Table of Contents

1 Appliance fails to boot after power outage

2 Overview

This article describes how to recover from an unclean shut down of a Swivel hardware or VM appliance. An unclean shut down can occur as a result of a power outage.

3 Symptoms

The symptom of failing to boot can include prevention of startup, due to an fsck disk check request. It can also include a very rapid (abnormal) boot sequence which leads to a prompt where you are asked for a root password.

In both instances you need to follow the instructions below to perform an fsck of the partitions.

Remote access to the Swivel hardware appliances can be made using the DRAC, see DRAC Card How To Guide

4 Solution

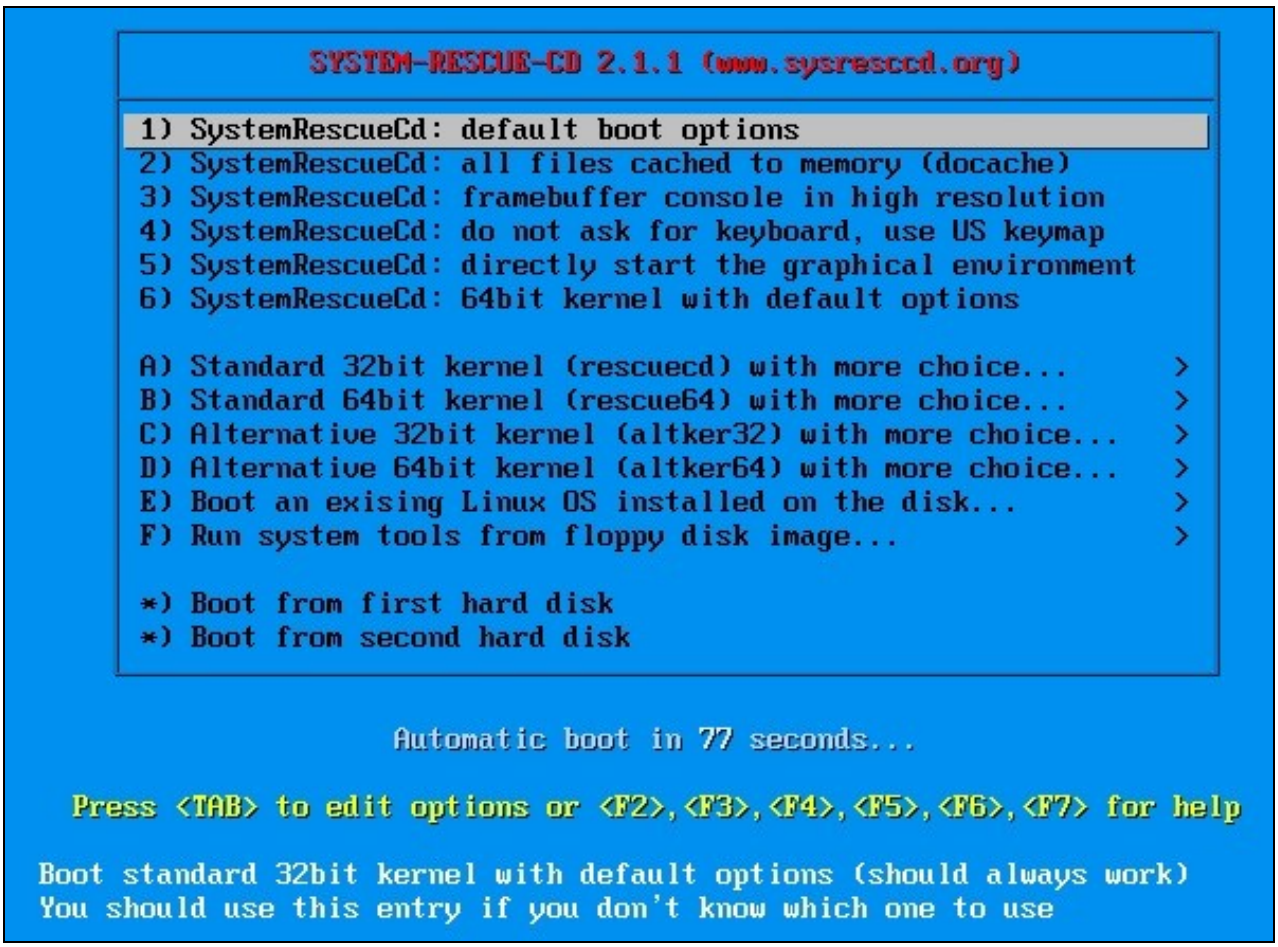
4.1 Boot from the Sysrescue CD

Our recommended method for performing a fsck is by downloading the free sysrescuecd.

This can be obtained from http://www.sysresccd.org, select downloads and then follow the link to download, this will usually be an iso image which for Swivel hardware appliances can be burnt to a CD from the image. VM's should be able to mount the iso image as CD and allow the image to be booted from CD, the boot from CD option may need to be selected for the Swivel server.

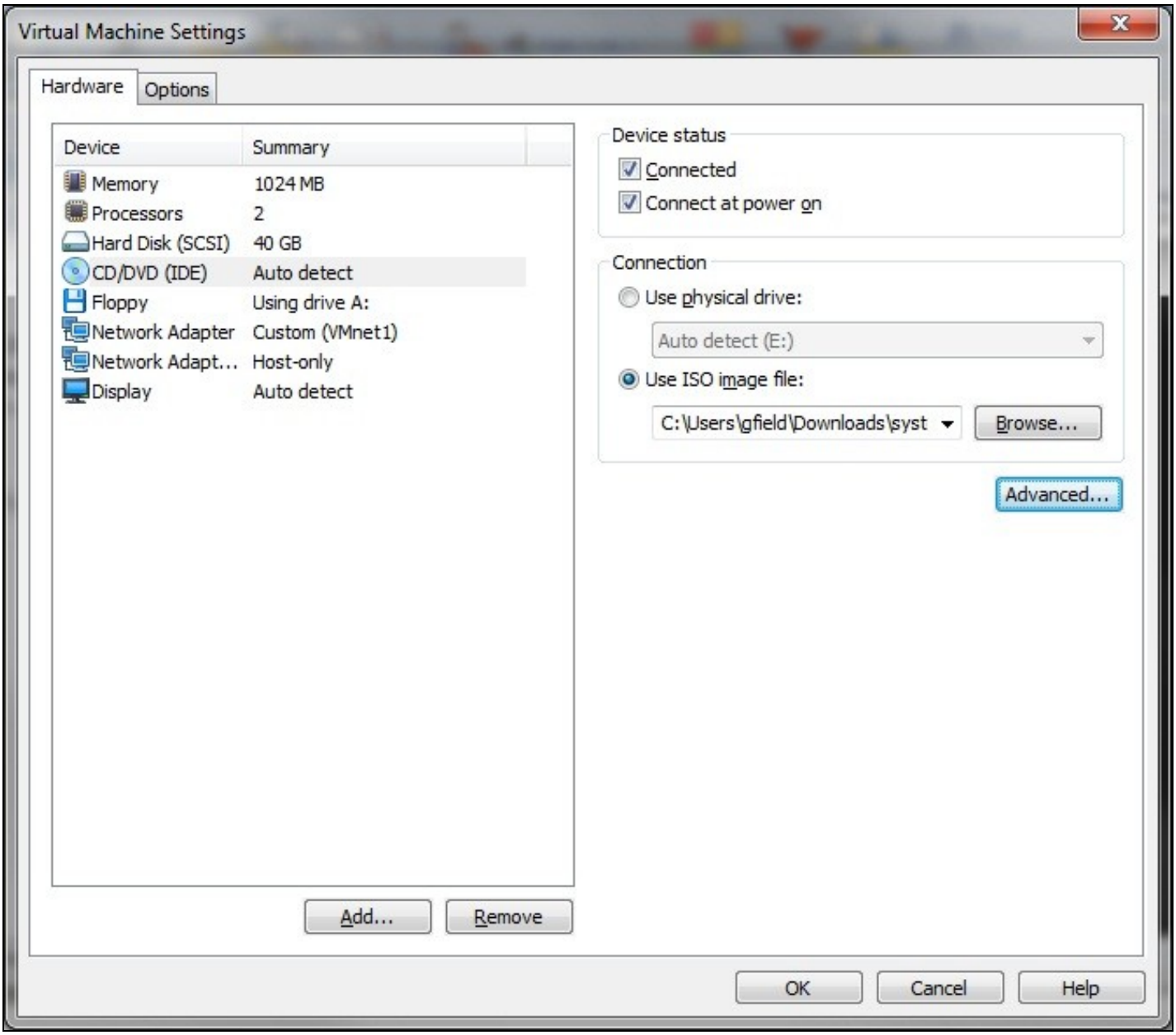
You do not need a root password using this method. Its also a requirement that the filesystem is not mounted by the operating systems when you scan it.

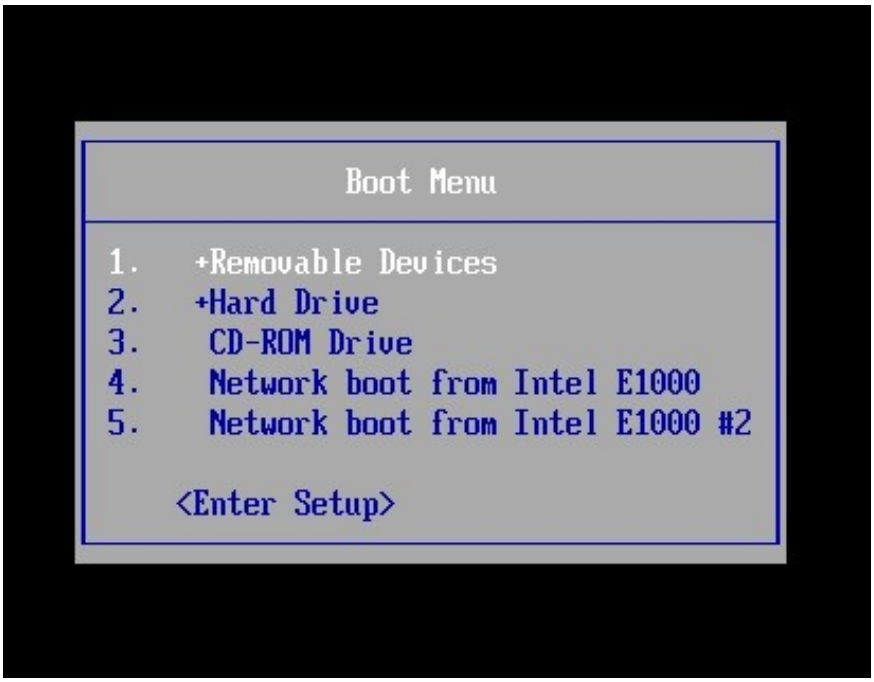
Once you've downloaded and burnt to disc (or mounted the ISO file as a CD if using vmware) you can boot from the disc, select 1). default boot options



4.1.1 Mounting a VM CD/ISO image

For VMware it is possible to specify the CDROM to use an ISO image, then when the system boots up, hitting Esc will bring up the Virtual BIOS menu and allow the CD-ROM Drive to be selected as a boot device.


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
1024 MB
Processors
2
Hard Disk (SCSI)
40 GB
CD/DVD (IDE)
Auto detect
Floppy
Using drive A:
Network Adapter
Custom (VMnet1)
Network Adapt...
Host-only
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Connection
Use physical drive:
Auto detect (E:)
Use ISO image file:
C:\Users\gfield\Downloads\syst
Browse...
Advanced...
OK
Cancel
Help



4.2 Run the file system checks

The commands to run once you get to the command line of sysrescuecd are:

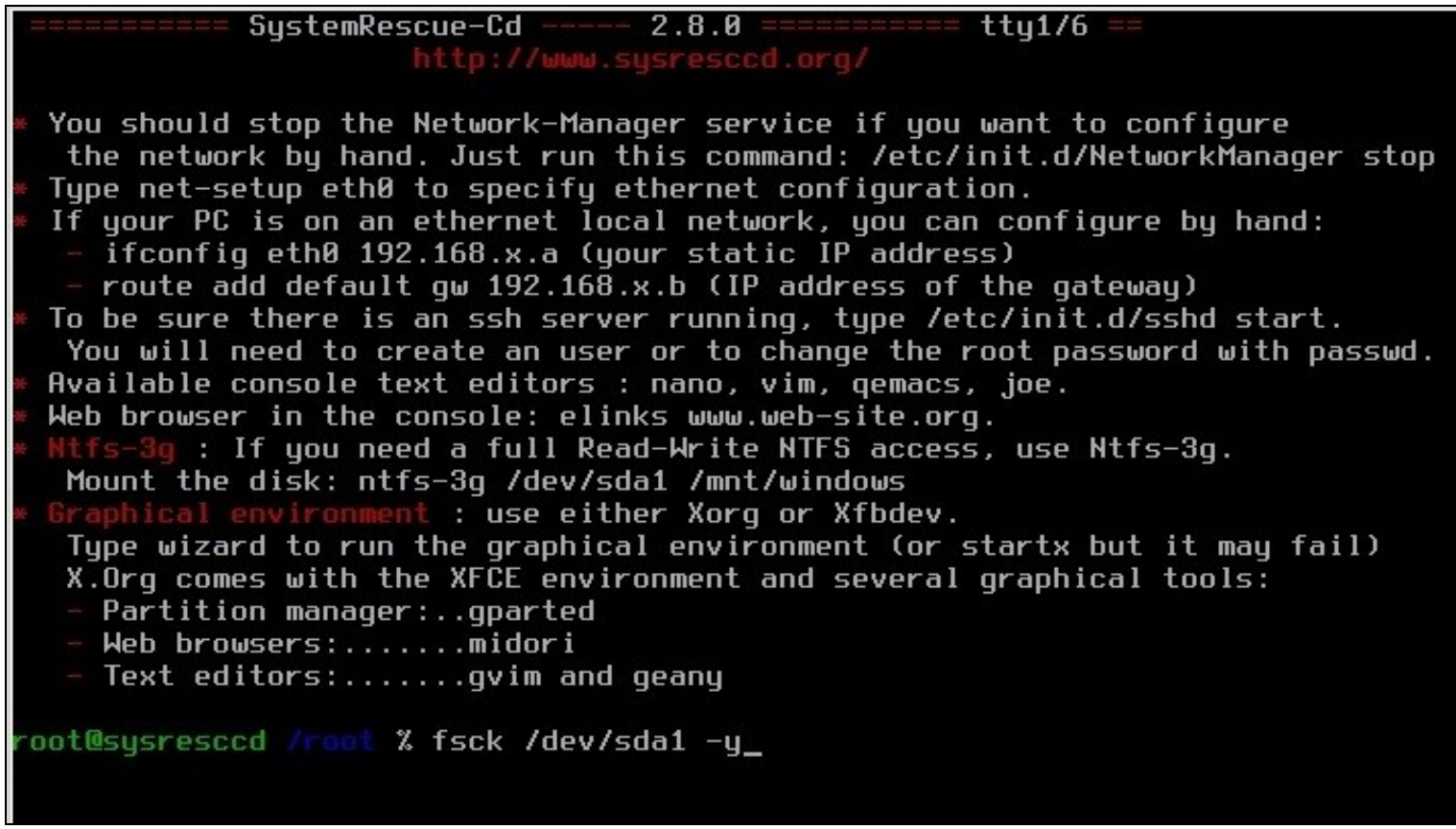
```
fsck /dev/sdX1 -y
fsck /dev/sdX2 -y
fsck /dev/sdX3 -y
fsck /dev/sdX5 -y
fsck /dev/sdX7 -y
```

Please Note: Constitute **X** in the above commands with the actual device e.g /dev/sda1 or /dev/sdb1.

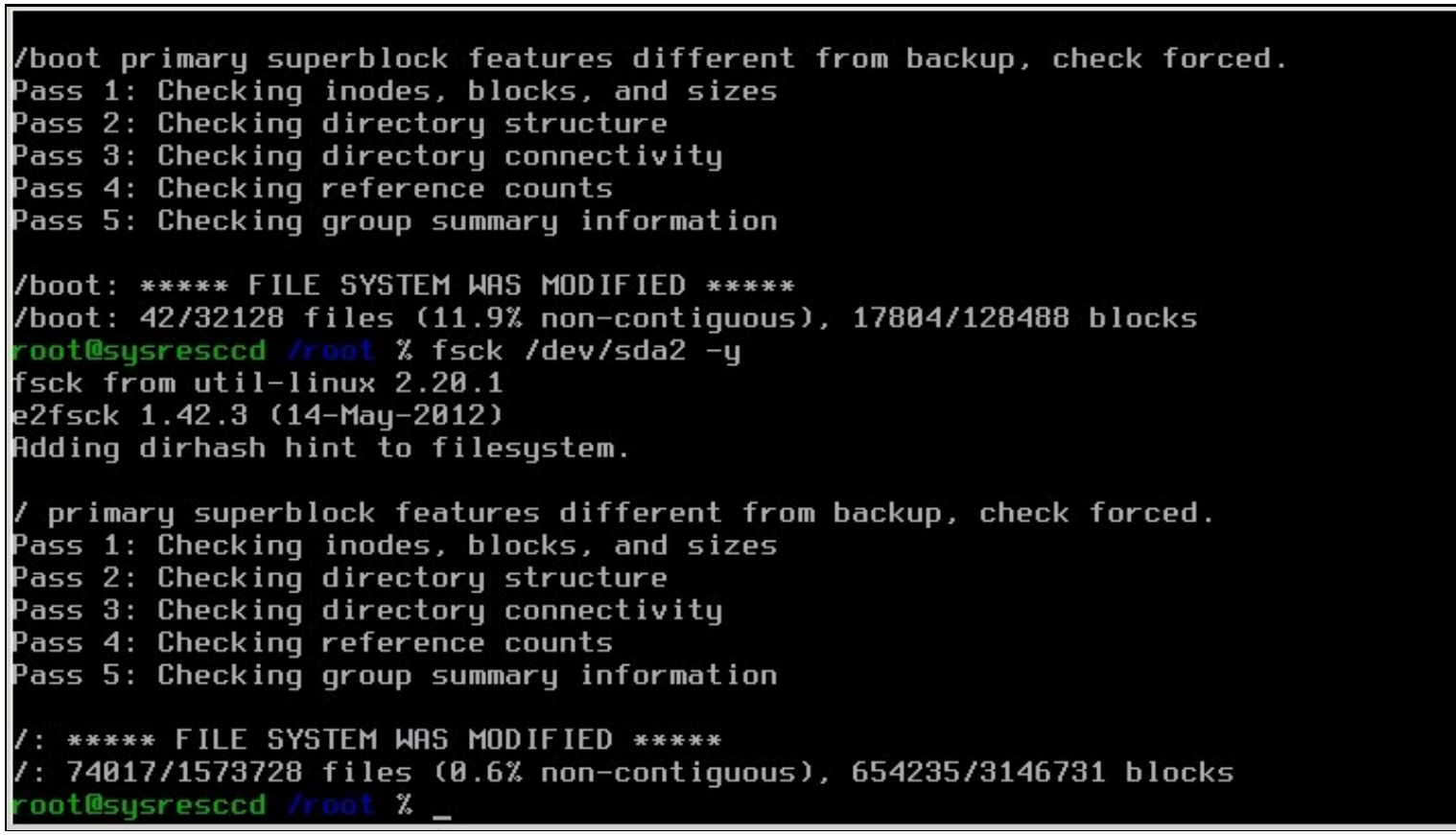
For more recent appliances *sda4* and *sda6* do not exist and can be safely ignored. Older appliances with sdX4 and sdX6 should have these checked.

```
fsck /dev/sdX4 -y
fsck /dev/sdX6 -y
```

Running the fsck from the command line



Fsck running



Fsck with sda4 absent

```
Pass 5: Checking group summary information

/: ***** FILE SYSTEM WAS MODIFIED *****
/: 74017/1573728 files (0.6% non-contiguous), 654235/3146731 blocks
root@sysresccd /root % fsck /dev/sda3 -y
fsck from util-linux 2.20.1
e2fsck 1.42.3 (14-May-2012)
Adding dirhash hint to filesystem.

/backups primary superblock features different from backup, check forced.
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information

/backups: ***** FILE SYSTEM WAS MODIFIED *****
/backups: 1593/524288 files (2.2% non-contiguous), 226805/1048241 blocks
root@sysresccd /root % fsck /dev/sda4 -y
fsck from util-linux 2.20.1
e2fsck 1.42.3 (14-May-2012)
fsck.ext2: Attempt to read block from filesystem resulted in short read while t
ying to open /dev/sda4
Could this be a zero-length partition?
root@sysresccd /root % _
```

Fsck repairing file system

```
Pass 4: Checking reference counts
Pass 5: Checking group summary information
Free blocks count wrong for group #0 (23915, counted=23916).
Fix? yes

Free blocks count wrong (506901, counted=506902).
Fix? yes

Inode bitmap differences:  -19
Fix? yes

Free inodes count wrong for group #0 (16372, counted=16373).
Fix? yes

Free inodes count wrong (262128, counted=262129).
Fix? yes


/tmp: ***** FILE SYSTEM WAS MODIFIED *****
/tmp: 15/262144 files (0.0% non-contiguous), 17210/524112 blocks
root@sysresccd /root % fsck /dev/sda6 -y
fsck from util-linux 2.20.1
fsck: fsck.swap: not found
fsck: error 2 while executing fsck.swap for /dev/sda6
root@sysresccd /root % _
```

4.3 Restart the system

Restart the Swivel appliance and ensure that it boots correctly.

5 Retrieving backups

Should the worst happen and the appliance is not recoverable, you can mount the backups directory to scp the contents from within it to a safe location:

```
mount /dev/sda2 /root/temp
```

An example scp command to retrieve the files would be:

```
scp /root/temp root@anothermachine:/home/admin
```

Where anothermachine is another linux machine with a username of root and a destination directory of /home/admin

6 If this doesn't work

If it's not possible to fix the problem with the sysrescuecd solution above, you should consider retrieving Swivel backups (as mentioned in the solution) from your broken appliance and deploying them into a freshly deployed VM. If you have not retained the VM you downloaded from us you may need to contact your reseller for a reissue of the download.

7 Further Troubleshooting

Check the /var/spool/clientmqueue or /var/log/tomcat folders for large numbers of files, this has been seen to prevent booting.

inode too big

Make a note of any inode numbers given as errors and these can be used to find problems if any partitions can be mounted. To search using an inode use:

find / -inum <inode_number>

Example:

find / -inum 722421

7.1 Sample Boot error log

```
Your system appears to have shut down uncleanly.

Press N within 1 second to not force file system integrity check...
Checking root filesystem
Inode 295605 is too big.

/:UNEXPECTED INCONSISTENCY; RUN fschk MANUALLY

                                              [FAILED]

*** An error occurred during the file system check
*** Droping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

8 Hardware Fault

If the cause is a hardware fault then it may be necessary to contact Dell Hardware support, see Dell Maintenance

9 Did you take a backup?

It's important to take backups for these occasions. Some other articles related to backup methods for the Swivel appliance can be found here:

Automated FTP Backups

Recovery Disk for Appliances How to Guide

10 Appliance Hardware

11 Swivel Appliance Hardware

This document covers aspects of the Swivel Appliance Hardware.

For installation see Hardware Appliance Installation and the Getting Started Hardware Appliance

For the Hardware Specification see Hardware Appliance Specification

For general questions see the Appliance General FAQ

For Hardware Troubleshooting see Appliance Hardware Troubleshooting

12 Appliance HTTPS How To Guide

12.1 Overview

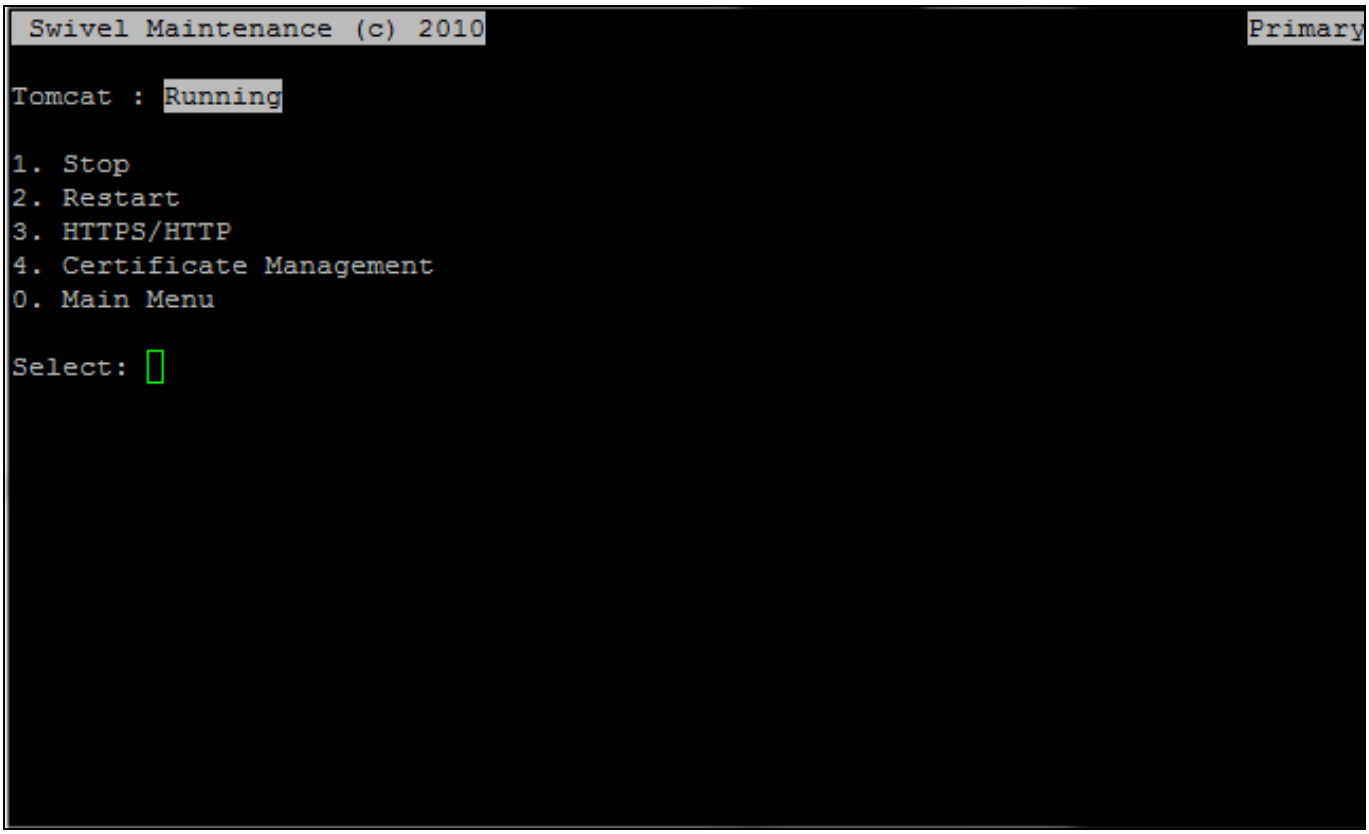
This article describes how to change the protocol of port 8080 and 8443 on the PINsafe Appliance. By default the appliance ships with HTTPS enabled. However you can independently configure each port to be different, through an easy to use menu.

12.2 Connecting via SSH

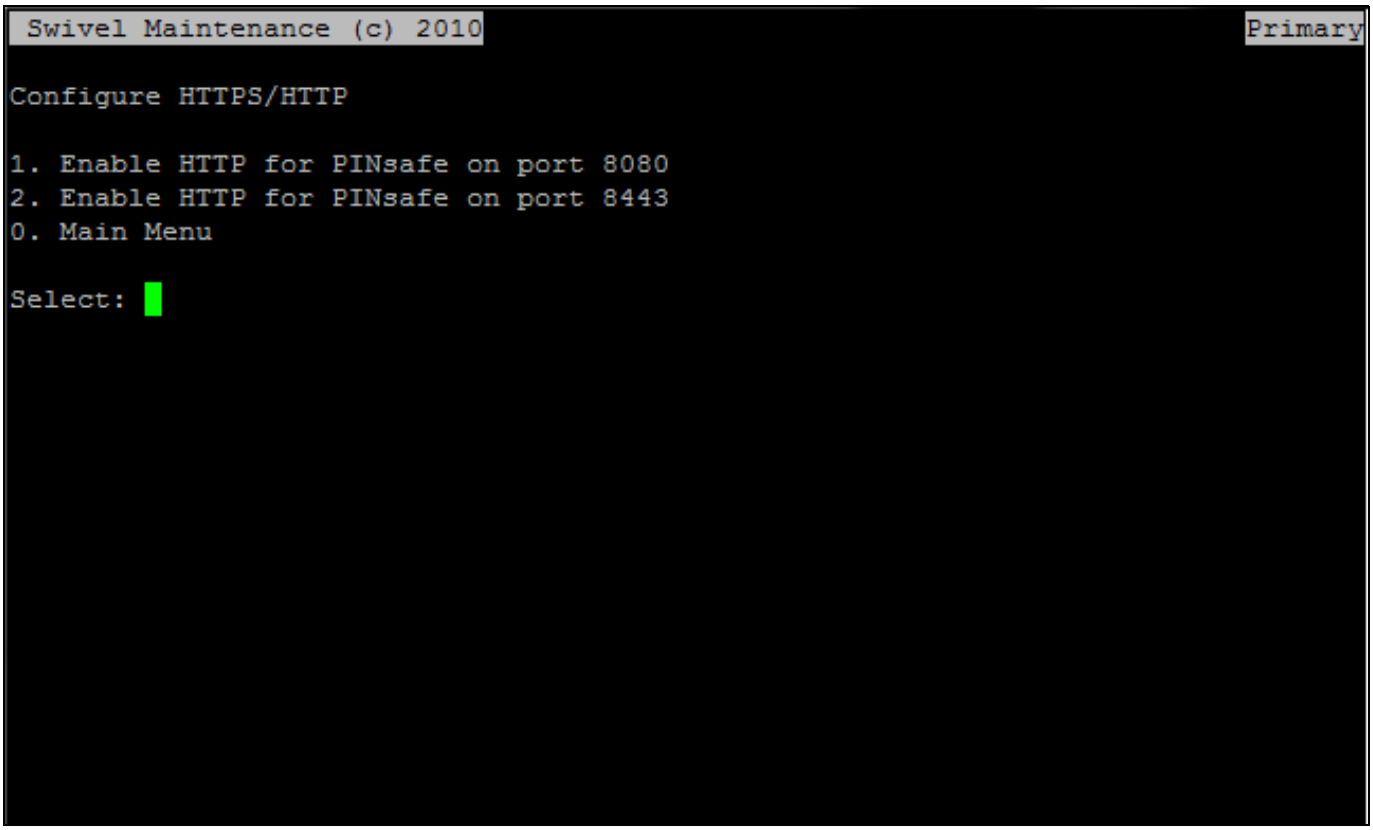
To change this setting, you first need to connect to the PINsafe appliance using SSH. For more information on how to do this, see the PuTTY How To Guide.

12.3 Get to the HTTPS/HTTP menu

Select the Tomcat option from the Main menu:



Then select the HTTPS/HTTP menu option:



From this menu you can change each individual port that Tomcat uses, either port 8080 or 8443. You will need to restart Tomcat for this to take effect. Note that the menu options will change, according to what is currently set. So if HTTPS is enabled already, you will find that the menu option offers to change this to HTTP and vice versa.

Note that if you change the protocol of port 8080 that you will need to ensure that you connect to the PINsafe Admin Console using the new protocol you have assigned.

12.4 Next steps - Installing a certificate

If you have just enabled HTTPS using this article, you may wish to consider installing a security certificate. This is explained in a separate article, SSL Certificate PINsafe Appliance How to Guide.

13 Appliance Synchronisation

14 Overview

Appliance synchronisation allows certain elements to be synchronised across appliances or another Swivel instance that is using a shared database. This method of sharing session information supersedes Single Channel Session Cache and Session Sharing and it is recommended to disable these if they have been enabled. By default session sharing and Appliance Synchronisation are not enabled.

Sessions that can be synchronised across appliances include:

- Single Channel Sessions (TURing, Pinpad)
- SMS by On Demand Authentication authentication
- Mobile Provision Codes

15 Prerequisites

Swivel 3.9.5 or later

Swivel Appliance 2.0.14 or later

Shared database between Swivel instances.

Where the older session sharing is used it is recommended to disable it before enabling the Appliance Synchronisation.

16 Appliance Synchronisation

From the Swivel Administration console select **Appliance Synchronisation**. Options available are:

Partner Appliance IP: The IP address or hostname of the partner appliance.

Context: The name of the Swivel installation, usually pinsafe.

Port: The port used for communication between appliances, usually 8080.

Ignore SSL Cert Errors: Options Yes/No. Ignore invalid certificates such as self-signed or expired.

Connection Timeout (ms): Default 3000. How long the server attempts to connect to the partner before stopping.

Use SSL: Options Yes/No. Select this if SSL is used on the appliances for the selected ports.

Shared Secret: Shared secret, also required on the other partner. For versions 3.9.6 and 3.9.7 the only shared secret that can be used is *secret*

Synchronise Sessions: Options: Yes/No. When enabled this will synchronise sessions between Swivel appliances. Sessions are used for Single Channel authentication images such as TURing and SMS on demand.

17 Testing

Enable the Appliance synchronisation. A single channel image generated for an admin user on one appliance should allow a login on the partner appliance (must allow a admin console login).

For each session sharing the follwing log message will be generated:

SESSION_UPDATE, <SyncResponse><Session><Data Username="admin"/></Session></SyncResponse>

18 Known Issues

18.1 Session sharing and Appliance Synchronisation

Disable Session Sharing where Appliance Synchronisation is used, as this may cause incompatibilities.

18.2 SSL vulnerability updates stop Appliance Synchronisation working

The following error may be displayed

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure, Time out now 10

This can be resolved by editing the file /usr/local/tomcat/conf/server.xml and changing both instances of 'sslProtocols=' or 'sslProtocol=' to be 'sslEnabledProtocols=', i.e. adding Enabled.

Restart Tomcat.

Test by generating an image and checking the logs.

18.3 3.9.6 and 3.9.7 appliance session sync issue

Swivel versions 3.9.6 and 3.9.7 contain a bug that allows session sharing to a second Swivel instance but breaks it when a session is started on that second instance, to resolve this download the Session Sync patch file and copy the contents to the following locations:

LocalSessionManager.class to: /usr/local/tomcat/webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/session

SyncXML.class to: /usr/local/tomcat/webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/sync

For a software only install substitute /usr/local/tomcat with the Tomcat install path

This issue is fixed in Swivel 3.10 Resolution, use shared secret of secret or to upgrade to 3.10

19 Troubleshooting

Check the Swivel log.

Check connectivity by a Telnet from each Swivel server to the other:

```
Telnet 192.168.1.100

Trying 192.168.1.100

connected to standby@swivel.local (192.168.1.100).

Escape character is '^]'.

Connection closed by foreign host.
```

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure, Time out now 10

1. This can be resolved by editing the file /usr/local/tomcat/conf/server.xml and changing both instances of 'sslProtocols=' or 'sslProtocol=' to be 'sslEnabledProtocols=', i.e. adding Enabled.

Restart Tomcat.

Test by generating an image and checking the logs.

2. The error is also seen on **Version 3 Appliances**, there you will need to enable TLSv1 either via the CMI menu (if available) or editing the server.xml from sslEnabledProtocols="TLSv1.1,TLSv1.2" To sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" for both connector ports and restart Tomcat.

Appliance Synchronisation unavailable

If the appliance synchronisation is not available in the Administration console, it may be due to Session Sharing. Disabling this will allow the appliance synchronisation to be selectable. Edit the /home/swivel/.swivel/conf/config.properies (path will be different for a non appliance) and change the following:

SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.DistributedCacheSessionManager

to

SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.LocalSessionManager

Then restart Tomcat

SYNC_ERROR, 404: Not Found, Time out now 10

Synchronisation has failed between appliances. Check the IP/Hostname, port, context, network connectivity, SSL, SSL errors permitted, on each partner.

SYNC_ERROR_UNAUTHORIZED

The shared secrets do not match, re-enter them on both instances. for 3.9.6 and 3.9.7 the only available option for the shared secrets is *secret*

SYNC_ERROR Unknown Time out now 10

Swivel instance has failed to send the synchronisation data to the partner. Check all settings and network connectivity on each partner. If the appliances have http/https enabled then the settings need to be used for no SSL or SSL respectively.

SYNC_ERROR, java.net.UnknownHostException: standby-swivel-local-pinsafe, Time out now 30

The hostname is not known to the Swivel instance, check the hostname and DNS servers are correct, or try with the IP address.

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target, Time out now 20

Certificate error in communication, used a valid certificate or use option to **Ignore SSL Cert Errors:**

SYNC_ERROR, Unexpected end of file from server, Time out now 60

Check to see if SSL or non SSL communications are used. On the Admin Console, navigate to Appliance > Appliance Synchronisation and check the setting Use SSL.

SYNC_ERROR, java.net.SocketTimeoutException: Read timed out, Time out now 20

Check Network connectivity between the Swivel instances.

20 Appliance Upgrade

Appliance upgrades are handled using Patch Appliance Install

21 Static Routes How to Guide

22 Overview

The Swivel appliance CMI allows one static route to be added, however subsequent static routes may need to be added manually. This is why you only see the Display Route option available on the appliance CMI if you already have a route configured.

23 View the routing table

From the CMI, select Advanced Menu > Admin > Networking > IPs & Routing > Diagnostics > Routing table

24 Add a Static Route

Swivel appliance 2.0.14

From the CMI, select Advanced Menu > Networking > IPs & Routing > Change Appliance Routing > Add a route

The following information is required:

- Address : The destination address
- Netmask : The network subnet mask for the address e.g. 255.255.255.0
- Gateway : The gateway address to be used

Press return when complete

To view a current route select Display route.

25 Multiple static routes

This option should only be used when multiple static route are required. Connect to the Swivel appliance using WinSCP How To Guide.

Then navigate to the following file on the appliance using WinSCP:

/etc/sysconfig/network-scripts/route-eth0

Edit this file by right clicking on it and selecting Edit.

You should see the route that you've already defined exists under the ADDRESS0, NETMASK0, GATEWAY0 entries. Add another set of values underneath as provided in the example below using ADDRESS1, NETMASK1, GATEWAY1 entries:

ADDRESS0=10.10.10.0

NETMASK0=255.255.255.0

GATEWAY0=192.168.0.1

ADDRESS1=172.16.1.0

NETMASK1=255.255.255.0

GATEWAY1=192.168.0.1

Save the file and restart networking through the command line or CMI

```
service network restart
```

26 Static Routes on different interfaces

create a routing file for the required network e.g. route-eth1, route-eth2

```
cd /etc/sysconfig/network-scripts
touch route-eth1
```

Edit the file with vi or WinSCP with the required parameters, for example:

ADDRESS0=192.168.0.0

NETMASK0=255.255.255.0

GATEWAY0=192.168.0.1

Save the file and restart networking through the command line or CMI

```
service network restart
```

27 Create a static route on a separate interface

create a routing file for the required network e.g. route-eth1 or route-eth2

```
cd /etc/sysconfig/network-scripts
touch route-eth1
```

Edit the file with vi or WinSCP with the required parameters, for example:

ADDRESS0=0.0.0.0

NETMASK0=0.0.0.0

GATEWAY0=192.168.0.1

Save the file and restart networking through the command line or CMI

```
service network restart
```

28 Verifying routes

the following commands are of use in verifying routes

```
route
```

```
netstat -r
```

to test if a route can be reached using traceroute

```
traceroute 192.168.0.1
```

29 Known Issues

If the delete route option is run from within the CMI menu, all routes are deleted.

30 Troubleshooting

View the /var/log/messages file as this may include network issues such as invalid format for the route or of the network is unreachable.

31 Why upgrade to v3

Upgrade to V3 Appliance

ASAP

Version 1.1 March 31, Updated March 2017

32 Introduction

This document referes to a general question about appliance upgrade.

32.1 Prerequisites

Appliance v2.X

33 Why shoud I upgrade?

The primary reason to upgrade to a version 3 appliance is that version 2 cannot support TLS versions higher than 1.0, which is now considered obsolete and insecure. Upgrading from version 2 to version 3 involves a complete rebuild, as the operating system is different. Version 4 will use the same operating system as version 3, so there will be an upgrade path.

33.1 EOL - When will it happen?

A grace period ending on 30-09-2017 can be applied to allow our VAD/VAR upgrade their customers to Appliances V3. x

SWIVEL SECURE going to generate download links for VIRTUAL Appliances has requested free of charge. For HARDWARE Appliance customer need to buy new appliances, because that old hardware don?t support V3.x

This operation is FREE OF CHARGE for VAD/VAR/CUSTOMERS if they manage all the upgrades without a need of a Solutions Engineer, in the case that is a request a analyse need to be performed by Solutions Engineer to identify the effort needed in PS days. (Sales Department, can request exceptions when exists a justification).

34 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com