allow on a delegate. The number increases when the master is unavailable and decreases when the master returns to service.

Internal services endpoint variables

The variables in the following table must be set identically on all Control Center delegate hosts. On the master host, the default values of these variables do not need to be changed, unless the Docker registry is hosted on a system other than the master. In that case, *SERVICED_DOCKER_REGISTRY* must be set explicitly on the master host, too.

The *SERVICED_AUTH_TOKEN_EXPIRATION* variable affects RPC, mux, and internal services endpoint traffic.

Variable	Endpoint	Description
<i>SERVICED_DOCKER_REGISTRY</i>	<i>Master-Host</i> : 9100	The local Docker registry for Control Center internal services images and application images.
<i>SERVICED_ENDPOINT</i>	<i>Master-Host</i> : 4979	The <i>serviced</i> RPC server. The endpoint port number must match the value of <i>SERVICED_RPC_PORT</i> .
<i>SERVICED_LOG_ADDRESS</i>	<i>Master-Host</i> : 5042	The <i>logstash</i> service.
<i>SERVICED_LOGSTASH_ES</i>	<i>Master-Host</i> : 9100	The Elasticsearch service.
<i>SERVICED_STATS_PORT</i>	<i>Master-Host</i> : 8443	The <i>serviced</i> metrics consumer service.

Variable	Endpoint	Description
<i>SERVICED_AUTH_TOKEN_EXPIRATION</i>	(none)	The length of time a delegate authentication token is valid.

RPC service variables

The variables in the following table must be set identically on all Control Center cluster hosts, except:

- *SERVICED_RPC_PORT*, set only on the master
- *SERVICED_MAX_RPC_CLIENTS*, set only on delegates

By default, *serviced* uses TLS to encrypt all RPC traffic. The *SERVICED_KEY_FILE* and *SERVICED_CERT_FILE* variables identify the digital certificate used for RPC, mux, and HTTP traffic.

The *SERVICED_AUTH_TOKEN_EXPIRATION* variable affects RPC, mux, and internal services endpoint traffic.

Variable	Where to set
<i>SERVICED_ENDPOINT</i>	Master, delegates
<i>SERVICED_MAX_RPC_CLIENTS</i>	Delegates
<i>SERVICED_RPC_PORT</i>	Master
<i>SERVICED_RPC_CERT_VERIFY</i>	Master, delegates
<i>SERVICED_RPC_DISABLE_TLS</i>	Master, delegates
<i>SERVICED_RPC_TLS_MIN_VERSION</i>	Master, delegates
<i>SERVICED_RPC_TLS_CIPHERS</i>	Master, delegates
<i>SERVICED_KEY_FILE</i>	Master
<i>SERVICED_CERT_FILE</i>	Master
<i>SERVICED_RPC_DIAL_TIMEOUT</i>	Master, delegates
<i>SERVICED_AUTH_TOKEN_EXPIRATION</i>	Master

Multiplexer variables

The variables in the following table must be set identically on all Control Center cluster hosts.

By default, *serviced* uses TLS to encrypt all mux traffic. The *SERVICED_KEY_FILE* and *SERVICED_CERT_FILE* variables identify the digital certificate used for RPC, mux, and HTTP traffic.

The *SERVICED_AUTH_TOKEN_EXPIRATION* variable affects RPC, mux, and internal services endpoint traffic.

Variable	Where to set
<i>SERVICED_MUX_PORT</i>	Master, delegates
<i>SERVICED_MUX_DISABLE_TLS</i>	Master, delegates
<i>SERVICED_MUX_TLS_MIN_VERSION</i>	Master, delegates

Variable	Where to set
<i>SERVICED_MUX_TLS_CIPHERS</i>	Master, delegates
<i>SERVICED_KEY_FILE</i>	Master
<i>SERVICED_CERT_FILE</i>	Master
<i>SERVICED_AUTH_TOKEN_EXPIRATION</i>	Master

Universal configuration variables

The tables in this section provide an overview of the `serviced` configuration variables that apply to all hosts in a Control Center cluster. Set these variables as required for your environment or applications.

Role variable

Variable	Description
<i>SERVICED_MASTER</i>	Assigns the role of a <code>serviced</code> instance, either master or delegate. The master runs the application services scheduler and other internal services. Delegates run the application services assigned to the resource pool to which they belong.

Browser interface variable (all hosts)

Variable	Description
<i>SERVICED_UI_PORT</i>	The port on which the HTTP server listens for requests.

Networking variables

Variable	Description
<i>SERVICED_STATIC_IPS</i>	A list of one or more static IP addresses for IP assignment.
<i>SERVICED_OUTBOUND_IP</i>	The IP address of the network interface for <code>serviced</code> to use. When this variable is not set, <code>serviced</code> uses the IP address of the default network interface and assumes it has internet access. To prevent <code>serviced</code> from assuming it has internet access, set this variable.
<i>SERVICED_VIRTUAL_ADDRESS_SUBNET</i>	The private network for containers that use virtual IP addresses. The default is <code>10.3.0.0/16</code> , and the network can be unique on each host. A <code>/29</code> network is sufficient.
<i>SERVICED_DOCKER_DNS</i>	A list of one or more DNS servers. The list is injected into all Docker Engine containers.

Debugging variables

Variable	Description
<i>SERVICED_LOG_LEVEL</i>	The log level <code>serviced</code> uses when writing to the system log.

Variable	Description
<i>SERVICED_DEBUG_PORT</i>	The port on which <code>serviced</code> listens for HTTP requests for the Go profiler .
<i>SERVICED_DOCKER_LOG_DRIVER</i>	The log driver for all Docker container logs.
<i>SERVICED_DOCKER_LOG_CONFIG</i>	Docker <code>--log-opt</code> options.

Tuning variables (all cluster hosts)

Variable	Description
<i>GOMAXPROCS</i>	The maximum number of CPU cores that <code>serviced</code> uses.
<i>SERVICED_MAX_CONTAINER_AGE</i>	The number of seconds <code>serviced</code> waits before removing a stopped container.
<i>SERVICED_ISVCS_ENV_[0-9]+</i>	Startup arguments to pass to specific internal services.
<i>SERVICED_SERVICE_MIGRATION_TAG</i>	Overrides the default value for the service migration image.
<i>SERVICED_OPTS</i>	Startup arguments for <code>serviced</code> .
<i>SERVICED_CONTROLLER_BINARY</i>	The path of the <code>serviced-controller</code> binary.
<i>SERVICED_HOME</i>	The path of the home directory for <code>serviced</code> .
<i>SERVICED_ETC_PATH</i>	The path of the directory for <code>serviced</code> configuration files.
<i>SERVICED_VHOST_ALIASES</i>	A list of hostname aliases for a host; for example, <code>localhost</code> .

Starting Control Center

Use this procedure to start `serviced` on a delegate host for the first time.

- 1 Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2 Verify the configuration settings.

```
grep -E '^\b*SERVICED' /etc/default/serviced
```

- 3 Start the Control Center service (`serviced`).

```
systemctl start serviced
```

To monitor progress, enter the following command:

```
journalctl -flu serviced -o cat
```

Delegate host authentication

Control Center uses RSA key pairs to create the authentication tokens that are required for all delegate communications. When you add a host to a resource pool, the `serviced` instance on the master host creates a private key for the delegate and bundles it with its own public key. The `serviced` instance on the delegate host uses the bundle to sign messages with its unique tokens.

Key bundles are installed by using an SSH connection or a file.

- The command to add a host to a pool can initiate an SSH connection with the delegate and install the key bundle. This option is the most secure, because no file is created. However, it requires either public key authentication or password authentication between the master and delegate hosts.
- When no SSH connection is requested, the command to add a host to a pool creates a file containing the key bundle. You can move the key bundle file to the delegate host with any file transfer method, and then install it on the delegate.

The following procedures demonstrate how to add a host to a resource pool and install its key bundle.

Adding a delegate host through an SSH connection

To succeed, the following statements about the login account used to perform this procedure must be true:

- The account exists on both the master host and on the delegate host.
- The account has `serviced` CLI privileges.
- The account has either public key authentication or password authentication enabled on the master host and on the delegate host.

Use this procedure to add a delegate host to a resource pool through an SSH connection.

- 1 Log in to the Control Center master host as a user with `serviced` CLI privileges.
- 2 Optional: Create a new resource pool, if desired.
 - a Display the names of the existing resource pools.

```
serviced pool list
```

- b Create a new resource pool.
Replace *Resource-Pool* with the name of a new resource pool:

```
serviced pool add Resource-Pool
```

- 3 Add a delegate host to a resource pool.

If the master and delegate host are configured for key-based access, the following command does not prompt you to add the delegate to the list of known hosts or to provide the password of the remote user account.

You can use a hostname or an IP address to identify a Control Center cluster host. If you use a hostname, all of the hosts in your cluster must be able to resolve it, either through an entry in `/etc/hosts` or through a nameserver on the network.

Replace *Hostname-Or-IP* with the hostname or IP address of a delegate host, and replace *Resource-Pool* with the name of a resource pool:

```
serviced host add --register Hostname-Or-IP:4979 Resource-Pool
```

Adding a delegate host using a file

Use this procedure to add a delegate host to a resource pool by using a key bundle file.

- 1 Log in to the Control Center master host as a user with `serviced` CLI privileges.
- 2 Optional: Create a new resource pool, if desired.
 - a Display the names of the existing resource pools.

```
serviced pool list
```

- b Create a new resource pool.

Replace *Resource-Pool* with the name of a new resource pool:

```
serviced pool add Resource-Pool
```

3 Add a delegate host to a resource pool.

You can use a hostname or an IP address to identify a Control Center cluster host. If you use a hostname, all of the hosts in your cluster must be able to resolve it, either through an entry in `/etc/hosts` or through a nameserver on the network.

Replace *Hostname-Or-IP* with the hostname or IP address of a delegate host, and replace *Resource-Pool* with the name of a resource pool:

```
serviced host add Hostname-Or-IP:4979 Resource-Pool
```

The command creates a unique key bundle file in the local directory.

4 Use a file transfer utility such as `scp` to copy the key bundle file to the delegate host.

Once copied to the delegate host, the key bundle file is not needed on the master host and can be deleted.

5 Log in to the Control Center delegate host as a user with `serviced` CLI privileges.

6 Install the key bundle.

Replace *Key-Bundle-Path* with the pathname of the key bundle file:

```
serviced host register Key-Bundle-Path
```

7 Delete the key bundle file.

The file is no longer needed on the delegate host.

Replace *Key-Bundle-Path* with the pathname of the key bundle file:

```
rm Key-Bundle-Path
```

5

Configuring a ZooKeeper ensemble

This chapter describes how to create a ZooKeeper ensemble (cluster) for a multi-host Control Center deployment. If you are installing a single-host deployment, or if your deployment includes fewer than two delegate hosts, skip this chapter.

ZooKeeper and Control Center

Control Center relies on [Apache ZooKeeper](#) to distribute and manage application services. ZooKeeper maintains the definitions of each service and the list of services assigned to each host. The scheduler, which runs on the master host, determines assignments and sends them to the ZooKeeper node that is serving as the ensemble leader. The leader replicates the assignments to the other ensemble nodes, so that the other nodes can assume the role of leader if the leader node fails.

All of the hosts in a Control Center cluster retrieve assignments and service definitions from the ZooKeeper ensemble leader and then start services in Docker containers as required. So, the Control Center configuration files of all Control Center cluster hosts must include a definition for the `SERVICED_ZK` variable, which specifies the ZooKeeper endpoints of the ensemble nodes. Additional variables are required on ensemble nodes.

A ZooKeeper ensemble requires a minimum of three nodes, which is sufficient for most environments. An odd number of nodes is recommended and an even number of nodes is strongly discouraged. A five-node ensemble improves failover protection during maintenance windows but larger ensembles yield no benefits.

The Control Center master host is always an ensemble node. All ensemble nodes should be on the same subnet.

Understanding the configuration process

The procedures in this chapter instruct you to create temporary variables that are used as building blocks, to construct Control Center configuration variables accurately. You append the Control Center variables to `/etc/default/serviced`, and then edit the file to move the variables to more appropriate locations.

The most important temporary variables specify the IP address or hostname of each host in the ZooKeeper ensemble. The following table identifies these important variables, the names and values of which must be identical on every Control Center cluster host.

Variable name	Placeholder value	Actual value
node1	<i>Master</i>	IP address or hostname of the master host
node2	<i>Delegate-A</i>	IP address or hostname of delegate host A
node1	<i>Delegate-B</i>	IP address or hostname of delegate host B

Note All ensemble hosts should be on the same subnet.

ZooKeeper variables

The variables in the following table are set only on ZooKeeper ensemble nodes, except *SERVICED_ZK*, which must be identical on all Control Center cluster hosts.

Variable	Where to set
<i>SERVICED_ISVCS_START</i>	ZooKeeper ensemble nodes
<i>SERVICED_ISVCS_ZOOKEEPER_ID</i>	ZooKeeper ensemble nodes
<i>SERVICED_ISVCS_ZOOKEEPER_QUORUM</i>	ZooKeeper ensemble nodes
<i>SERVICED_ZK</i>	All Control Center cluster hosts
<i>SERVICED_ZK_SESSION_TIMEOUT</i>	ZooKeeper ensemble nodes

Example multi-host ZooKeeper configuration

This example shows the ZooKeeper variables in the `/etc/defaults/serviced` configuration file of each host in a 4-node Control Center cluster. For convenience, the relevant settings for each node or host are also included in subsequent procedures.

Note The value of the *SERVICED_ISVCS_ZOOKEEPER_QUORUM* variable is formatted to fit the available space. In the configuration file, the variable and value are on the same line.

Master host and ZooKeeper ensemble node, 198.51.100.135:

```
SERVICED_ISVCS_ZOOKEEPER_ID=1
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@0.0.0.0:2888:3888,\
  2@198.51.100.136:2888:3888,3@198.51.100.137:2888:3888
SERVICED_ZK_SESSION_TIMEOUT=15
```

Delegate host and ZooKeeper ensemble node, 198.51.100.136:

```
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=2
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
  2@0.0.0.0:2888:3888,3@198.51.100.137:2888:3888
SERVICED_ZK_SESSION_TIMEOUT=15
```

Delegate host and ZooKeeper ensemble node, 198.51.100.137:

```
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=3
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
  2@198.51.100.136:2888:3888,3@0.0.0.0:2888:3888
SERVICED_ZK_SESSION_TIMEOUT=15
```

Delegate host, 198.51.100.138:

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
```

Configuring the master host as a ZooKeeper node

This procedure configures the Control Center master host as a node in a ZooKeeper ensemble.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Define the IP address variables for each node in the ZooKeeper ensemble.
Replace *Master* with the IP address or hostname of the Control Center master host, and replace *Delegate-A* and *Delegate-B* with the IP addresses or hostnames of the delegate hosts to include in the ensemble:

```
node1=Master
node2=Delegate-A
node3=Delegate-B
```

- 3 Set the ZooKeeper node ID to 1.

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=1" >> /etc/default/serviced
```

- 4 Specify the nodes in the ZooKeeper ensemble.
You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 5 Specify the nodes in the ZooKeeper quorum.
ZooKeeper requires a unique quorum definition for each node in its ensemble. To achieve this, replace the IP address or hostname of the master host with `0.0.0.0`.

You can copy the following text and paste it in your console:

```
q1="1@0.0.0.0:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 6 Specify the timeout for inactive connections.
You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK_SESSION_TIMEOUT=15" >> /etc/default/serviced
```

- 7 Clean up the Control Center configuration file.
 - a Open `/etc/default/serviced` in a text editor.
 - b Navigate to the end of the file, and cut the line that contains the `SERVICED_ZK` variable declaration at that location.
 - c Locate the original `SERVICED_ZK` variable declaration, and then paste the cut line immediately below it.
 - d Navigate to the end of the file, and cut the line that contains the `SERVICED_ISVCS_ZOOKEEPER_ID` variable declaration at that location.
 - e Locate the original `SERVICED_ISVCS_ZOOKEEPER_ID` variable declaration, and then paste the cut line immediately below it.
 - f Navigate to the end of the file, and cut the line that contains the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable declaration at that location.

- g Locate the original `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable declaration, and then paste the cut line immediately below it.
 - h Navigate to the end of the file, and cut the line that contains the `SERVICED_ZK_SESSION_TIMEOUT` variable declaration at that location.
 - i Locate the original `SERVICED_ZK_SESSION_TIMEOUT` variable declaration, and then paste the cut line immediately below it.
 - j Save the file, and then close the editor.
- 8 Verify the ZooKeeper environment variables.

```
grep -E '^\\b*SERVICED' /etc/default/serviced | grep -E '_Z(OO|K) '
```

The following example shows the environment variables for a master host with IP address 198.51.100.135.

Note The value of the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable is formatted to fit the available space. The result of the `grep` command shows the variable and value on the same line.

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_ZOOKEEPER_ID=1
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@0.0.0.0:2888:3888, \
    2@198.51.100.136:2888:3888,3@198.51.100.137:2888:3888
SERVICED_ZK_SESSION_TIMEOUT=15
```

Configuring delegate host A as a ZooKeeper node

Use this procedure to configure the delegate host designated as *Delegate-A* as a ZooKeeper node.

- 1 Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2 Define the IP address variables for each node in the ZooKeeper ensemble.
Replace *Master* with the IP address or hostname of the Control Center master host, and replace *Delegate-A* and *Delegate-B* with the IP addresses or hostnames of the delegate hosts to include in the ensemble:

```
node1=Master
node2=Delegate-A
node3=Delegate-B
```

- 3 Set the ID of this node in the ZooKeeper ensemble.

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=2" >> /etc/default/serviced
```

- 4 Specify the nodes in the ZooKeeper ensemble.
You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 5 Specify the nodes in the ZooKeeper quorum.

ZooKeeper requires a unique quorum definition for each node in its ensemble. To achieve this, replace the IP address or hostname of delegate host A with `0.0.0.0`.

You can copy the following text and paste it in your console:

```
q1="1@${node1}:2888:3888"
q2="2@0.0.0.0:2888:3888"
q3="3@${node3}:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
```

```
>> /etc/default/serviced
```

- 6 Specify the timeout for inactive connections.

You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK_SESSION_TIMEOUT=15" >> /etc/default/serviced
```

- 7 Set the *SERVICED_ISVCS_START* variable, and clean up the Control Center configuration file.

- a Open `/etc/default/serviced` in a text editor.
- b Locate the line for the *SERVICED_ISVCS_START* variable, and then make a copy of the line, immediately below the original.
- c Remove the number sign character (#) from the beginning of the line.
- d Delete all but `zookeeper` from its list of values.
- e Navigate to the end of the file, and cut the line that contains the *SERVICED_ZK* variable declaration at that location.
- f Locate the original *SERVICED_ZK* variable declaration, and then paste the cut line immediately below it.
- g Comment the original *SERVICED_ZK* declaration, which references only the master host.
Insert the number sign character (#) immediately in front of the original *SERVICED_ZK* variable.
- h Navigate to the end of the file, and cut the line that contains the *SERVICED_ISVCS_ZOOKEEPER_ID* variable declaration at that location.
- i Locate the original *SERVICED_ISVCS_ZOOKEEPER_ID* variable declaration, and then paste the cut line immediately below it.
- j Navigate to the end of the file, and cut the line that contains the *SERVICED_ISVCS_ZOOKEEPER_QUORUM* variable declaration at that location.
- k Locate the original *SERVICED_ISVCS_ZOOKEEPER_QUORUM* variable declaration, and then paste the cut line immediately below it.
- l Navigate to the end of the file, and cut the line that contains the *SERVICED_ZK_SESSION_TIMEOUT* variable declaration at that location.
- m Locate the original *SERVICED_ZK_SESSION_TIMEOUT* variable declaration, and then paste the cut line immediately below it.
- n Save the file, and then close the editor.

- 8 Verify the ZooKeeper environment variables.

```
grep -E '^b*SERVICED' /etc/default/serviced \
| grep -E '(CS_ZO|_ZK|CS_ST)'
```

The following example shows the environment variables for a delegate host with IP address 198.51.100.136.

Note The value of the *SERVICED_ISVCS_ZOOKEEPER_QUORUM* variable is formatted to fit the available space. The result of the `grep` command shows the variable and value on the same line.

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=2
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
2@0.0.0.0:2888:3888,3@198.51.100.137:2888:3888
SERVICED_ZK_SESSION_TIMEOUT=15
```

- 9 Pull the required Control Center ZooKeeper image from the master host.

- a Identify the image to pull.

```
serviced version | grep IsvcsImages
```

Example result:

```
IsvcsImages: [zenoss/serviced-isvcs:v48 zenoss/isvcs-zookeeper:v7]
```

- b** Pull the Control Center ZooKeeper image.

Replace *Isvcs-ZK-Image* with the name and version number of the ZooKeeper image from the previous substep:

```
docker pull Isvcs-ZK-Image
```

Configuring delegate host B as a ZooKeeper node

Use this procedure to configure the delegate host designated as *Delegate-B* as a ZooKeeper node.

- 1** Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2** Define the IP address variables for each node in the ZooKeeper ensemble.
Replace *Master* with the IP address or hostname of the Control Center master host, and replace *Delegate-A* and *Delegate-B* with the IP addresses or hostnames of the delegate hosts to include in the ensemble:

```
node1=Master
node2=Delegate-A
node3=Delegate-B
```

- 3** Set the ID of this node in the ZooKeeper ensemble.

```
echo "SERVICED_ISVCS_ZOOKEEPER_ID=3" >> /etc/default/serviced
```

- 4** Specify the nodes in the ZooKeeper ensemble.
You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

- 5** Specify the nodes in the ZooKeeper quorum.
ZooKeeper requires a unique quorum definition for each node in its ensemble. To achieve this, replace the IP address or hostname of delegate host B with `0.0.0.0`.

You can copy the following text and paste it in your console:

```
q1="1@${node1}:2888:3888"
q2="2@${node2}:2888:3888"
q3="3@0.0.0.0:2888:3888"
echo "SERVICED_ISVCS_ZOOKEEPER_QUORUM=${q1},${q2},${q3}" \
>> /etc/default/serviced
```

- 6** Specify the timeout for inactive connections.
You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK_SESSION_TIMEOUT=15" >> /etc/default/serviced
```

- 7** Set the `SERVICED_ISVCS_START` variable, and clean up the Control Center configuration file.
 - a** Open `/etc/default/serviced` in a text editor.
 - b** Locate the line for the `SERVICED_ISVCS_START` variable, and then make a copy of the line, immediately below the original.
 - c** Remove the number sign character (`#`) from the beginning of the line.

- d Delete all but `zookeeper` from its list of values.
 - e Navigate to the end of the file, and cut the line that contains the `SERVICED_ZK` variable declaration at that location.
 - f Locate the original `SERVICED_ZK` variable declaration, and then paste the cut line immediately below it.
 - g Comment the original `SERVICED_ZK` declaration, which references only the master host.
Insert the number sign character (#) immediately in front of the original `SERVICED_ZK` variable.
 - h Navigate to the end of the file, and cut the line that contains the `SERVICED_ISVCS_ZOOKEEPER_ID` variable declaration at that location.
 - i Locate the original `SERVICED_ISVCS_ZOOKEEPER_ID` variable declaration, and then paste the cut line immediately below it.
 - j Navigate to the end of the file, and cut the line that contains the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable declaration at that location.
 - k Locate the original `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable declaration, and then paste the cut line immediately below it.
 - l Navigate to the end of the file, and cut the line that contains the `SERVICED_ZK_SESSION_TIMEOUT` variable declaration at that location.
 - m Locate the original `SERVICED_ZK_SESSION_TIMEOUT` variable declaration, and then paste the cut line immediately below it.
 - n Save the file, and then close the editor.
- 8 Verify the ZooKeeper environment variables.

```
grep -E '^\\b*SERVICED' /etc/default/serviced \
| grep -E '(CS_ZO|_ZK|CS_ST)'
```

The following example shows the environment variables for a delegate host with IP address 198.51.100.137.

Note The value of the `SERVICED_ISVCS_ZOOKEEPER_QUORUM` variable is formatted to fit the available space. The result of the `grep` command shows the variable and value on the same line.

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
SERVICED_ISVCS_START=zookeeper
SERVICED_ISVCS_ZOOKEEPER_ID=3
SERVICED_ISVCS_ZOOKEEPER_QUORUM=1@198.51.100.135:2888:3888,\
2@198.51.100.136:2888:3888,3@0.0.0.0:2888:3888
SERVICED_ZK_SESSION_TIMEOUT=15
```

- 9 Pull the required Control Center ZooKeeper image from the master host.
- a Identify the image to pull.

```
serviced version | grep IsvcsImages
```

Example result:

```
IsvcsImages: [zenoss/serviced-isvcs:v48 zenoss/isvcs-zookeeper:v7]
```

- b Pull the Control Center ZooKeeper image.

Replace *Isvcs-ZK-Image* with the name and version number of the ZooKeeper image from the previous substep:

```
docker pull Isvcs-ZK-Image
```

Starting a ZooKeeper ensemble

Use this procedure to start a ZooKeeper ensemble.

This procedure uses the `nc` utility to query ensemble hosts. If `nc` is not available, you can use `telnet` with [interactive ZooKeeper commands](#).

The window of time for starting a ZooKeeper ensemble is relatively short. The goal of this procedure is to restart Control Center on each ensemble node at about the same time, so that each node can participate in electing the leader.

- 1 Log in to the Control Center master host as `root`, or as a user with superuser privileges.
- 2 In a separate window, log in to the second node of the ZooKeeper ensemble (*Delegate-A*) as `root`, or as a user with superuser privileges.
- 3 In a different window, log in to the third node of the ZooKeeper ensemble (*Delegate-B*) as `root`, or as a user with superuser privileges.
- 4 On all ensemble hosts, stop and start `serviced`.

```
systemctl stop serviced && systemctl start serviced
```

- 5 On the master host, check the status of the ZooKeeper ensemble.

- a Attach to the container of the ZooKeeper service.

```
serviced service attach serviced-isvcs_zookeeper
```

- b Query the master host and identify its role in the ensemble.
Replace *Master* with the hostname or IP address of the master host:

```
{ echo stats; sleep 1; } | nc Master 2181 | grep Mode
```

The result includes `leader` or `follower`.

- c Query delegate host A and identify its role in the ensemble.
Replace *Delegate-A* with the hostname or IP address of delegate host A:

```
{ echo stats; sleep 1; } | nc Delegate-A 2181 | grep Mode
```

- d Query delegate host B and identify its role in the ensemble.
Replace *Delegate-B* with the hostname or IP address of delegate host B:

```
{ echo stats; sleep 1; } | nc Delegate-B 2181 | grep Mode
```

- e Detach from the container of the ZooKeeper service.

```
exit
```

If none of the hosts reports that it is the ensemble leader within a few minutes of starting `serviced`, reboot the hosts.

Updating delegate hosts

The default configuration of delegate hosts sets the value of the `SERVICED_ZK` variable to the master host only. Use this procedure to update the setting to include all of the hosts in the ZooKeeper ensemble. Perform this procedure on each delegate host in a Control Center cluster that is not an ensemble node.

- 1 Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2 Define the IP address variables for each node in the ZooKeeper ensemble.

Replace *Master* with the IP address or hostname of the Control Center master host, and replace *Delegate-A* and *Delegate-B* with the IP addresses or hostnames of the delegate hosts to include in the ensemble:

```
node1=Master
node2=Delegate-A
node3=Delegate-B
```

3 Specify the nodes in the ZooKeeper ensemble.

You can copy the following text and paste it in your console:

```
echo "SERVICED_ZK=${node1}:2181,${node2}:2181,${node3}:2181" \
>> /etc/default/serviced
```

4 Update the variable.

- a** Open `/etc/default/serviced` in a text editor.
- b** Navigate to the end of the file, and cut the line that contains the `SERVICED_ZK` variable declaration at that location.
The value of this declaration specifies three endpoints.
- c** Locate the `SERVICED_ZK` variable near the beginning of the file, and then delete the line it is on.
The value is just the master host endpoint.
- d** Paste the `SERVICED_ZK` variable declaration from the end of the file in the location of the just-deleted declaration.
- e** Save the file, and then close the editor.

5 Verify the setting.

```
grep -E '^\b*SERVICED_ZK' /etc/default/serviced
```

The following example shows the environment variable for a delegate host that is not a node in the ZooKeeper ensemble:

```
SERVICED_ZK=198.51.100.135:2181,198.51.100.136:2181,198.51.100.137:2181
```

6 Restart Control Center.

```
systemctl restart serviced
```


Starting and stopping Control Center deployments

A

This appendix includes procedures for stopping and starting both single-host and multi-host Control Center deployments.

Note The procedures in this appendix assume that Control Center is the only source of Docker Engine containers that are run on a host.

Stopping Control Center (single-host deployment)

Use this procedure to stop the Control Center service (*serviced*) in a single-host deployment.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Identify the top-level service *serviced* is managing.

```
serviced service list
```

The top-level service is the service listed immediately below the headings line.

- 3 Stop the top-level service.
Replace *Service* with the name or identifier of the top-level service:

```
serviced service stop Service
```

- 4 Monitor the stop.

```
serviced service status
```

When the status of the top-level service and all child services is `stopped`, proceed to the next step.

- 5 Stop the Control Center service.

```
systemctl stop serviced
```

- 6 Ensure that no containers remain in the local repository.
 - a List all containers.

```
docker ps -a
```

Containers in `Exited` status must be removed.

- b** Remove all remaining containers.

```
docker ps -qa | xargs --no-run-if-empty docker rm -fv
```

- c** Determine whether any containers remain.

```
docker ps -a
```

If containers are still present, perform the following substeps.

- d** Disable the automatic startup of `serviced`.

```
systemctl disable serviced
```

- e** Reboot the host.

```
reboot
```

- f** Log in to the master host as `root`, or as a user with superuser privileges.

- g** Enable the automatic startup of `serviced`.

```
systemctl enable serviced
```

Starting Control Center (single-host deployment)

Use this procedure to start Control Center in a single-host deployment. The default configuration of the Control Center service (`serviced`) is to start when the host starts. This procedure is only needed after stopping `serviced` to perform maintenance tasks.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Determine whether `serviced` is configured to start when the system starts.

```
systemctl is-enabled serviced
```

- If the result is `enabled`, proceed to the next step.
- If the result is `disabled`, enter the following command:

```
systemctl enable serviced
```

- 3 Start the Control Center service.

```
systemctl start serviced
```

- 4 Optional: Monitor the startup, if desired.

```
journalctl -uf serviced -o cat
```

Once Control Center is started, it is ready to start managing applications. For more information, refer to the documentation of your application.

Stopping Control Center (multi-host deployment)

To stop Control Center in a multi-host deployment, perform the procedures in this section, in order.

Stopping a master host (multi-host deployment)

Use this procedure to stop the Control Center service (`serviced`) on the master host in a multi-host deployment.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Identify the top-level service `serviced` is managing.

```
serviced service status
```

The top-level service is the service listed immediately below the headings line.

- 3 Stop the top-level service.
Replace *Service* with the name or identifier of the top-level service:

```
serviced service stop Service
```

- 4 Monitor the stop.

```
serviced service status
```

When the status of the top-level service and all child services is `stopped`, proceed to the next step.

- 5 Stop the Control Center service.

```
systemctl stop serviced
```

- 6 Ensure that no containers remain in the local repository.
 - a Display the identifiers of all containers, running and exited.

```
docker ps -qa
```

- If the command returns no result, stop. This procedure is complete.
 - If the command returns a result, perform the following substeps.
- b Remove all remaining containers.

```
docker ps -qa | xargs --no-run-if-empty docker rm -fv
```

- c Display the identifiers of all containers, running and exited.

```
docker ps -qa
```

- If the command returns no result, stop. This procedure is complete.
 - If the command returns a result, perform the remaining substeps.
- d Disable the automatic startup of `serviced`.

```
systemctl disable serviced
```

- e Reboot the host.

```
reboot
```

- f Log in to the master host as `root`, or as a user with superuser privileges.
- g Enable the automatic startup of `serviced`.

```
systemctl enable serviced
```

Stopping a delegate host (multi-host deployment)

Use this procedure to stop the Control Center service (`serviced`) on a delegate host in a multi-host deployment. Repeat this procedure on each delegate host in your deployment.

- 1 Log in to the delegate host as `root`, or as a user with superuser privileges.
- 2 Stop the Control Center service.

```
systemctl stop serviced
```

- 3 Ensure that no containers remain in the local repository.

- a Display the identifiers of all containers, running and exited.

```
docker ps -qa
```

- If the command returns no result, proceed to the next step.
 - If the command returns a result, perform the following substeps.
 - b Remove all remaining containers.

```
docker ps -qa | xargs --no-run-if-empty docker rm -fv
```

- If the remove command completes, proceed to the next step.
 - If the remove command does not complete, the most likely cause is an NFS conflict. Perform the following substeps.
 - c Stop the NFS and Docker Engine services.

```
systemctl stop nfs && systemctl stop docker
```

- d Start the NFS and Docker Engine services.

```
systemctl start nfs && systemctl start docker
```

- e Repeat the attempt to remove all remaining containers.

```
docker ps -qa | xargs --no-run-if-empty docker rm -fv
```

- If the remove command completes, proceed to the next step.
 - If the remove command does not complete, perform the remaining substeps.
 - f Disable the automatic startup of `serviced`.

```
systemctl disable serviced
```

- g Reboot the host.

```
reboot
```

- h Log in to the delegate host as `root`, or as a user with superuser privileges.
 - i Enable the automatic startup of `serviced`.

```
systemctl enable serviced
```

- 4 Dismount all filesystems mounted from the Control Center master host.

This step ensures no stale mounts remain when the storage on the master host is replaced.

- a** Identify filesystems mounted from the master host.

```
awk '/serviced/ { print $1, $2 }' < /proc/mounts
```

- If the preceding command returns no result, stop. This procedure is complete.
 - If the preceding command returns a result, perform the following substeps.
- b** Force the filesystems to dismount.

```
for FS in $(awk '/serviced/ { print $2 }' < /proc/mounts)
do
    umount -f $FS
done
```

- c** Identify filesystems mounted from the master host.

```
awk '/serviced/ { print $1, $2 }' < /proc/mounts
```

- If the preceding command returns no result, stop. This procedure is complete.
 - If the preceding command returns a result, perform the following substeps.
- d** Perform a lazy dismount.

```
for FS in $(awk '/serviced/ { print $2 }' < /proc/mounts)
do
    umount -f -l $FS
done
```

- e** Restart the NFS service.

```
systemctl restart nfs
```

- f** Determine whether any filesystems remain mounted.

```
awk '/serviced/ { print $1, $2 }' < /proc/mounts
```

- If the preceding command returns no result, stop. This procedure is complete.
 - If the preceding command returns a result, perform the remaining substeps.
- g** Disable the automatic startup of serviced.

```
systemctl disable serviced
```

- h** Reboot the host.

```
reboot
```

- i** Log in to the delegate host as `root`, or as a user with superuser privileges.
- j** Enable the automatic startup of serviced.

```
systemctl enable serviced
```

Starting Control Center (multi-host deployment)

Use this procedure to start Control Center in a multi-host deployment. The default configuration of the Control Center service (`serviced`) is to start when the host starts. This procedure is only needed after stopping `serviced` to perform maintenance tasks.

- 1 Log in to the master host as `root`, or as a user with superuser privileges.
- 2 Determine whether `serviced` is configured to start when the system starts.

```
systemctl is-enabled serviced
```

- If the result is `enabled`, proceed to the next step.
- If the result is `disabled`, enter the following command:

```
systemctl enable serviced
```

- 3 Identify the hosts in the ZooKeeper ensemble.

```
grep -E '^\\b*SERVICED_ZK=' /etc/default/serviced
```

The result is a list of 3 or 5 hosts, separated by the comma character (,). The master host is always a node in the ZooKeeper ensemble.

- 4 In separate windows, log in to each of the delegate hosts that are nodes in the ZooKeeper ensemble as `root`, or as a user with superuser privileges.
- 5 On all ensemble hosts, start `serviced`.

The window of time for starting a ZooKeeper ensemble is relatively short. The goal of this step is to start Control Center on each ensemble node at about the same time, so that each node can participate in electing the leader.

```
systemctl start serviced
```

- 6 On the master host, check the status of the ZooKeeper ensemble.
 - a Attach to the container of the ZooKeeper service.

```
serviced service attach serviced-isvcs_zookeeper
```

- b Query the master host and identify its role in the ensemble.
Replace *Master* with the hostname or IP address of the master host:

```
{ echo stats; sleep 1; } | nc Master 2181 | grep Mode
```

The result includes `leader` or `follower`.

- c Query the other delegate hosts to identify their role in the ensemble.
Replace *Delegate* with the hostname or IP address of a delegate host:

```
{ echo stats; sleep 1; } | nc Delegate 2181 | grep Mode
```

- d Detach from the container of the ZooKeeper service.

```
exit
```

If none of the nodes reports that it is the ensemble leader within a few minutes of starting `serviced`, reboot the ensemble hosts.

- 7 Log in to each of the delegate hosts that are not nodes in the ZooKeeper ensemble as `root`, or as a user with superuser privileges, and then start `serviced`.

```
systemctl start serviced
```

- 8 Optional: Monitor the startup, if desired.

```
journalctl -uf serviced -o cat
```

Once Control Center is started, it is ready to start managing applications. For more information, refer to the documentation of your application.

B

Storage management utility

This appendix includes a description of the `serviced-storage` command, the required utility for creating the Docker thin pool and creating and managing the Control Center application data thin pool.

serviced-storage

The `serviced-storage` command manages Control Center storage.

USAGE

Use this command to create LVM thin pools for Docker Engine and Control Center.

SYNTAX

```
serviced-storage [-h|--help] [-o DeviceMapperOption=Value] \
  [-v] Command [CommandOptions]
```

GLOBAL OPTIONS

--help, -h

Shows the help information.

-o *DeviceMapperOption=Value*

A device mapper option. Applies only to device mapper drivers.

-v

Displays verbose logging.

COMMANDS

check

Check for orphaned devices.

create

Create a volume on a driver.

create-thin-pool

Create an LVM thin pool.

disable

Disable a driver.

init

Initialize a driver.

list

Print volumes on a driver.

mount

Mount an existing volume from a driver.

remove

Remove an existing volume from a driver.

resize

Resize an existing volume.

set

Set the default driver.

status

Print the driver status

sync

Sync data from a volume to another volume.

unset

Unset the default driver.

version

Print the version and exit.

serviced-storage check

The `serviced-storage check` command searches for orphaned snapshot devices in the `serviced` application data thin pool and removes them, if requested. This command requires the path of `serviced` tenant volumes, which is determined by the `SERVICED_VOLUMES_PATH` variable in `/etc/default/serviced`. The default path is `/opt/serviced/var/volumes`.

Syntax:

```
serviced-storage [GlobalOptions] check [-c|--clean] Path
```

Command options:

[-c|--clean]

Remove orphaned snapshot devices.

serviced-storage create-thin-pool

The `serviced-storage create-thin-pool` command creates an LVM thin pool either for Docker data or for Control Center application data. When devices are specified, the command creates an LVM volume group.

Syntax:

```
serviced-storage [GlobalOptions] create-thin-pool \
  [-s|--size]=[Value][G|%] [docker|serviced] \
  [DevicePath [DevicePath...] | VolumeGroupName]
```

Command options:

`[-s|--size]=[Value][G|%]`

The size of the thin pool to create. The size can be a fixed value (in gigabytes) or a relative value (a percentage) of the available storage. When this option is not used, the thin pool size defaults to 90% of the specified storage resource.

serviced-storage resize

The `serviced-storage resize` command increases the size of a serviced tenant device in its LVM thin pool. Like LVM thin pools, the size of a serviced tenant device can never decrease.

Syntax:

```
serviced-storage [GlobalOptions] resize \
  [-d|--driver]=Value TenantID NewSize
```

Command options:

`[-d|--driver]=Value`

The path of the tenant volume.

EXAMPLES

Create an LVM volume group named `zenoss` and use it for both thin pools:

```
vgcreate zenoss /dev/sdb /dev/sdc
serviced-storage create-thin-pool --size=50G docker zenoss
serviced-storage create-thin-pool --size=50% serviced zenoss
```

If you specify devices or partitions, `serviced-storage` creates an LVM volume group with the same name as the thin pool. The following example yields the same result as the previous, except the name of the volume group is `docker` instead of `zenoss`:

```
serviced-storage create-thin-pool --size=50G docker /dev/sdb /dev/sdc
serviced-storage create-thin-pool --size=50% serviced docker
```

Create thin pools on separate block devices:

```
serviced-storage create-thin-pool --size=50G docker /dev/sdb
serviced-storage create-thin-pool --size=200G serviced /dev/sdc
```

Create thin pools on separate partitions:

```
serviced-storage create-thin-pool --size=50% docker /dev/sdb1
serviced-storage create-thin-pool serviced /dev/sdc3
```

Increase the size of the `serviced` LVM thin pool, and then increase the size of a serviced tenant device.

```
lvextend -L+300G zenoss/serviced-pool
serviced-storage -o dm.thinpooldev=/dev/mapper/zenoss-serviced--pool \
  resize -d /opt/serviced/var/volumes 58uuetj38draeu9alp6002b1y 200G
```

Identify the `serviced` application data thin pool, and then remove orphaned snapshot devices.

```
ls /dev/mapper | grep serviced  
serviced-storage -o dm.thinpooldev=/dev/mapper/zenoss-serviced--pool \  
check -c /opt/serviced/var/volumes
```



Control Center configuration variables

This appendix includes recommended best practices for editing the `serviced` configuration file, and descriptions of the variables in the file.

Best practices for configuration files

The Control Center configuration file, `/etc/default/serviced`, contains Bash environment variables that are read by the `serviced` daemon startup script. The following list describes recommended best practices for its use and maintenance:

- 1 When in doubt, make a backup. Making a backup copy of the configuration file before editing it is always the safest choice.
- 2 Copy a variable, then edit the copy. If you need to revert a variable to its default value, you don't have to leave the file to look it up.
- 3 Put the first character of the variable declaration in the first column of its line. It's easier to `grep` for settings when each one starts a line.
- 4 Add customizations to the top of the file. Customizations at the end of the file or scattered throughout the file can be overlooked.

Control Center configuration file

The Control Center configuration file, `/etc/default/serviced`, contains Bash environment variables that are read by the `serviced` daemon startup script. The order of the following list matches the order of the variables in the file.

Note All of the environment variables declared in this file are available to all of the containers that `serviced` manages. You can add any valid Bash shell variable to this file for application containers to use. For compatibility, please avoid variables that begin with `SERVICED`.

HOME

Default: (the value of shell variable `HOME`)

The path Docker Engine clients use to locate the `.dockercfg` authentication file, which contains Docker Hub credentials.

TMPDIR

Default: (the value of shell variable `TMPDIR`)

The path `serviced` uses for temporary files.

GOMAXPROCS**Default:** 2The maximum number of CPU cores `serviced` uses.**SERVICED_MASTER****Default:** 1 (true)

Assigns the role of a `serviced` instance, either master or delegate. The master runs the application services scheduler and other internal services. Delegates run the application services assigned to the resource pool to which they belong.

Only one `serviced` instance can be the master; all other instances must be delegates. The default value assigns the master role. To assign the delegate role, set the value to 0 (false). This variable must be explicitly set on all Control Center cluster hosts.

SERVICED_MASTER_IP**Default:** 127.0.0.1

A convenience variable, for use in places where the IP address or hostname of the master host is required. This variable is unused unless it is both set here and referenced elsewhere. (For example, by replacing `{{SERVICED_MASTER_IP}}` with `$SERVICED_MASTER_IP`.)

SERVICED_MASTER_POOLID**Default:** defaultThe name of the default resource pool. This variable is only used the first time `serviced` is started.**SERVICED_ZK****Default:** (none)

The list of endpoints in the `serviced` ZooKeeper ensemble, separated by the comma character (,). Each endpoint identifies an ensemble node.

SERVICED_DOCKER_REGISTRY**Default:** `{{SERVICED_MASTER_IP}}:5000`

The endpoint of the `serviced` Docker registry host. On delegate hosts, replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the registry host, which by default is the `serviced` master host.

SERVICED_OUTBOUND_IP**Default:** (none)

The default startup routines of `serviced` include attempting to ping `google.com`. When a value is set for this variable, `serviced` does not attempt the ping and assumes it does not have internet access.

Use this variable to specify the IP address of a network interface other than the default, or to prevent `serviced` from assuming it has internet access.

Note Setting the Docker `HTTP_PROXY` or `HTTPS_PROXY` environment variables prevents access to the IP address defined with this variable. To enable access, unset the Docker variables, and then reboot the host.

SERVICED_STATIC_IPS**Default:** (none)

A list of one or more static IP addresses that are available for IP assignment. Use the comma character (,) to separate addresses.

SERVICED_ENDPOINT**Default:** `{{SERVICED_MASTER_IP}}:4979`

The endpoint of the `serviced` RPC server. Replace `{{SERVICED_MASTER_IP}}` with the IP address or hostname of the `serviced` master host. The port number of this endpoint must match the value of the `SERVICED_RPC_PORT` variable defined on the `serviced` master host.

SERVICED_MAX_RPC_CLIENTS**Default:** 3

The preferred maximum number of simultaneous connections a `serviced` delegate uses for RPC requests. The value is used to create a pool of sockets, which are reused as needed. Increasing the value increases the number of open sockets and the use of socket-related operating system resources.

When the demand for connections exceeds the supply of open sockets, `serviced` opens more sockets.

When demand eases, `serviced` reduces the number of open sockets to the preferred maximum.

SERVICED_RPC_PORT**Default:** 4979

The port on which the `serviced` RPC server listens for connections. The value of this variable must match the port number defined for the `SERVICED_ENDPOINT` variable on all `serviced` delegate hosts.

SERVICED_RPC_CERT_VERIFY**Default:** false

Determines whether `serviced` performs TLS certificate verification for RPC connections. The certificate is defined by the `SERVICED_CERT_FILE` variable.

SERVICED_RPC_DISABLE_TLS**Default:** false

Determines whether `serviced` encrypts RPC traffic with TLS.

SERVICED_RPC_TLS_MIN_VERSION**Default:** VersionTLS10

The minimum version of TLS `serviced` accepts for RPC connections. Valid values include the default, VersionTLS11, and VersionTLS12.

SERVICED_RPC_TLS_CIPHERS**Default:** (list of ciphers)

The list of TLS ciphers `serviced` prefers for RPC connections, separated by the comma character (,):

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Other ciphers are supported; the preceding ciphers provide strong security for relatively low processing overhead.

An instance of `serviced` is on both ends of an RPC connection, so both daemons use the first cipher in the list. To use a different cipher, put it first in the list, on all cluster hosts.

SERVICED_UI_PORT**Default:** :443

The port on which the HTTP server listens for requests. The value may be expressed as follows:

- *IP-Address:Port-Number*
- *:Port-Number*
- *Port-Number*

All Control Center cluster hosts must have the same value for this variable.

SERVICED_UI_POLL_FREQUENCY**Default:** 3

The number of seconds between polls from Control Center browser interface clients. The value is included in a JavaScript library that is sent to the clients.

SERVICED_MUX_PORT**Default:** 22250The port `serviced` uses for traffic among Docker containers.***SERVICED_MUX_DISABLE_TLS*****Default:** 0

Determines whether inter-host traffic among Docker containers is encrypted with TLS. Intra-host traffic among Docker containers is not encrypted. To disable encryption, set the value to 1.

SERVICED_MUX_TLS_MIN_VERSION**Default:** `VersionTLS10`The minimum version of TLS `serviced` accepts for mux traffic. Valid values include the default, `VersionTLS11`, and `VersionTLS12`.***SERVICED_MUX_TLS_CIPHERS*****Default:** (list of ciphers)The list of TLS ciphers `serviced` prefers for mux traffic, separated by the comma character (,):

- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`

Other ciphers are supported; the preceding ciphers provide strong security for relatively low processing overhead.

An instance of `serviced` is on both ends of a mux connection, so both daemons use the first cipher in the list. To use a different cipher, put it first in the list, on all cluster hosts.***SERVICED_ISVCS_PATH*****Default:** `/opt/serviced/var/isvcs`The location of `serviced` internal services data.***SERVICED_VOLUMES_PATH*****Default:** `/opt/serviced/var/volumes`The location of `serviced` application data.***SERVICED_BACKUPS_PATH*****Default:** `/opt/serviced/var/backups`The location of `serviced` backup files.***SERVICED_KEY_FILE*****Default:** `$TMPDIR/zenoss_key.[0-9]+`The path of a digital certificate key file. Choose a location that is not modified during operating system updates, such as `/etc`.This key file is used for all TLS-encrypted communications (RPC, mux, and HTTP). The default, insecure key file is created when the `serviced` web server first starts, and is based on a public key that is compiled into `serviced`.***SERVICED_CERT_FILE*****Default:** `$TMPDIR/zenoss_cert.[0-9]+`The path of a digital certificate file. Choose a location that is not modified during operating system updates, such as `/etc`. Certificates with passphrases are not supported.This certificate file is used for all TLS-encrypted communications (RPC, mux, and HTTP). The default, insecure certificate file is created when the `serviced` web server first starts, and is based on a public certificate that is compiled into `serviced`.

SERVICED_TLS_MIN_VERSION**Default:** VersionTLS10

The minimum version of TLS that `serviced` accepts for HTTP traffic. Valid values include the default, VersionTLS11, and VersionTLS12.

SERVICED_TLS_CIPHERS**Default:** (list of ciphers)

The list of TLS ciphers that `serviced` accepts for HTTP traffic, separated by the comma character (,):

- 1 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- 3 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 4 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 5 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- 6 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- 7 TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- 8 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- 9 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- 10 TLS_RSA_WITH_AES_256_CBC_SHA
- 11 TLS_RSA_WITH_AES_128_CBC_SHA
- 12 TLS_RSA_WITH_3DES_EDE_CBC_SHA
- 13 TLS_RSA_WITH_RC4_128_SHA
- 14 TLS_RSA_WITH_AES_128_GCM_SHA256
- 15 TLS_RSA_WITH_AES_256_GCM_SHA384
- 16 TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- 17 TLS_ECDHE_RSA_WITH_RC4_128_SHA

To disable support for most ciphers, you can remove them from the list. The following rules apply to the list:

- The first cipher, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, must always be present in the list of ciphers.
- The first four ciphers in the list must always precede any of the ciphers that appear after the first four. The first four ciphers are valid for HTTP/2, while the remaining ciphers are not.

SERVICED_FS_TYPE**Default:** devicemapper

The driver to manage application data storage on the `serviced` master host. Only `devicemapper` is supported in production deployments.

The only supported storage layout for the `devicemapper` driver is an LVM thin pool. To create a thin pool, use the `serviced-storage` utility. To specify the name of the thin pool device, use the `SERVICED_DM_THINPOOLDEV` variable.

SERVICED_DM_ARGS**Default:** (none)

Customized startup arguments for the `devicemapper` storage driver.

SERVICED_DM_BASESIZE**Default:** 100G

The base size of virtual storage devices for tenants in the application data thin pool, in gigabytes. The units symbol (G) is required. This variable is used when `serviced` starts for the first time, to set the initial size of tenant devices, and when a backup is restored, to set the size of the restored tenant device.

The base size device is sparse device that occupies at most 1MB of space in the application data thin pool; its size has no immediate practical impact. However, the application data thin pool should have enough

space for twice the size of each tenant device it supports, to store both the data itself and snapshots of the data. Since the application data thin pool is an LVM logical volume, its size can be increased at any time. Likewise, the size of a tenant device can be increased, as long as the available space in the thin pool can support the larger tenant device plus snapshots.

SERVICED_DM_LOOPDATASIZE

Default: 100G

Specifies the size of the data portion of the loop-back file. This setting is ignored when *SERVICED_ALLOW_LOOP_BACK* is false.

SERVICED_DM_LOOPMETADATASIZE

Default: 2G

Specifies the size of the metadata portion of the loop-back file. This setting is ignored when *SERVICED_ALLOW_LOOP_BACK* is false.

SERVICED_DM_THINPOOLDEV

Default: (none)

The name of the thin pool device to use with the `devicemapper` storage driver.

SERVICED_STORAGE_STATS_UPDATE_INTERVAL

Default: 300 (5 minutes)

The number of seconds between polls of kernel statistics about the application data thin pool.

This setting is ignored when the operating system kernel version is less than 3.10.0-366.

SERVICED_ALLOW_LOOP_BACK

Default: false

Determines whether loop-back files can be used with the `devicemapper` storage driver. This option is not supported for production use.

SERVICED_MAX_CONTAINER_AGE

Default: 86400 (24 hours)

The number of seconds `serviced` waits before removing a stopped container.

SERVICED_VIRTUAL_ADDRESS_SUBNET

Default: 10.3.0.0/16

The private subnet for containers that use virtual IP addresses on a host. This value may be unique on each cluster host, if necessary.

RFC 1918 restricts private networks to the 10.0/24, 172.16/20, and 192.168/16 address spaces. However, `serviced` accepts any valid IPv4 address space.

Specify the value in CIDR notation. A /29 network provides sufficient address space.

SERVICED_LOG_LEVEL

Default: 0

The log level `serviced` uses when writing to the system log. Valid values are 0 (normal) and 2 (debug).

SERVICED_LOG_ADDRESS

Default: {{SERVICED_MASTER_IP}}:5042

The endpoint of the logstash service. Replace {{SERVICED_MASTER_IP}} with the IP address or hostname of the `serviced` master host.

SERVICED_LOGSTASH_ES

Default: {{SERVICED_MASTER_IP}}:9100

The endpoint of the logstash Elasticsearch service. On delegate hosts, replace {{SERVICED_MASTER_IP}} with the IP address or hostname of the Elasticsearch host, which by default is the `serviced` master host.

SERVICED_LOGSTASH_MAX_DAYS**Default:** 14

The maximum number of days to keep application logs in the logstash database before purging them.

SERVICED_LOGSTASH_MAX_SIZE**Default:** 10

The maximum size of the logstash database, in gigabytes.

SERVICED_LOGSTASH_CYCLE_TIME**Default:** 6

The amount of time between logstash purges, in hours.

SERVICED_STATS_PORT**Default:** {{SERVICED_MASTER_IP}}:8443The endpoint of the `serviced` metrics consumer service. Replace {{SERVICED_MASTER_IP}} with the IP address or hostname of the `serviced` master host.***SERVICED_STATS_PERIOD*****Default:** 10The frequency, in seconds, at which delegates gather metrics to send to the `serviced` metrics consumer service on the master host.***SERVICED_SVCSTATS_CACHE_TIMEOUT*****Default:** 5

The number of seconds to cache statistics about services. The cache is used by Control Center browser interface clients.

SERVICED_DEBUG_PORT**Default:** 6006The port on which `serviced` listens for HTTP requests for the [Go profiler](#). To stop listening for requests, set the value to `-1`.***SERVICED_ISVCS_ENV_[0-9]+*****Default:** (none)

Startup arguments to pass to internal services. You may define multiple arguments, each for a different internal service. The variables themselves, and their arguments, use the following syntax:

SERVICED_ISVCS_ENV_%dEach variable name ends with a unique integer in place of `%d`.***Service-Name:Key=Value***

The value of each variable includes the following elements, in order:

- 1 *Service-Name*, the internal service name. The following command returns the internal service names that may be used for *Service-Name*:

```
docker ps | awk '/serviced-isvcs:/{print $NF}'
```

- 2 The colon character (`:`).
- 3 *Key*, a variable to pass to the internal service.
- 4 The equals sign character (`=`).
- 5 *Value*, the definition of the variable to pass to the internal service.

The following example variable passes `ES_JAVA_OPTS=-Xmx4g` to the Elasticsearch internal service.

```
SERVICED_ISVCS_ENV_0=serviced-isvcs_elasticsearch-  
logstash:ES_JAVA_OPTS=-Xmx4g
```

SERVICED_ADMIN_GROUP

Default: wheel

The name of the Linux group on the `serviced` master host whose members are authorized to use the `serviced` browser interface. You may replace the default group with a group that does not have superuser privileges.

SERVICED_ALLOW_ROOT_LOGIN

Default: 1 (true)

Determines whether the `root` user account on the `serviced` master host may be used to gain access to the `serviced` browser interface.

SERVICED_IPTABLES_MAX_CONNECTIONS

Default: 655360

The default value of this variable ensures that a `serviced` delegate does not run out of connections if the `serviced` master goes down. The connections are automatically cleaned up by the kernel soon after the `serviced` master comes back online.

SERVICED_SNAPSHOT_TTL

Default: 12

The number of hours an application data snapshot is retained before removal. To disable snapshot removal, set the value to zero. The application data storage can fill up rapidly when this value is zero or too high.

SERVICED_NFS_CLIENT

Default: 1

DEPRECATED: Prevent a delegate host from mounting the DFS.

SERVICED_SERVICE_MIGRATION_TAG

Default: 1.0.2

Overrides the default value for the service migration image.

SERVICED_ISVCS_START

Default: (none)

Enables one or more internal services to run on a delegate host. Currently, only `zookeeper` is supported.

SERVICED_ISVCS_ZOOKEEPER_ID

Default: (none)

The unique identifier of a ZooKeeper ensemble node. The identifier must be a positive integer.

SERVICED_ISVCS_ZOOKEEPER_QUORUM

Default: (none)

The comma-separated list of nodes in a ZooKeeper ensemble. Each entry in the list specifies the ZooKeeper ID, IP address or hostname, peer communications port, and leader communications port of a node in the ensemble. Each quorum definition must be unique, so the IP address or hostname of the "current" host must be 0.0.0.0.

The following example shows the syntax of a node entry:

```
ZooKeeper-ID@Host-IP-Or-Name:2888:3888
```

SERVICED_DOCKER_LOG_DRIVER

Default: json-file

The log driver for all Docker container logs, including containers for Control Center internal services. Valid values:

- json-file
- syslog
- journald
- gelf
- fluentd
- none

This is a direct port of the Docker `--log-driver` option.

SERVICED_DOCKER_LOG_CONFIG

Default: `max-file=5,max-size=10m`

A comma-separated list of Docker `--log-opt` options as *key=value* pairs. To specify the default values for a log driver, or for drivers that need no additional options, such as `journald`, use a single comma character (,) as the value of this variable.

SERVICED_DOCKER_DNS

Default: (empty)

The IP address of one or more DNS servers. The value of this variable is injected into each Docker Engine container that `serviced` starts. Separate multiple values with the comma character (,).

SERVICED_OPTS

Default: (empty)

Special options for the `serviced` startup command.

SERVICED_SNAPSHOT_USE_PERCENT

Default: 20

The amount of free space in the thin pool specified with `SERVICED_DM_THINPOOLDEV`, expressed as a percentage the total size. This value is used to determine whether the thin pool can hold a new snapshot.

SERVICED_ZK_SESSION_TIMEOUT

Default: 15

The number of seconds the ZooKeeper leader waits before flushing an inactive connection.

SERVICED_ES_STARTUP_TIMEOUT

Default: 240

The number of seconds to wait for the Elasticsearch service to start.

SERVICED_MAX_DFS_TIMEOUT

Default: 300

The number of seconds until a DFS snapshot attempt times out.

SERVICED_RPC_DIAL_TIMEOUT

Default: 30

The number of seconds until an RPC connection attempt times out.

SERVICED_AUTH_TOKEN_EXPIRATION

Default: 3600 (1 hour)

The expiration time, in seconds, of delegate authentication tokens. This timeout affects RPC, mux, and `serviced` internal services endpoint communications.

SERVICED_CONTROLLER_BINARY

Default: `/opt/serviced/bin/serviced-controller`

The path of the `serviced-controller` binary, which runs in every container that `serviced` manages.

SERVICED_HOME

Default: /opt/serviced

The path of the home directory for serviced.

SERVICED_ETC_PATH

Default: /opt/serviced/etc

The path of the directory for serviced configuration files. The default is *SERVICED_HOME*/etc.

SERVICED_VHOST_ALIASES

Default: (none)

A list of hostname aliases for a host; for example, localhost. Separate multiple values with the comma character (,).

Preparing to install without internet access

D

This appendix includes procedures for downloading and installing or staging Control Center software and its operating system dependencies. This distribution option is available only to Zenoss customers, to enable creating Control Center deployments without internet access.

The following table identifies where to perform each procedure in this appendix.

Procedure	Where to perform
Downloading repository and image files on page 78	A workstation with internet access
Installing the repository mirror on page 79	The Control Center master host and all delegate hosts
Staging Docker image archive files on page 79	The Control Center master host

Downloading repository and image files

To perform this procedure, you need:

- A workstation with internet access.
- Permission to download files from the [File Portal - Download Zenoss Enterprise Software](#) site. Zenoss customers may request permission by filing a ticket at the [Zenoss Support](#) site.
- A secure network copy program.

Use this procedure to

- download the required files to a workstation
- copy the files to the hosts that need them

Perform these steps:

- 1 In a web browser, navigate to the [File Portal - Download Zenoss Enterprise Software](#) site.
- 2 Log in with the account provided by Zenoss Support.
- 3 Download the self-installing Docker image files.
Select the files with the highest version number. The version number is represented as *Version* in the following file names:
 - `install-zenoss-isvcs-zookeeper:vVersion.run`
 - `install-zenoss-serviced-isvcs:vVersion.run`

4 Download a RHEL/CentOS repository mirror file.

The download site provides a repository mirror file each supported release of RHEL/CentOS. Each file contains the Control Center package and its dependencies.

To download the correct repository mirror file, match the operating system release number in the file name (`centos7.1` or `centos7.2`) with the version of RHEL/CentOS installed on all of the hosts in your Control Center cluster. Also, choose the file with the highest version number. The version number represented as *Version* in the following file names:

- `yum-mirror-centos7.centos7.1-Version.x86_64.rpm`
- `yum-mirror-centos7.centos7.2-Version.x86_64.rpm`

5 Use a secure copy program to copy the files to Control Center cluster hosts.

- Copy all of the files to the master host.
- Copy the repository mirror (RPM) file to all delegate hosts.

Installing the repository mirror

Use this procedure to install a local RHEL/CentOS repository mirror on a Control Center host. The mirror contains packages that are required on all Control Center cluster hosts, and its size is approximately 55MB.

- 1** Log in to the target host as `root`, or as a user with superuser privileges.
- 2** Copy or move the RPM file to `/tmp`.
- 3** Install the RHEL/CentOS repository mirror.

```
yum install -y /tmp/yum-mirror-*.x86_64.rpm
```

- 4** Optional: Delete the RPM file, if desired.

```
rm /tmp/yum-mirror-*.x86_64.rpm
```

Staging Docker image archive files

Before performing this procedure, verify that approximately 640MB of temporary space is available on the file system where `/root` is located.

Use this procedure to add Docker image archive files to the Control Center master host. The files are used when Docker is fully configured.

- 1** Log in to the master host as `root`, or as a user with superuser privileges.
- 2** Copy or move the archive files to `/root`.
- 3** Add execute permission to the files.

```
chmod +x /root/*.run
```



Configuring a private master NTP server

Control Center requires a common time source. The procedures in this appendix configure a private master [NTP](#) server to synchronize the system clocks of all hosts in a Control Center cluster.

A private master server is only required when a multi-host deployment does not have internet access and no time synchronization servers are available behind the firewall. Single-host deployments do not require time synchronization, and deployments with internet access can rely on the default public time servers that are configured in `/etc/ntp.conf`.

Note VMware vSphere guest systems can synchronize their system clocks with the host system. If that feature is enabled, it must be disabled to configure a private master NTP server or to use a time synchronization server that is available behind the firewall. For more information, refer to the VMware documentation for your version of vSphere.

Configuring an NTP master server

Use this procedure to configure an NTP master server on the Control Center master host. Perform this procedure only if the host does not have internet access.

Note On VMware vSphere guests, disable time synchronization between guest and host operating systems before performing this procedure.

- 1 Log in to the Control Center master host as `root`, or as a user with superuser privileges.
- 2 Create a backup of the NTP configuration file.

```
cp -p /etc/ntp.conf /etc/ntp.conf.orig
```

- 3 Edit the NTP configuration file.
 - a Open `/etc/ntp.conf` with a text editor.
 - b Replace all of the lines in the file with the following lines:

```
# Use the local clock
server 127.127.1.0 prefer
fudge 127.127.1.0 stratum 10
driftfile /var/lib/ntp/drift
broadcastdelay 0.008

# Give localhost full access rights
restrict 127.0.0.1
```



```
# Grant access to client hosts
restrict ADDRESS_RANGE mask NETMASK nomodify notrap
```

- c Replace ADDRESS_RANGE with the range of IPv4 network addresses that are allowed to query this NTP server.

For example, the following IP addresses are assigned to the hosts in an Control Center cluster:

```
203.0.113.10
203.0.113.11
203.0.113.12
203.0.113.13
```

For the preceding addresses, the value for ADDRESS_RANGE is 203.0.113.0.

- d Replace NETMASK with the IPv4 network mask that corresponds with the address range.
For example, a valid network mask for 203.0.113.0 is 255.255.255.0.
- e Save the file and exit the editor.

4 Stop Control Center.

```
systemctl stop serviced
```

5 Enable and start the NTP daemon.

- a Enable the ntpd daemon.

```
systemctl enable ntpd
```

- b Configure ntpd to start when the system starts.

Currently, an unresolved issue associated with NTP prevents ntpd from restarting correctly after a reboot, and the following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
```

- c Start ntpd.

```
systemctl start ntpd
```

6 Start Control Center.

```
systemctl start serviced
```

Configuring NTP clients

Use this procedure to configure a delegate hosts to synchronize its clocks with the NTP server on the Control Center master host. Perform this procedure only if the hosts do not have internet access. Repeat this procedure on each delegate host in your Control Center cluster.

Note On VMware vSphere guests, disable time synchronization between guest and host operating systems before performing this procedure.

- 1 Log in to the Control Center delegate host as `root`, or as a user with superuser privileges.

- 2 Create a backup of the NTP configuration file.

```
cp -p /etc/ntp.conf /etc/ntp.conf.orig
```

- 3 Edit the NTP configuration file./

- a Open `/etc/ntp.conf` with a text editor.
 - b Replace all of the lines in the file with the following lines:

```
# Point to the master time server
server MASTER_ADDRESS

restrict default ignore
restrict 127.0.0.1
restrict MASTER_ADDRESS mask 255.255.255.255 nomodify notrap noquery

driftfile /var/lib/ntp/drift
```

- c Replace both instances of `MASTER_ADDRESS` with the IPv4 address of the host where the NTP server is running (the Control Center master host).
 - d Save the file and exit the editor.

- 4 Stop Control Center.

```
systemctl stop serviced
```

- 5 Synchronize the clock with the master server.

```
ntpdate -gq
```

- 6 Enable and start the NTP daemon.

- a Enable the `ntpd` daemon.

```
systemctl enable ntpd
```

- b Configure `ntpd` to start when the system starts.

Currently, an unresolved issue associated with NTP prevents `ntpd` from restarting correctly after a reboot, and the following commands provide a workaround to ensure that it does.

```
echo "systemctl start ntpd" >> /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local
```

- c Start `ntpd`.

```
systemctl start ntpd
```

- 7 Start Control Center.

```
systemctl start serviced
```