IBM InfoSphere Guardium Rescue System

User Guide

Version 2.02

The IBM InfoSphere Guardium Rescue System enables you to boot the Guardium appliance into an emergency rescue mode. The situations that require emergency boot include:

- CLI and GuardCLI passwords are lost and the root passkey is unavailable to reset the password.
- The appliance will not boot and is stuck in "grub" stage.
- The appliance will not complete the booting process due to disk corruption.
- Use a fileserver to download data from a down system not otherwise recoverable.

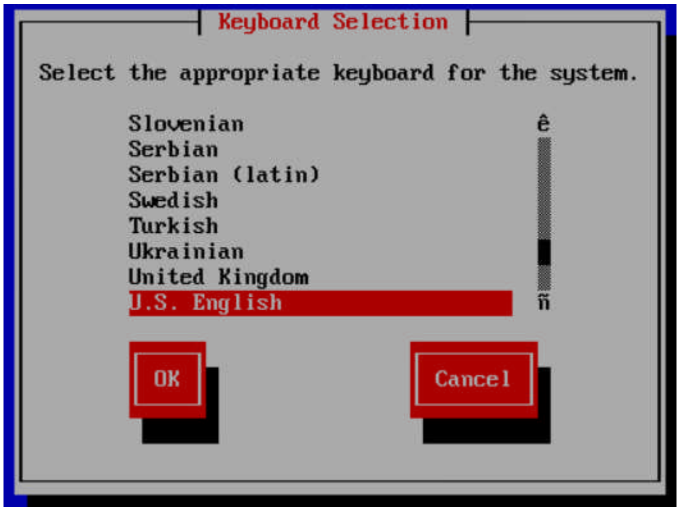
The rescue system cannot be used to recover from hardware problems. If there are hardware errors, please contact Guardium Technical Support for assistance.

Usage

1. Obtain the rescue ISO file from Guardium Technical Support.
2. Boot the appliance off the ISO file by burning it to a CD/DVD. If your Guardium appliance is running in a Virtual Machine, it may be possible to boot from the ISO directly. Please consult the manuals of your virtualization software regarding this option.
3. Login as user "rescue". A password is not required for this user.
4. A Guardium CLI like interface will be presented with a limited number of rescue related commands.

Select the system Keyboard

When logging is as user rescue for the first time from the console, a dialog to set the system keyboard will be presented. This can be changed later by executing ‘`system set_keyboard`’ from the console.



Keyboard Selection

Select the appropriate keyboard for the system.

Key of the Day

The rescue system provides the facility to start a fileserver and SAMBA service to download files from the appliance in the event of an irrecoverable disaster. These services and commands like disk repair are protected by a Key of the Day. Please obtain this key from Guardium Support. The key is valid only for the day for which the key was issued, regardless of when the key was generated and issued. For instance, if the key was generated on 1-Jan-2013 for use on 15- Jan-2013, the key is valid only on 15-Jan-2013.

If you have scheduled a disaster recovery exercise for a particular day, specify that date to Support. Requests for a Key of the Day must be accompanied by a business justification, recorded in the relevant PMR.

Password management

When all user passwords are lost and password reset mechanism is not feasible, the only option is for Guardium Support to remotely log in as root and reset the password. If IBM Technical support cannot access the system as root using their internal repository or the root passkey is not available, then the Rescue System provides the ability to change the password for the CLI accounts, cli and guardcli users.

If the password cannot be set using the rescue system, please contact Guardium Technical Support with the details of the error. Guardium Technical Support will attempt to reset the password on a best effort basis

Password cli_users

This command is used to change the password for the Guardium CLI users.

Syntax:

```
Password cli_users <username>
```

Example:

```
GuardRescue> password cli_users
guardcli1 Enter password for
guardcli1:
Re enter password:
Attempting to mount the Guardium filesystems
If there are errors in the process DO NOT CONTINUE!
Changing password for user guardcli1.
passwd: all authentication tokens updated successfully.

ok
```

password reset_root_passkey

This password resets the root password of the underlying Guardium appliance. This is a protected function and requires the key of the day.

Syntax:

```
Password cli_users <username>
```

Example:

```
You are resetting the root password of the Guardium
appliance. Please confirm [Y/n]: Y

This protected function requires the Key of the day
If you do not have it, please contact Guardium Technical
Support. This key is valid only for the day for which it
```

```
was issued.

Please enter the Key of the Day: XXXXX
Attempting to mount the Guardium filesystems
If there are errors in the process, DO NOT
CONTINUE!
Changing password for user root.
passwd: all authentication tokens updated successfully.

Root passkey:

13614603 ok
```

Password get_root_passkey

This command prints the root passkey for the underlying Guardium appliance. This is not the password for the root account. It is a key that Guardium Support will decode into the actual password.

Syntax:

```
Password get_root_passkey
```

Example:

```
GuardRescue> password get_root_passkey
Guardium root passkey: 12345678
```

Network Operations

Most rescue operations can be performed from the console. Sometimes network access to the system may be required while it is in rescue mode. For instance, the appliance maybe a physical box and remote login via ssh or putty may be required. Under these circumstances, network must be configured. By default, it is not configured in the rescue system.

Any change made to the network configuration may alter the NIC. So, when the rescue is completed and the appliance is booted up normally, the network configuration may need to be reconfigured.

Network show

This command displays the current network configuration.

Syntax:

```
Network show
```

Example:

```
GuardRescue> network show

inet addr:192.168.1.134  Bcast:192.168.1.255  Mask:255.255.255.0

Kernel IP routing table
Destination  Gateway      Genmask        Flags Metric Ref    Use Iface
192.168.1.0  0.0.0.0      255.255.255.0  U     0      0      0   eth0
0.0.0.0      192.168.1.1  0.0.0.0        UG    0      0      0    eth0

Resolvers:
192.168.1.1
ok
```

Network store

This command is used to configure the network parameters. The current values, if any, will be displayed and used as the default value, if no value is supplied for that parameter.

It is recommended that this command be executed in the console. If the network settings are changed in a remote shell, connectivity in that shell may be disrupted.

Changing the network configuration while files are being downloaded using fileserver or samba will disrupt the download.

Syntax:

```
Network store
```

Example:

```
GuardRescue> network store
Please enter the values. Enter to accept default:
IP address []: 192.168.102.123
Netmask []: 255.255.255.0
Default route []:192.168.1.1
Resolver: 192.168.1.1
```

Network ping

Test network connectivity using ping. Resolver must be set during network configuration to use a hostname to ping.

Syntax:

```
Network ping <IP address> | <hostname>
```

Example:

```
GuardRescue> net ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=0.332 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.328 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=64 time=0.419 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=64 time=0.358 ms
64 bytes from 192.168.1.11: icmp_seq=5 ttl=64 time=0.269 ms

--- 192.168.1.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.269/0.341/0.419/0.049 ms
```

Disk Operations

Mounting and un-mounting Guardium Filesystems

Most commands automatically mount and un-mount the Guardium file systems as necessary. Operations like repairing the boot loader require the file systems to the manually mounted. The Guardium filesystems must also be manually mounted, when Guardium Support requires direct access to the Guardium filesystems.

If there are errors during mounting or un-mounting, DO NOT CONTINUE and contact Guardium Support.

Syntax:

```
GuardRescue> disk mount_gaurdium

GuardRescue> disk unmount_gaurdium

GuardRescue> disk show_mount
```

Repair disk corruption

Sometimes due to disk corruption, the Guardium appliance may fail to boot. In such an event, messages like the following may be displayed on the screen at boot time followed by a request for the root password:

```
fsck failed. Please repair manually and reboot
```

This indicates that the system has run into a disk error that it could not correct automatically. The rescue system provides the ability to manually run fsck and attempt to fix the errors. This is a protected function and requires the key of the day. Please contact Guardium Technical Support and obtain the key of the day.

Repairing corrupt disks are done in a best effort basis. Depending on where the corruption exists, running “fsck” on the disk may not resolve the problem.

This command must be run from the console and cannot be run from a remote terminal, since any loss of network connectivity will interrupt the check/repair and lead to further complications. If run from a remote terminal, the following error message will be printed:

```
Please run this command from the console.
Loss of network connectivity will interrupt
fsck and lead to unexpected results.
```

If an error occurs, the error code will be printed to the console. Please contact Guardium Support and supply the error number.

Syntax:

```
disk check_disk
```

Example:

```
This protected function requires the Key of the day
If you do not have it, please contact Guardium Technical
Support. This key is valid only for the day for which it
was issued.

Please enter the Key of the Day: XXXXX
You are attempting to run fsck on the Guardium filesystems
You should run it only if instructed by Guardium Support

Fixing disk errors by fsck is on a best effort basis.
Depending on where the corruption is, this may not fix the issues

Do you agree? [Y/n]: Y
Please select one of the following filesystems:
1 : /dev/sda1
2 : /dev/sda2
3 : /dev/sda3
4 : Quit
2
Attempting to check/fix /dev/sda2
Output is written to /var/log/rescue/fsck_out__dev_sda2.out
Please use the fileserver utility to view/download it
Please do not interrupt this process ...
Filesystem errors corrected ok
```

Services and Utilities

The Guardium Rescue System provides tools and services to check connectivity, provide remote access to Guardium Support and a file server facility to download files from the appliance, useful in cases of disaster recovery.

SSHD Server

This set of commands manages remote access. Please start this service in order to enable remote access by Guardium Support.

The SSHD service is disabled by default for security reasons.

Syntax:

```
Service ssh {start | stop | status}
```

Description:

Service ssh start: Starts SSHD service

Service ssh stop: Stops SSHD service

Service ssh status: Displays if the service is active or not.

Fileserver

The fileserver service can be used:

- As part of disaster recovery to download files from the Guardium appliance.
- To upload patches to the Guardium appliance, when the normal methods via CLI or GUI are not feasible.

Commands that start the file servers are protected by a Key of the Day. Please obtain this key from Guardium Support. The key is valid only for the day for which the key was issued, regardless of when the key was generated and issued. For instance, if the key was generated on 1-Jan-2013 for use on 15- Jan-2013, the key is valid only on 15-Jan-2013.

HTTP Fileserver

This command starts a simple HTTP server on port 8000. Press “enter” to terminate the fileserver.

Syntax:

```
Service fileserver {start | stop | status}
```

Example:

```
GuardRescue> service fileserver

This protected function requires the Key of the day
If you do not have it, please contact Guardium Technical Support. This key is valid only for
the day for which it was issued.

Please enter the Key of the Day: XXXX

Connect to http://192.168.1.134:8000

Press enter to terminate fileserver
```

Samba Fileserver

This set of commands manages SAMBA service that shares Guardium directories. This is useful to scrape files and the Guardium internal database during disaster recovery. This is turned off by default.

When the service is started, the system will ask for a password that is necessary to mount to Windows explorer or a SAMBA client in Linux/Unix.

The username is "guardium" and the system prints the directories that are shared by the system.

The Samba server uses ports 139/TCP and 445/TCP

List Samba shares

Syntax:

service samba shares

Description:

This command lists the shares that can be mounted on a remote computer.

All of the Samba shares excepting "patches" are read-only. The "patches" is read-write and enables uploading patches to the Guardium patches directory.

Example:

```
GuardRescue> service samba
shares
The following files are shared:
[guardlog]
[mysql]
[patches]
ok
```

Start Samba service

Syntax:

service samba start

Description:

This command starts the shares that can be mounted on a remote computer. Please enter the password for user 'guardium'. This password must be used in the remote Samba client to connect to the Samba server.

Example:

```
GuardRescue> service samba start

This protected function requires the Key of the day
If you do not have it, please contact Guardium Technical
Support. This key is valid only for the day for which it was
issued.

Please enter the Key of the Day: XXXXX
Please enter the password to share the
filesystem:

Reenter password:

Starting share ... Done

Guardium filesystems can be mounted as user
'guardium'.

The following files are shared:
[guardlog]
[mysql]
[patches] ok
```

Stop Samba service

Syntax:

service samba stop

Description:

Stops the Samba service

Example:

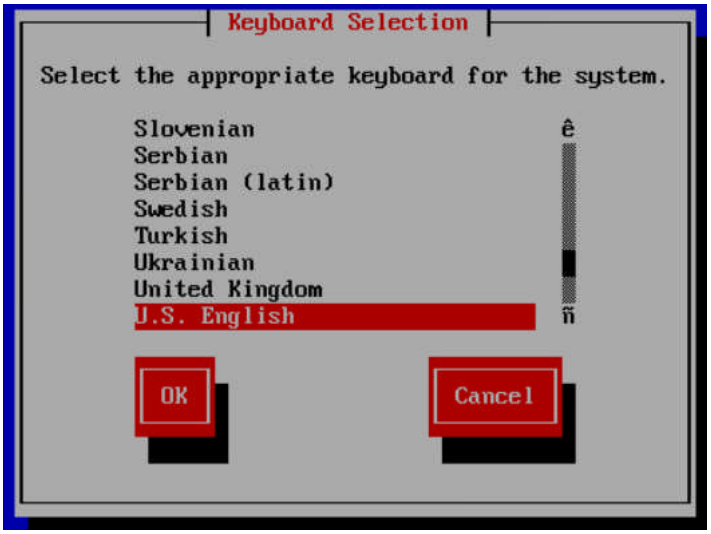
```
GuardRescue> service samba stop

Stopping share ... Done
ok
```

System Operations

Change System Keyboard

The default keyboard is US English. This can be changed by executing '`system set_keyboard`'. Select the keyboard as required.

This command can be run only from the console for the new keyboard layout to take effect.



Keyboard Selection

Select the appropriate keyboard for the system.

Repair GRUB

This command attempts to repair the boot loader, if the appliance is stuck in "GRUB" or will not boot up due to corruption of the Master Boot Record (MBR.)

If there are other errors in the disk DO NOT attempt to repair the system and contact Guardium Support.

Syntax:

System repair_grub

Example:

```
GuardRescue> system repair_grub
You are attempting to repair the boot loader
This is on a best effort basis
If there are other corruptions, this may not fix the boot record

Please confirm[Y/n]: Y
Attempting to mount the Guardium filesystems
If there are errors in the process, DO NOT CONTINUE!

Repair GRUB ... Installation finished. No error
```

```
reported. This is the contents of the device map
/boot/grub/device.map.
Check if this is correct or not. If any of the lines is
incorrect, fix it and re-run the script `grub-install'.

# this device map was generated by
anaconda (hd0)/dev/sda
Done

Attempt to repair boot loader complete.
```

If there were no errors, remove the CD/DVD and reboot appliance.
If there were errors, please contact Guardium Technical Support

Exit to Root Shell

This command is reserved for use by Guardium Technical Support. The root passkey will be displayed that must be decoded to the actual password and entered when prompted. Upon exiting the root shell the rescue prompt will be restored.

Syntax:

```
System shell
```

Example:

```
GuardRescue> system shell
Root passkey for this rescue instance: 91147762
Enter password:
[root@GuardRescue ~]#
```