Configuring SEC Software for a Cray® XC™, Cray® XE™, or Cray® XK™ System

S–2542–7202

RECORD OF REVISION

S–2542–7202 Published October 2014 Supports the System Management Workstation (SMW) 7.2.UP02 release.

S–2542–7201 Published June 2014 Supports the System Management Workstation (SMW) 7.2.UP01 release.

S–2542–72 Published March 2014 Supports the System Management Workstation (SMW) 7.2.UP00 release.

S–2542–7101 Published December 2013 Supports the System Management Workstation (SMW) 7.1.UP01 release.

Changes to this Document

Configuring SEC Software for a Cray® XC™, Cray® XE™, or Cray® XK™ System S–2542–7202

S–2542–7202

This version of *Configuring SEC Software for a Cray XC, Cray XE, or Cray XK System* supports the System Management Workstation (SMW) 7.2.UP02 release and also includes editorial changes and clarifications.

Added information

- SEC is now disabled by default. When SEC is enabled, it starts automatically at system startup. This document describes how to enable SEC during configuration; see Configuring the SEC Package on page 11.
- The format of SEC log file names is described in About SEC Log Files on page 19.

Changed information

- With this release, the log file directory always includes a partition subdirectory. For an unpartitioned system, the log file directory is `/var/log/sec/p0/sec_logs`. On a partitioned system, the log file directory is the same as in the previous release, but SEC automatically creates the partition-specific subdirectory for each defined partition. See About SEC Log Files on page 19.
- Corrected the command to create a partition-specific copy of the default `SHELL_VARIABLES` configuration file; see Procedure 2 on page 13.
- Added an example of checking that the `sec` process is not running after executing `cray_sec stop`; see Procedure 4 on page 15.
- Clarified the different steps required for unpartitioned and partitioned systems in several procedures.

Removed information

- Removed information about the `%sec_log_dir` variable. With this release, the location of the SEC log directory is not configurable, so the `%sec_log_dir` variable is not used.
- Removed the step to create a p*N* log subdirectory when configuring SEC on a partitioned system. SEC now creates this subdirectory at startup; see Procedure 2 on page 13.
- Removed the procedure on editing the auto boot script to start SEC during system startup. SEC now starts automatically when it is enabled. See Configuring the SEC Package on page 11.

Contents

Page

Introduction [1]

The System Management Workstation (SMW) release includes the Open Source simple event correlator (SEC) package, `sec-2.7.0`, and an SEC support package, `cray-sec-4.0.0`. The SEC support package contains control scripts to manage the starting and stopping of SEC around a Cray mainframe boot session, in addition to other utilities. The SEC support package contains a rule set that is based on Cray Service personnel best practices. References to SEC in this document refer synonymously to both the SEC tool and the Cray provided support package.

The SEC package also includes the `check_xt` utility, which reports on state changes in the Cray system (such as system boots or compute nodes going down), and logs data about the state of nodes and jobs. `check_xt` is designed to work in conjunction with SEC to send email and text alerts about critical system issues.

Note: Cray has attempted to provide the optimal amount of notification information from SEC and `check_xt`. However, due to the intrinsic nature of computer systems and software, the behavior on an individual system is not always predictable. If the notifications from SEC or `check_xt` provide too much or too little information, you can easily customize these tools to meet system needs or site requirements.

In addition, Cray welcomes your feedback about the default notification settings for SEC and `check_xt`. If notifications from SEC or `check_xt` deviate from optimal notification, or if you identify changes that you think others may find helpful, please open a bug report or a request for enhancement (RFE) so that Cray can investigate modifying the distributed tools or making changes available by other means; see To Submit a Bug Report or a Request for Enhancement on page 9.

1.1 Simple Event Correlator (SEC)

The simple event correlator (SEC) is released under the GNU Public License (GPL) v2. As described at http://simple-evcorr.sourceforge.net, SEC is "... an event correlation tool for advanced event processing which can be harnessed for event log monitoring, for network and security management, for fraud detection, and for any other task which involves event correlation. *Event correlation* is a procedure where a stream of events is processed, in order to detect (and act on) certain event groups that occur within predefined time windows. Unlike many other event correlation products which are heavyweight solutions, SEC is a lightweight and platform-independent event correlator which runs as a single process. The user can start it as a daemon, employ it in shell pipelines, execute it interactively in a terminal, run many SEC processes simultaneously for different tasks, and use it in a wide variety of other ways."

A simplified description of SEC is that it parses every line being appended to system log files, watches for specific strings to show up that represent significant events occurring in the system, and sends out email notification that the event has occurred.

Note: You can use SEC with or without the Lightweight Log Management (LLM) system running on your Cray system.

1.1.1 Related SEC Information

Additional information about SEC can be found as follows:

- The `sec-2.7.0` package (RPM) contains the following GPL-related documents:
  - `/usr/share/doc/sec/COPYING`
  - `/usr/share/doc/sec/ChangeLog`
  - `/usr/share/doc/sec/README`
  - `/usr/share/man/man1/sec.1.gz`
- The website: http://simple-evcorr.sourceforge.net

  At that website, the `sec`(1) man page and FAQ are especially helpful, as is *Working with SEC – the Simple Event Correlator* by Jim Brown – a tutorial paper with part 1 (2003) providing an introduction to SEC and part 2 (2004) covering several advanced topics.
- Searches from the newsgroup: http://sourceforge.net/search/?group_id=42089&type_of_search=mlists.
- A brief introduction to SEC under the following article, which is under "Tools, Tips, and Tweaks" at: http://arstechnica.com/information-technology/2005/05/linux-20050519/.
- On an SMW with the SMW release installed, you can type **`man sec`** to display the `sec`(1) man page.

1.1.2 To Submit a Bug Report or a Request for Enhancement

If you encounter an issue when attempting to configure or use SEC or the SEC support package provided, please open a bug report through CrayPort and include sufficient detail, using the following bug information:

Bug Severity: minor

Bug OS: SMW

Bug Product: SMW

Bug Component: HSS Infrastructure

Bug Version: *SMW_release_version*

In addition to bugs or configuration issues, please submit a request for enhancement (RFE) for any beneficial enhancements or local rules you develop (see Changing or Adding a Rule).

Configuring SEC for the Cray System [2]

To configure the base SEC package, you will do the following tasks:

- Edit the configuration files to enable SEC and define required and optional configuration variables. See Configuring the SEC Package on page 11.
- For a partitioned system, create partition-specific configuration files and set the partition variables in these files. See Configuring SEC on a Partitioned System on page 13.
- Customize the recipients for SEC email notifications. By default, email notifications from SEC are sent only to the `crayadm` user on the SMW; most sites add an alias to specify a broader list of recipients of the email generated by SEC. See Setting Up an Email Alias on the SMW on page 16.
- Ensure that email is configured on the SMW. See Configuring the SEC Package on page 11.

2.1 Configuring the SEC Package

The SEC configuration procedure depends on whether your system is partitioned. On an unpartitioned system, you modify the released configuration files, which control SEC for entire system. On a partitioned system, you must create separate configuration files for each partition that will run SEC.

2.1.1 Configuring SEC on an Unpartitioned System

To configure the SEC package, you define the variables that enable SEC and specify the mainframe hostname and its serial number. You can also specify who should receive SEC notification and/or verification email.

On an unpartitioned system, SEC runs on the entire system (also referred to as partition `p0`). The configuration files `/opt/cray/sec/default/SEC_VARIABLES` and `/opt/cray/sec/default/SHELL_VARIABLES` define the SEC settings for the system.

Procedure 1. Configuring SEC on an unpartitioned system

If you made changes to the SEC configuration files in a past release, the SMW installation procedures directed you to save backup copies of the files before upgrading or updating the SMW software. This procedure requires the backup copies of `/opt/cray/sec/default/SEC_VARIABLES` and `/opt/cray/sec/default/SHELL_VARIABLES`.

1. Log in as `crayadm` on the SMW.
2. Edit the `/opt/cray/sec/default/SEC_VARIABLES` file.

   ```
   crayadm@smw:~> vi /opt/cray/sec/default/SEC_VARIABLES
   ```

3. Change the `%host` variable to the hostname of the Cray mainframe. The released file contains an example value for this variable.
4. Change the `%SNUM` variable to the serial number of the Cray mainframe. The released file contains an example value for this variable.
5. (Optional.) Modify the variables that specify the recipients of SEC notification and verification email.
   a. (Optional.) Change the `%list` variable to specify an email alias and/or a list of recipients to receive the SEC notification email. The default recipient is `crayadm`.
   b. (Optional.) Change the `%list_verify_sec` variable to specify an email alias and/or a list of recipients to receive SEC verification email (intended for testing SEC).
6. If you made changes to `/opt/cray/sec/default/SEC_VARIABLES` in a past release, merge any local changes from the backup copies into the upgraded version.
7. Save your changes and exit the editor.
8. Edit the `/opt/cray/sec/default/SHELL_VARIABLES` file.

   ```
   crayadm@smw:~> vi /opt/cray/sec/default/SHELL_VARIABLES
   ```

9. Change the `SEC_ENABLE` variable to `"yes"`. By default, this variable is set to `"no"`.
10. If you made changes to `/opt/cray/sec/default/SHELL_VARIABLES` in a past release, merge any local changes from the backup copies into the upgraded version.
11. Save your changes and exit the editor.
12. If necessary, configure email on the SMW. SEC requires email on the SMW, which is usually an optional feature. To configure email, see http://www.postfix.org/BASIC_CONFIGURATION_README.html.

SEC will start automatically at the next system boot. To activate the SEC configuration on a running system, you must start or restart SEC to read in the changed values; see Manually Starting and Stopping SEC on page 15 or Restarting SEC After Customizing Rules on page 18.

2.1.2 Configuring SEC on a Partitioned System

To configure the SEC package, you define the variables that enable SEC and specify the mainframe hostname and its serial number. You can also specify who should receive SEC notification and/or verification email.

On a partitioned system, the SEC configuration for individual partitions is controlled by the configuration files `/opt/cray/sec/default/SEC_VARIABLES_p`*N* and `/opt/cray/sec/default/SHELL_VARIABLES_p`*N*, where *N* is the partition number. For example, the files for partition 2 would be `SEC_VARIABLES_p2` and `SHELL_VARIABLES_p2`.

To configure SEC to run on a specific partition, you must create partition-specific files in the directory `/opt/cray/sec/default/` and set the partition variables in these files.

Procedure 2. Configuring SEC on an individual partition

If you made changes to the SEC configuration files in a past release, the SMW installation procedures directed you to save backup copies of the files before upgrading or updating the SMW software. This procedure requires the backup copies of `/opt/cray/sec/default/SEC_VARIABLES_p`*N* and `/opt/cray/sec/default/SHELL_VARIABLES_p`*N*.

1. Log in as `crayadm` on the SMW.
2. Copy the default configuration file `/opt/cray/sec/default/SEC_VARIABLES` into a new partition-specific file `SEC_VARIABLES_p`*N*, where *N* is the partition number.

```
crayadm@smw:~> cp /opt/cray/sec/default/SEC_VARIABLES \
/opt/cray/sec/default/SEC_VARIABLES_pN
```

3. Edit the `/opt/cray/sec/default/SEC_VARIABLES_p`*N* file.

```
crayadm@smw:~> vi /opt/cray/sec/default/SEC_VARIABLES_pN
```

4. Change the `%partition_id` variable to the partition name (for example, `p2`).

```
assign %partition_id pN ;\
```

5. Change the `%host` variable to the hostname of the Cray mainframe. The released file contains an example value for this variable.
6. Change the `%SNUM` variable to the serial number of the Cray mainframe. The released file contains an example value for this variable.

7. (Optional.) Modify the variables that specify the recipients of SEC notification and verification email.

   a. (Optional.) Change the `%list` variable to specify an email alias and/or a list of recipients to receive the SEC notification email. The default recipient is `crayadm`.

   b. (Optional.) Change the `%list_verify_sec` variable to specify the email alias and/or a list of recipients to receive SEC verification email (intended for testing SEC).

8. If you made changes to `/opt/cray/sec/default/SEC_VARIABLES_p`*N* in a past release, merge any local changes from the backup copies into the upgraded version.

9. Save your changes and exit the editor.

10. Copy the default `/opt/cray/sec/default/SHELL_VARIABLES` file into a new partition-specific file `SHELL_VARIABLES_p`*N*, where *N* is the partition number.

```
crayadm@smw:~> cp /opt/cray/sec/default/SHELL_VARIABLES \
/opt/cray/sec/default/SHELL_VARIABLES_pN
```

11. Edit the `/opt/cray/sec/default/SHELL_VARIABLES_p`*N* file.

    ```
    crayadm@smw:~> vi /opt/cray/sec/default/SHELL_VARIABLES_pN
    ```

12. Change the `SEC_ENABLE` variable to `"yes"`. By default, this variable is set to `"no"`.

13. Change the `PART_ID` variable to the partition name (for example, `p2`).

    ```
    PART_ID=pN
    ```

14. If you made changes to `/opt/cray/sec/default/SHELL_VARIABLES_p`*N* in a past release, merge any local changes from the backup copies into the upgraded version.

15. Save your changes and exit the editor.

16. If necessary, configure email on the SMW. SEC requires email on the SMW, which is usually an optional feature. To configure email, see http://www.postfix.org/BASIC_CONFIGURATION_README.html.

SEC will start automatically at the next system boot. To activate the SEC configuration on a running system, you must start or restart SEC to read in the changed values; see Manually Starting and Stopping SEC on page 15 or Restarting SEC After Customizing Rules on page 18.

2.2 Manually Starting and Stopping SEC

Procedure 3. Manually starting SEC

If the mainframe is already up and is running, you can use the `cray_sec start` command to manually start SEC.

Note: This command will stop the prior instance of SEC if it was not stopped automatically during a normal mainframe shutdown.

1. Log in as `crayadm` on the SMW.
2. The command to start SEC depends on whether you have an unpartitioned system or a partitioned system.
   - For an unpartitioned system, use this command to manually start SEC:

     ```
     crayadm@smw:~> /opt/cray/sec/default/bin/cray_sec start
     ```

   - For a partitioned system, include the partition number as an argument to the `cray_sec start` command. Specify the partition as p*N*, where *N* is the partition number.

     ```
     crayadm@smw:~> /opt/cray/sec/default/bin/cray_sec start pN
     ```

Procedure 4. Manually stopping SEC

1. Log in as `crayadm` on the SMW.
2. The command to stop SEC depends on whether you have an unpartitioned system or a partitioned system.
   - For an unpartitioned system, use this command to manually stop SEC:

     ```
     crayadm@smw:~> /opt/cray/sec/default/bin/cray_sec stop
     ```

   - For a partitioned system, include the partition number as an argument to this command. Specify the partition as p*N*, where *N* is the partition number.

     ```
     crayadm@smw:~> /opt/cray/sec/default/bin/cray_sec stop pN
     ```

3. Verify that SEC has stopped by ensuring that the `sec` process is not running. For example, the output of `ps` should not show a process named `sec`.

```
crayadm@smw:~> ps aux | grep sec
root      3243  0.0  0.0  34764  2096 ?        S    Sep29   0:01 hald-addon-storage: polling /dev/sr0
crayadm  48717  0.0  0.0   5732   824 pts/17   S+   15:06   0:00 grep sec
```

If necessary, you can stop SEC by killing the process ID (pid) of the SEC process, which takes the same action as executing the `cray_sec stop` command.

2.3 Setting Up an Email Alias on the SMW

By default, SEC sends email notifications only to the `crayadm` user on the SMW. Most sites add an alias to `/etc/aliases` on the SMW in order to specify a broader list of recipients for SEC email notifications.

Procedure 5. Setting up an email alias on the SMW

1. Log in as `root` on the SMW.
2. Create a backup copy of the `/etc/aliases` file.

   ```
   smw:~ # cd /etc
   smw:~ # cp -p aliases aliases_`date +%d%b%y_%H%M.%S`
   ```

3. Edit `/etc/aliases`.
4. Add the new alias at the end. The following example creates the alias `mysite_monitoring` that includes two recipients, `mysite_support@mycray.com` and `sysadm@mysite.edu`.

   ```
   mysite_monitoring:      mysite_support@mycray.com,sysadm@mysite.edu
   ```

   Important: Do not include `crayadm` in an email alias. Always include `crayadm` in the `EMAIL_LIST` configuration variable to ensure that `crayadm` always receives SEC alerts on the SMW, even if there are errors in `/etc/aliases` or delays in email delivery to other systems.

5. Save your changes and exit the editor.
6. Execute the following command with no options to build a new copy of the aliases database from the updated `/etc/aliases` file.

   ```
   smw:~ # newaliases
   ```

7. Exit from `root`.
8. Ensure that the `%list` variable in the `/opt/cray/sec/default/SEC_VARIABLES` file specifies the new email alias. For more information, see Configuring the SEC Package on page 11.
9. Start or restart SEC to activate the email alias change; see Manually Starting and Stopping SEC on page 15 or Restarting SEC After Customizing Rules on page 18.
10. After starting SEC, check mail on the SMW for any email delivery failures.

Customizing SEC Rules [3]

An SEC rule defines a monitored system event and describes how to respond to that event. In almost all cases, there is one SEC rule per SEC rule file. A rule file has the suffix `.sr`.

The default rules are located in the `/opt/cray/sec/default/rules/` directory. The variables used by those rules and the SEC scripts are defined in the `SEC_VARIABLES` configuration file; see Chapter 2, Configuring SEC for the Cray System on page 11.

SEC is configured to send email by default when a rule with notification logic is triggered. While the email frequency should be minimal, it will be a function of how many rules you have active (with notification logic), how well the rules are defined (to protect against false positives or to suppress insignificant occurrences of a signature), and how large or stable your system may be. Please keep the notification frequency in mind if you plan to change existing rules or create new rules. Cray recommends that you test the mail frequency to a local (on the SMW) mail box or to an isolated email address to understand the notification behavior on your system.

3.1 Disabling a Rule

SEC will skip any rule file that does not have a `.sr` suffix. To disable a rule, change the file suffix from `.sr` to something else. Cray recommends that you append `-skip` or `-dist` (for a distributed rule) to the file suffix. If necessary, you can remove the rule file.

After disabling a rule, you must restart SEC if it is already running; see Restarting SEC After Customizing Rules on page 18.

3.2 Changing or Adding a Rule

Cray recommends that you store any local (site-customized) SEC rules in the directory `/opt/cray/sec/default/rules/local`. Keeping local rules separated from the distributed rules in the `/opt/cray/sec/default/rules/` directory will help simplify the process of upgrading the standard rules, and of the general management of local rules.

If you modify a distributed rule, Cray recommends that you store the localized version of that rule in the `local` subdirectory. Usually, you will also disable the distributed version of that rule by changing the suffix to `-skip` or `-dist`, as described in Disabling a Rule on page 17.

Important: Because the default rule base may change, Cray recommends that you verify the behavior of your local rules between upgrades and that you review any previously disabled or modified rules (or versions thereof) between upgrades.

If you identify new rules or features that you think others may find helpful, please notify Cray; see To Submit a Bug Report or a Request for Enhancement on page 9.

3.3 Restarting SEC After Customizing Rules

To activate changes after disabling, changing, or adding a rule, you must restart SEC if it is already running.

Procedure 6. Restarting SEC after customizing rules

1. Log in as `crayadm` on the SMW.
2. The command to restart SEC depends on whether you have an unpartitioned system or a partitioned system.
   - For an unpartitioned system, use this command to restart SEC:

     ```
     crayadm@smw:~> /opt/cray/sec/default/bin/cray_sec restart
     ```

   - For a partitioned system, include the partition number as an argument to the `cray_sec restart`command. Specify the partition as p*N*, where *N* is the partition number.

     ```
     crayadm@smw:~> /opt/cray/sec/default/bin/cray_sec restart pN
     ```

3. To verify the actions being taken by SEC, examine the SEC log files. For more information, see Chapter 4, Testing SEC on page 19.

Testing SEC [4]

4.1 About SEC Log Files

SEC stores log output from the SEC process (`sec`) in the `/var/log/sec/p`*N*`/sec_logs/` directory. The name of the `p`*N* subdirectory depends on whether the system is partitioned.

- On an unpartitioned system, the SEC log directory is `/var/log/sec/p0/sec_logs/`. The `p0` partition represents the entire system.
- On a partitioned system, the SEC log directory is `/var/log/sec/p`*N*`/sec_logs/`, where *N* is the partition number.

SEC creates a new log file each time it starts or restarts. The log file name is in the format `sec_log.pN-`*yyyymmddtHHMMSS*, where *N* is the partition number (`p0` for an unpartitioned system) and *yyyymmddtHHMMSS* is a time stamp.

The file `/var/log/sec/p`*N*`/seclog` is a symbolic link to the current log file.

4.2 Testing SEC Rules

If you want to test SEC, especially if you have developed or modified rules, you can write strings to the file `/var/log/sec/p`*N*`/control_and_test_portal`. For each rule that you want to test, write a string that matches the regular expression of the rule.

For example, the rule `/opt/cray/sec/default/rules/base/bug.sr` looks for a match to the following regular expression:

```
(\d\d:\d\d:\d\d).*(c\d+-\d+c\d+s\d+[sn]\d+)\W+(BUG|\w+\sBUG)
```

To test this rule, you could navigate to the `/var/log/sec/p`*N*`/` directory and write the following string to the `control_and_test_portal` file:

```
smw:/var/log/sec/pN/> echo "2012-05-14T20:12:09.941558-05:00 c9-9c1s5n1 BUG: unable to \
handle kernel paging request at 00000000000022d0" > control_and_test_portal
```

Important: Designing a test string must be done very carefully because all active rules can be triggered from strings going to this file.

To check whether SEC had any problems parsing the rules when starting or restarting, review the log files and search for `fail`, `error`, and `Warning` messages.

Tip: If you restarted SEC after modifying or adding a rule, first search for the string `restart` in the log file, then look for any following `fail`, `error`, or `Warning` messages.

Using check_xt [5]

5.1 About check_xt

The SEC package includes the check_xt utility, which reports on state changes in the Cray system (such as system boots or compute nodes going down), and logs data about the state of nodes and jobs. check_xt is designed to work in conjunction with SEC to send email and text alerts about critical system issues.

The check_xt utility consists of the shell script check_xt.sh and the wrapper script check_xt_wrapper.ex, which is an Expect script that provides a time-out capability for the ssh calls to the boot node made in check_xt.sh. Usually, an administrator creates a cron job to run check_xt_wrapper.ex every five minutes.

The check_xt utility monitors when the Cray system enters a critical state. By default, the critical states are:

- The number of up or suspect nodes drops below a specified threshold.
- The SMW cannot ping the boot node (a ping operation from the SMW to the boot node fails).
- The boot node cannot ping the SDB node (a ping operation from the boot node to the SDB node fails).

The following state changes can also be included in the alerts:

- System shutdown began.
- The system has been rebooted (the boot node was previously unpingable and the number of up or suspect nodes was below the threshold and is now greater than or equal to this value).

check_xt gathers system status data and statistics in the /var/log/check_xt/ directory. This information can often be a good source for historical reference.

5.2 Configuring check_xt

To enable check_xt, you must set required and optional configuration variables, define an optional email alias for notifications, then create a crontab entry to run check_xt_wrapper.ex.

Procedure 7. Configuring check_xt

Important: check_xt requires passwordless ssh login functionality between crayadm on the SMW to root on the boot node.

1. Log in as crayadm on the SMW.
2. Edit /opt/cray/sec/default/bin/check_xt.sh to set the required configuration variables.
   a. Change the SN variable to the system's serial number.
   b. Change the SYSTEM_NAME variable to the site name and Cray system hostname, using the format *Sitename-hostname*.
   c. Change the EMAIL_LIST variable to the list of email addresses to notify. The default recipient is crayadm.

      Cray recommends that you keep crayadm in EMAIL_LIST rather than in an email alias. Doing so ensures that crayadm always receives SEC alerts on the SMW, even if there are errors in /etc/aliases or delays in email delivery to other systems.
   d. Change the SCHEDULER variable to the scheduler-specific portion of the path to the qstat command (/opt/$SCHEDULER/default). Set this variable to the appropriate value for your system's scheduler, such as pbs or torque (the default).

      Tip: To disable the call to qstat, remove the comment character from the line that sets QSTAT to/bin/true.
3. (Optional.) Customize the following variables in check_xt.sh.

   TEXT_LIST Lists the recipients for text alerts, which are intended as notification of critical problems.

   MIN_LIMIT_UP_OR_SUSPECT

   Specifies the number of nodes required to be either up or suspect (that is, not down). Going below this value will send a text alert to the recipients defined in TEXT_LIST. See the comments in check_xt.sh for guidelines on an appropriate initial value for this variable. The default is 1.

   NOTIFY_SUSPECT_COUNT

   Specifies the threshold for an alert about nodes in the suspect state. check_xt sends an alert when this amount is exceeded, then sends a follow-up alert when the number of suspect nodes returns to 0. See the comments in check_xt.sh for guidelines on an appropriate initial value for this variable.

To disable this alert, set NOTIFY_SUSPECT_COUNT to a number that is greater than the number of nodes in the system. The default is 2500 (disabled on most systems).

4. Save your changes and exit the editor.
5. Edit /opt/cray/sec/default/bin/check_xt_wrapper.ex to set the required Expect script variables.

   Note: The syntax for Expect script variables is different from the shell script syntax used in check_xt.sh.

   a. Change the SYSTEM_NAME variable to the site name and Cray system hostname, using the format *Sitename-hostname*. Use the same site name and hostname as in the SYSTEM_NAME variable in check_xt.sh.

   b. Change the EMAIL_LIST variable to the list of email addresses to notify about any time-out issues. Use the same list as in the SYSTEM_NAME variable in check_xt.sh. The default recipient is crayadm.

   c. Save your changes and exit the editor.
6. (Optional.) Define and activate a monitoring email alias on the SMW.

   a. Log in as root.

   b. Edit the /etc/aliases file.

   c. Add a monitoring alias at the end of the file, using the following format:

*systemname*_monitoring: *user*@*site*.com, *site_systemname*_monitoring@cray.com

   For example:

```
MyCo_k2_monitoring:     crayadm,k2_monitoring@MyCo.com,MyCo_k2_monitoring@cray.com
```

   d. Save your changes and exit the editor.

   e. Execute the following command, with no options, to build a new copy of the aliases database from the updated /etc/aliases file.

```
smw:~ # newaliases
```

   f. Exit from root.
7. As crayadm, create a crontab entry to call check_xt_wrapper.ex frequently. The following example crontab entry calls check_xt_wrapper.ex every five minutes.

```
*/5 * * * * /opt/cray/sec/default/bin/check_xt_wrapper.ex
```

8. Ensure that passwordless ssh is configured between crayadm on the SMW to root on the boot node. For information on setting up passwordless ssh, see *Managing System Software for the Cray Linux Environment* (S–2393).