Oracle® Exalogic Elastic Cloud

STIGfix User's Guide

Release 1.0

E53111-02

October 2015

STIGfix is a tool that you can use to harden guest vServers and physical Oracle Linux nodes on an Exalogic machine, to make them compliant with STIGs (Security Technical Implementation Guides).

STIGs are security configuration standards defined by Defense Information Systems Agency (DISA), an agency of the United States Department of Defense (DoD). For more information about STIGs, go to `http://iase.disa.mil/stigs/`.

For a list of the STIGs that are addressed by the current version of Oracle STIGfix, see Section 5, "STIGs Addressed by the STIGfix Tool."

This guide contains the following sections:

1 Supported Platforms

For a list of the EECS releases that are supported for STIGfix, see the My Oracle Support document ID 1912063.1.

2 Installing STIGfix

STIGfix is installed automatically when you install the ExaLogic Lifecycle (ELLC) toolkit. For the ELLC installation instructions, see the My Oracle Support document ID 1912063.1.

The STIGfix tool (`stigfix`) is available in the `/exalogic-lctools/bin` directory on the compute node on which you installed the ELLC toolkit. To find out the version of the STIGfix tool that is currently installed, go to the `/exalogic-lctools/bin` directory and run the `stigfix --version` command.

3 Preparing to Use STIGfix

This section describes the steps that you must perform before running STIGfix.

3.1 Ensure that `root` Is Not the Only User

After you run STIGfix on a compute node or vServer, direct SSH access to that vServer or compute node as the `root` user will be restricted. So before running STIGfix, check whether `root` is not the only user that exists on the vServer or compute node that you want to harden by using STIGfix.

If `root` is the only user, create another user, by using the following commands.

```
# useradd username
# passwd username
```

3.2 Configure STIGfix Parameters

The `stigfix.json` file specifies the STIGs for which the STIGfix tool hardens the target system. For each STIG, the file lists certain fields, some of which are configurable.

- You can configure the STIGfix tool to skip hardening the target system for selected STIGs, by setting the `enabled` field to `false` for those STIGs.
- For certain STIGs, you can configure additional parameters as described in Table 1.

> **Note:** For these STIGs, use only lower case alphabets to define a parameter.

Table 1 Configurable Parameters in `stigfix.json`

STIG ID	STIG Title	Configurable Parameter	Default Value
GEN000580	The system must require passwords contain a minimum of 14 characters.	`minlen`: Minimum number of characters in a password	`14`
GEN000590	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes.	`hash`: Algorithm for generating hashes for account passwords	`sha256`
GEN000700	User passwords must be changed at least every 60 days.	`days`: Password-expiry duration, in days	`60`

- You can configure the STIGfix tool to completely enable or disable auditing by modifying the `audit_script` entry in the `stigfix.json` file. Alternatively, you can disable specific audit rules by modifying the `stigfix_audit.rules` file.

To configure the STIGfix parameters, complete the following steps:

1. Open the `stigfix.json` file in a text editor.

   This file exists in the `/lib/stigfix` subdirectory of the directory on which you mounted the `/export/common/exalogic-lctools` share.

2. Look for the STIGs for which you do not want to harden the compute node or vServer.

3. For each such STIG, set the value of the `enabled` field to `false`, as shown in the following example:

```
{
  "name": "GEN007080",
  "description": "The Datagram Congestion Control Protocol (DCCP) must be
```

```
disabled unless required.",
  "script": "GEN007080.py",
  "script-params": null,
  "severity": "Medium",
  "enabled": false
},
```

Caution: Do not change any field in `stigfix.json` other than those explicitly mentioned in this document.

4. If you want to configure any of the parameters listed in Table 1, identify the relevant STIG in `stigfix.json`, and change the value of the parameter.

   In the following example, the algorithm for generating hashes for account passwords is changed from the default SHA-256 to SHA-512:

```
{
   "name": "GEN000590",
   "description": "The system must use a FIPS 140-2 approved cryptographic
hashing algorithm for generating account password hashes.",
   "script": "GEN000590.sh",
   "script-params": [{
           "name": "hash",
           "value": "sha512"
       }],
   "severity": "Medium",
   "enabled": true
 },
```

Caution: Do not change any field in `stigfix.json` other than those explicitly mentioned in this document.

5. Save and close the `stigfix.json` file.

4 Running STIGfix

To run the STIGfix tool, complete the following steps:

1. Ensure that you have fulfilled the prerequisites listed in Section 3, "Preparing to Use STIGfix."
2. SSH, as `root`, to the compute node or guest vServer that you want to harden.
3. Mount the ELLC shares by doing the following:
   a. Copy the ELLC installer `exalogic-lctools-`*`release_number`*`-installer.sh` to the compute node or guest vServer that you want to harden.
   b. Run the following command on the host to which you copied the installation script:

      ```
      # ./exalogic-lctools-release_number-installer.sh ZFS_Address -m
      ```

      In this command, `ZFS_Address` is the host name or IP address of the storage appliance.

4. For each guest vServer you want to run STIGfix on, ensure that the guest vServer has read/write permissions to the share by doing the following:

   a. Log in to the ZFS Storage Appliance BUI at `https://ZFS_Address:215` as the `root` user.

   b. Click the **Shares** tab.

   c. Find and select the `common / exalogic-lctools` share and click the **edit entry** icon.

      The details of the share are displayed.

   d. Click the **Protocols** tab.

   e. Click the plus (+) button next to NFS Exceptions, and specify the following for each guest vServer on which you want to run STIGfix:

      Type: Network

      Entity: *ip_address_of_vserver*/32 (in CIDR format)

      Access mode: Read/write

      Charset: default

      Root Access: Selected

   f. Click the **Apply** button near the upper right corner.

5. Go to the `bin` subdirectory within the directory on which the `/export/common/exalogic-lctools` share is mounted:

   Example:

   ```
   # cd /exalogic-lctools/bin
   ```

6. Run the following command:

   ```
   # sh ./stigfix
   ```

   Note: The STIGfix tool may display an error for GEN003080-2 because a `symlink` under `/etc/cron.daily` will continue to have permission mode `0777`. You can ignore this error.

7. Perform the manual hardening steps described in the following table:

STIG	Manual Steps
GEN008700: The system boot loader must require authentication	Run the `GEN008700.py` script, which is available in the `/lib/stigfix/scripts` subdirectory of the directory on which you mounted the `/export/common/exalogic-lctools` share. This script adds a password for the grub bootloader.

8. Reboot the compute node or guest vServer:

   ```
   # reboot -n
   ```

   The compute node or guest vServer reboots.

9. After the compute node or guest vServer reboots, you are prompted to enter new passwords which are STIG compliant.

The STIGfix tool hardens the system for all the STIG IDs listed in Section 5, "STIGs Addressed by the STIGfix Tool."

It creates a log file in the `/var/log` directory on the compute node or guest vServer on which you ran STIGfix, in the format `stigfix.`*`YYMMDDHHMMSS`*`.log`. The following is an example of a log file created by STIGfix:

`stigfix.`*`140624123608`*`.log`

For each file that the STIGfix tool updates, it creates a backup in the `/lib/stigfix/backups` directory of the directory on which you mounted the `/export/common/exalogic-lctools` share, in the format *`FIX_NAME-FILE_NAME`*`.bak`*`YYYYMMDD.HHMMSS.NN`*, where `NN` is milliseconds. The following is an example of a backup file created by STIGfix:

`GEN005550.py-sshd_config``.bak`*`20140429.003034.53`*
`GEN003610.sh-sysctl.conf``.bak`*`20140429.003035.42`*

5 STIGs Addressed by the STIGfix Tool

The list of STIGs addressed by the STIGfix tool varies based on the version of Oracle Linux that you are running. This section contains the following topics:

- Section 5.1, "STIGs Addressed by the STIGfix Tool for Oracle Enterprise Linux 5"
- Section 5.2, "STIGs Addressed by the STIGfix Tool For Oracle Enterprise Linux 6"

5.1 STIGs Addressed by the STIGfix Tool for Oracle Enterprise Linux 5

The following table lists the STIGs that are addressed by the current version of STIGfix.

STIG ID	STIG Title
GEN000000-LNX00320	The system must not have special privilege accounts such as shutdown and halt.
GEN000000-LNX00440	The `/etc/security/access.conf` file must have mode `0640` or less permissive.
GEN000000-LNX00520	The `/etc/sysctl.conf` file must have mode `0600` or less permissive.
GEN000000-LNX00580	The x86 CTRL-ALT-DELETE key sequence must be disabled.
GEN000020	The system must require authentication upon booting into single-user and maintenance modes. (CCE-4241-6)
GEN000252	The time synchronization configuration file (such as `/etc/ntp.conf`) must have mode `0640` or less permissive.
GEN000290-2	The system must not have the unnecessary (news) account.
GEN000290-3	The system must not have the unnecessary (gopher) account.
GEN000290-4	The system must not have the unnecessary (ftp) account.
GEN000460	The system must disable accounts after three consecutive unsuccessful login attempts.
GEN000500-2	The graphical desktop environment must set the idle timeout to no more than 15 minutes.
GEN000500-3	Graphical desktop environments provided by the system must have automatic lock enabled.

STIG ID	STIG Title
GEN000540	Users must not be able to change passwords more than once every 24 hours.
GEN000560	The system must not have accounts configured with blank or null passwords.
GEN000580	The system must require passwords contain a minimum of 14 characters.
GEN000590	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes.
GEN000600	The system must require passwords contain at least one uppercase alphabetic character.
GEN000610	The system must require passwords contain at least one lowercase alphabetic character.
GEN000620	The system must require passwords contain at least one numeric character.
GEN000640	The system must require passwords contain at least one special character.
GEN000680	The system must require passwords contain no more than three consecutive repeating characters.
GEN000700	User passwords must be changed at least every 60 days.
GEN000750	The system must require at least four characters be changed between the old and new passwords during a password change.
GEN000800	The system must prohibit the reuse of passwords within five iterations.
GEN000920	The `root` account's home directory (other than `/`) must have mode `0700`.
GEN000940	The `root` account's executable search path must be the vendor default and must contain only absolute paths.
GEN000980	The system must prevent the `root` account from directly logging in except from the system console.
GEN001120	The system must not permit `root` logins using remote access programs such as `ssh`.
GEN001720	All global initialization files must have mode 0644 or less permissive.
GEN002100	The `.rhosts` file must not be supported in PAM.
GEN002720	The audit system must be configured to audit failed attempts to access files and programs.
GEN002720-2	The audit system must be configured to audit failed attempts to access files and programs.
GEN002720-3	The audit system must be configured to audit failed attempts to access files and programs.
GEN002720-4	The audit system must be configured to audit failed attempts to access files and programs.
GEN002720-5	The audit system must be configured to audit failed attempts to access files and programs.
GEN002752	The audit system must be configured to audit account disabling.
GEN002760-10	The audit system must be configured to audit all administrative, privileged, and security actions.

STIG ID	STIG Title
GEN002760-2	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002760-3	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002760-4	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002760-6	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002760-7	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002760-8	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002760-9	The audit system must be configured to audit all administrative, privileged, and security actions.
GEN002800	The audit system must be configured to audit login, logout, and session initiation.
GEN002820	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-10	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-11	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-12	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-13	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-2	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-3	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-4	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-5	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-6	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-7	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-8	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002820-9	The audit system must be configured to audit all discretionary access control permission modifications.
GEN002825-3	The audit system must be configured to audit the loading and unloading of dynamic kernel modules - `/sbin/insmod`.
GEN002825-4	The audit system must be configured to audit the loading and unloading of dynamic kernel modules - `/sbin/modprobe`.

STIG ID	STIG Title
GEN002825-5	The audit system must be configured to audit the loading and unloading of dynamic kernel modules - `/sbin/rmmod`.
GEN003060	Default system accounts (with the exception of `root`) must not be listed in the `cron.allow` file or must be included in the cron.deny file if the `cron.allow` file does not exist.
GEN003080	Crontab files must have mode `0600` or less permissive and files in `cron` script directories must have mode `0700` or less.
GEN003080-2	Files in `cron` script directories must have mode `0700` or less permissive.
GEN003200	The `cron.deny` file must have mode `0600` or less permissive.
GEN003320	Default system accounts (with the exception of `root`) must not be listed in the `at.allow` file or must be included in the `at.deny` file if the `at.allow` file does not exist.
GEN003609	The system must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.
GEN003610	The system must not send IPv4 Internet Control Message Protocol (ICMP) redirects.
GEN003740	The `xinetd` configuration files must have mode `0640` or less permissive.
GEN003810	The `portmap` or `rpcbind` service must not be running unless needed.
GEN004000	The `traceroute` file must have mode `0700` or less permissive.
GEN004540	The SMTP service HELP command must not be enabled.
GEN004580	The system must not use `.forward` files.
GEN005040	All FTP users must have a default `umask` of `077`.
GEN005320	The `snmpd.conf` file must have mode `0600` or less permissive.
GEN005390	The `/etc/syslog.conf` file must have mode `0640` or less permissive.
GEN005501	The SSH client must be configured to only use the SSHv2 protocol.
GEN005505	The SSH daemon must be configured to only use FIPS 140-2 approved ciphers.
GEN005507	The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.
GEN005550	The SSH daemon must be configured with the Department of Defense (DoD) logon banner. This file contains the banner message which will be displayed to any user accessing the hardened system. Users should modify this file to add their company policy or banner message before applying STIGfix.
GEN007020	The Stream Control Transmission Protocol (SCTP) must be disabled unless required.
GEN007080	The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.
GEN007480	The Reliable Datagram Sockets (RDS) protocol must be disabled or not installed unless required.
GEN007540	The Transparent Inter-Process Communication (TIPC) protocol must be disabled or uninstalled.
GEN007660	The Bluetooth protocol handler must be disabled or not installed.

STIG ID	STIG Title
GEN008020	If the system is using LDAP for authentication or account information, the LDAP TLS connection must require that the server provide a certificate with a valid trust path to a trusted CA.
GEN008040	If the system is using LDAP for authentication or account information, the system must verify that the LDAP server's certificate has not been revoked.
GEN008700	The system boot loader must require authentication.

5.2 STIGs Addressed by the STIGfix Tool For Oracle Enterprise Linux 6

The following table lists the STIGs addressed by STIGfix tool for Oracle Enterprise Linux 6

STIG ID	STIG Title
CCE-26242-8	The audit system must be configured to audit all attempts to alter system time using the `adjtimex` command.
CCE-26280-8	Record events that modify the system's discretionary access controls: `chmod`.
CCE-26573-6	Ensure `auditd` collects information on exporting to media successfully.
CCE-26651-0	Ensure `auditd` collects file deletion events by the user.
CCE-26657-7	Record events that modify the system's mandatory access controls.
CCE-26662-7	Ensure `auditd` collects the system administrator's actions.
CCE-26664-3	Record events that modify user or group information.
CCE-26831-8	Disable kernel parameter for accepting secure redirects by default.
CCE-26854-0	Disable kernel parameter for accepting secure redirects for all interfaces.
CCE-26915-9	Enable kernel parameter to use reverse path filtering by default.
CCE-26969-6	Ensure Security-Enhanced Linux (SELinux) state is enforcing.
CCE-26979-5	Enable kernel parameter to use reverse path filtering for all interfaces.
CCE-26993-6	Enable kernel parameter to ignore bogus ICMP error responses.
CCE-27002-5	Set password hashing algorithm in `/etc/login.defs`.
CCE-27015-7	Disable kernel parameter for accepting ICMP redirects by default.
CCE-27018-1	Enable iptables.
CCE-27027-2	Disable kernel parameter for accepting ICMP redirects for all interfaces.
CCE-27037-1	Disable kernel parameter for accepting source-routed packets for all interfaces.
CCE-27066-0	Enable kernel parameter to log martian packets.
CCE-27153-6	Disable IPv6 networking support automatic loading.
CCE-27166-8	Disable accepting IPv6 redirects by setting `net.ipv6.conf.default.accept_redirects` to 0.
CCE-27170-0	Record attempts to alter time through `clock_settime`.

STIG ID	STIG Title
CCE-27172-6	The audit system must be configured to audit all attempts to alter system time through `/etc/localtime`.
CCE-27173-4	Record events that modify the system's discretionary access controls: `chown`.
CCE-27174-2	Record events that modify the system's discretionary access controls: `fchmod`.
CCE-27175-9	Record events that modify the system's discretionary access controls: `fchmodat`.
CCE-27177-5	Record events that modify the system's discretionary access controls: `fchown`.
CCE-27178-3	Record events that modify the system's discretionary access controls: `fchownat`.
CCE-27179-1	Record events that modify the system's discretionary access controls: `fremovexattr`.
CCE-27180-9	Record events that modify the system's discretionary access controls: `fsetxattr`.
CCE-27181-7	Record events that modify the system's discretionary access controls: `lchown`.
CCE-27182-5	Record events that modify the system's discretionary access controls: `lremovexattr`.
CCE-27183-3	Record events that modify the system's discretionary access controls: `lsetxattr`.
CCE-27184-1	Record events that modify the system's discretionary access controls: `removexattr`.
CCE-27185-8	Record events that modify the system's discretionary access controls: `setxattr`.
CCE-27203-9	Record attempts to alter time through `settimeofday`.
CCE-27228-6	Set password hashing algorithm in `/etc/login.defs`. Preferred is SHA512.
CCE-27238-5	Configure `auditd space_left_action` on low disk space to email.
CCE-27247-6	Disable automatic bug reporting tool (`abrtd`).
CCE-27283-1	Limit the number of concurrent login sessions allowed per user.
CCE-27291-4	Set last log in or access notification.
CCE-27457-1	Limit the number of concurrent login sessions allowed per user.

6 Known Issues

See the My Oracle Support document ID 1912063.1.

7 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Exalogic Elastic Cloud STIGfix User's Guide, Release 1.0
E53111-02