Chapter 2
Configuring the SAE with the SRC CLI

This chapter describes how to use the SRC CLI to configure general SAE properties. You can use the SRC CLI to configure the SAE on a Solaris platform or on a C-series Controller.

To use the C-Web interface to configure an SAE on a Solaris platform or on a C-series Controller, see *Chapter 4, Managing SAE Data with the C-Web Interface*.

Topics in this chapter include:

- Configuring LDAP Access to Directory Data on page 13

- Storing Subscriber and Service Session Data on page 23

- Configuring the Session Store Feature on page 24

- Configuring the Number of Threads for Sessions on page 29

Configuring LDAP Access to Directory Data

The SRC software stores subscriber, service, persistent login, policy, router, and cached subscriber profiles and session data in a directory. The SAE uses LDAP to store and retrieve the data.

If you do not store data in the local directory, you need to configure the LDAP connections to the directories in which the data is stored. You can also select the filter that the SAE uses to search for subscriptions in the directory and directory eventing parameters for data stored in the directory.

The tasks to configure LDAP access to directory data are:

- (Optional) Configuring Access Through LDAPS to Service and Subscriber Data on page 14

- Configuring Access to Subscriber Data on page 15

- Configuring Access to Service Data on page 17

- Configuring Access to Policy Data on page 18

- Configuring Access to the Persistent Login Cache on page 19

- Configuring the Location of Network Device Data on page 21

- Enabling Automatic Discovery of Changes in SAE Configuration Data on page 21

- Setting the Timeout and Number of Events for SAE Directory Eventing on page 22

Configuring Access Through LDAPS to Service and Subscriber Data

You can secure connections between a router and an external directory that contains service data or subscriber data, and you can configure the router to use LDAPS when it connects to the same data source.

Use the following configuration statements to configure access through LDAPS to service data and subscriber data:

```
shared sae configuration ldap service-data {
    (ldaps);
}
```

```
shared sae configuration ldap subscriber-data {
    (ldaps);
}
```

To use LDAPS to secure connections between a router and an external directory:

1. Configure the directory connection from the SAE to use LDAPs. For example:

   user@host# **set shared sae configuration ldap service-data ldaps**

   user@host# **set shared sae configuration ldap subscriber-data ldaps**

2. In the router initialization script you specify the directory context.

   The */opt/UMC/sae/lib/poolPublisher.py* script and the */opt/UMC/sae/lib/IorPublisher.py* script provide examples of how to configure a directory context, For example, from the */opt/UMC/sae/lib/IorPublisher.py* script:

   dirContext = Ssp.registry.get('ServiceDataSource.component').getContext()

   In addition, you can change the directory context.

   For information about how to use InitialDirContext class or the DirContext class to specify directory context, see:

http://java.sun.com/j2se/1.4.2/docs/api/javax/naming/directory/
InitialDirContext.html

http://java.sun.com/j2se/1.4.2/docs/api/javax/naming/directory/DirContext.html

Related Topics

■ *Configuring Access to Subscriber Data* on page 15

■ *Configuring Access to Service Data* on page 17

Configuring Access to Subscriber Data

Use the following configuration statements to configure access to subscriber data:

```
shared sae configuration ldap subscriber-data {
    subscription-loading-filter (subscriberRefFilter | objectClassFilter);
    load-subscriber-schedules;
    login-cache-dn login-cache-dn;
    session-cache-dn session-cache-dn;
    server-address server-address;
    dn dn;
    authentication-dn authentication-dn;
    password password;
    directory-eventing;
    polling-interval polling-interval;
    (ldaps);
}
```

To configure SAE access to subscriber data:

1. From configuration mode, access the configuration statement that configures SAE access to subscriber data in the directory. In this sample procedure, the subscriber data is configured in the se-region group.

    user@host# **edit shared sae group se-region configuration ldap subscriber-data**

2. Select the filter that the SAE uses to search for subscriptions in the directory when the SAE loads a subscription to a subscriber reference filter.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set subscription-loading-filter** (subscriberRefFilter | objectClassFilter)

3. (Optional) Enable loading of subscriber schedules.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set load-subscriber-schedules**

4. Specify the subtree in the directory in which subscriber information is stored.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set login-cache-dn** *login-cache-dn*

5. Specify the subtree in the directory in which persistent session data is cached.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set session-cache-dn** *session-cache-dn*

6. (Optional) Specify the directory server that stores subscriber information.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set server-address** *server-address*

7. Specify the subtree in the directory where subscriber data is cached.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set dn** *dn*

8. (Optional) Specify the DN that the SAE uses to authenticate access to the directory server.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set authentication-dn** *authentication-dn*

9. (Optional) Specify the password used to authenticate access to the directory server.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set password** *password*

10. (Optional) Enable automatic discovery of changes in subscriber profiles.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set directory-eventing**

11. Set the frequency for checking the directory for updates.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set polling-interval** *polling-interval*

12. Enable LDAPS as the secure protocol for connections to the server that stores subscriber data.

    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# **set ldaps**

13. (Optional) Verify your configuration.

    ```
    [edit shared sae group se-region configuration ldap subscriber-data]
    user@host# show
    subscription-loading-filter objectClassFilter;
    load-subscriber-schedules;
    login-cache-dn o=users,<base>;
    session-cache-dn o=PersistentSessions,<base>;
    server-address 127.0.0.1;
    dn o=users,<base>;
    authentication-dn cn=ssp,o=components,o=operators,<base>;
    password ********;
    directory-eventing;
    polling-interval 30;
    ldaps;
    ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

- *Configuring Access Through LDAPS to Service and Subscriber Data* on page 14

Configuring Access to Service Data

Use the following configuration statements to configure access to service data:

```
shared sae configuration ldap service-data {
    server-address server-address;
    dn dn;
    authentication-dn authentication-dn;
    password password;
    directory-eventing;
    polling-interval polling-interval;
    (ldaps);
}
```

To configure SAE access to service data:

1. From configuration mode, access the configuration statement that configures SAE access to service data in the directory. In this sample procedure, the service data is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration ldap service-data**

2. (Optional) Specify the directory server that stores service data.

   [edit shared sae group se-region configuration ldap service-data]
   user@host# **set server-address** *server-address*

3. Specify the subtree in the directory where service data is cached.

   [edit shared sae group se-region configuration ldap service-data]
   user@host# **set dn** *dn*

4. (Optional) Specify the DN that the SAE uses to authenticate access to the directory server.

   [edit shared sae group se-region configuration ldap service-data]
   user@host# **set authentication-dn** *authentication-dn*

5. (Optional) Specify the password used to authenticate access to the directory server.

   [edit shared sae group se-region configuration ldap service-data]
   user@host# **set password** *password*

6. (Optional) Enable or disable automatic discovery of changes to service data.

   [edit shared sae group se-region configuration ldap service-data]
   user@host# **set directory-eventing**

7. Set the frequency for checking the directory for updates.

   [edit shared sae group se-region configuration ldap service-data]
   user@host# **set polling-interval** *polling-interval*

8. Enable LDAPS as the secure protocol for connections to the server that stores service data.

   edit shared sae group se-region configuration ldap service-data]
   user@host# **set ldaps**

9. (Optional) Verify your configuration.

   ```
   [edit shared sae group se-region configuration ldap service-data]
   user@host# show
   server-address 10.10.45.3;
   dn <base>;
   authentication-dn <base>;
   password ********;
   directory-eventing;
   polling-interval 30;
   ldaps;
   ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

- *Configuring Access Through LDAPS to Service and Subscriber Data* on page 14

Configuring Access to Policy Data

Use the following configuration statements to configure access to policy data:

```
shared sae configuration ldap policy-data {
    policy-dn policy-dn;
    parameter-dn parameter-dn;
    directory-eventing;
    polling-interval polling-interval;
}
```

To configure SAE access to subscriber data:

1. From configuration mode, access the configuration statement that configures SAE access to policy data in the directory. In this sample procedure, the policy data is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration ldap policy-data**

2. Specify the subtree in the directory in which policy data stored.

   [edit shared sae group se-region configuration ldap policy-data]
   user@host# **set policy-dn** *policy-dn*

3. Specify the subtree in the directory in which policy parameter data is cached.

    [edit shared sae group se-region configuration ldap policy-data]
    user@host# **set parameter-dn** *parameter-dn*

4. (Optional) Enable or disable automatic discovery of changes to policy data.

    [edit shared sae group se-region configuration ldap policy-data]
    user@host# **set directory-eventing**

5. Set the frequency for checking the directory for updates.

    [edit shared sae group se-region configuration ldap policy-data]
    user@host# **set polling-interval** *polling-interval*

6. (Optional) Verify your configuration.

    ```
    [edit shared sae group se-region configuration ldap policy-data]
    user@host# show
    policy-dn o=Policy,<base>;
    parameter-dn o-Parameters,<base>;
    directory-eventing;
    polling-interval 30;
    ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Configuring Access to the Persistent Login Cache

Use the following configuration statements to configure access to persistent login cache data:

```
shared sae configuration ldap persistent-login-cache {
    server-address server-address;
    dn dn;
    authentication-dn authentication-dn;
    password password;
    directory-eventing;
    polling-interval polling-interval;
    (ldaps);
}
```

To configure SAE access to persistent login cache data:

1. From configuration mode, access the configuration statement that configures SAE access to persistent login cache data in the directory. In this sample procedure, the persistent login cache data is configured in the se-region group.

    user@host# **edit shared sae group se-region configuration ldap persistent-login-cache**

2. (Optional) Specify the directory server that stores service data.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set server-address** *server-address*

3. Specify the subtree in the directory where persistent login cache data is cached.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set dn** *dn*

4. (Optional) Specify the DN that the SAE uses to authenticate access to the
   directory server.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set authentication-dn** *authentication-dn*

5. (Optional) Specify the password used to authenticate access to the directory
   server.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set password** *password*

6. (Optional) Enable automatic discovery of changes to persistent login cache
   data.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set directory-eventing**

7. Set the frequency for checking the directory for updates.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set polling-interval** *polling-interval*

8. Enable LDAPS as the secure protocol for connections to the server that stores
   persistent login cache data.

   [edit shared sae group se-region configuration ldap persistent-login-cache]
   user@host# **set ldaps**

9. (Optional) Verify your configuration.

```
[edit shared sae group se-region configuration ldap persistent-login-cache]
user@host# show
dn "o=authCache, <base>";
directory-eventing;
polling-interval 30;
ldaps;
```

Related Topics

■ For information about setting up SAE groups, see *SRC-PE Getting Started Guide,
   Chapter 21, Setting Up an SAE with the SRC CLI.*

Configuring the Location of Network Device Data

Use the following configuration statement to configure access to network device data:

```
shared sae configuration ldap {
    network-dn network-dn;
}
```

To configure SAE access to network device data:

1. From configuration mode, access the configuration statement that configures SAE access to network device data in the directory. In this sample procedure, the network device data is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration ldap**

2. Specify the subtree in the directory where network device data is stored.

   ```
   [edit shared sae group se-region configuration ldap]
   user@host# set network-dn network-dn
   ```

3. Verify your configuration.

   ```
   [edit shared sae group se-region configuration ldap]
   user@host# show network-dn
   network-dn o=Network,<base>;
   ```

Related Topics

■ For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Enabling Automatic Discovery of Changes in SAE Configuration Data

Use the following configuration statement to enable automatic discovery of changes in SAE configuration data:

```
shared sae configuration ldap {
    enable-directory-eventing;
}
```

To enable automatic discovery of changes in SAE configuration data:

1. From configuration mode, access the configuration statement that enables automatic discovery of changes in SAE configuration data in the directory. In this sample procedure, automatic discovery is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration ldap**

2. Enable automatic discovery of changes to SAE configuration data.

   ```
   [edit shared sae group se-region configuration ldap]
   user@host# enable-directory-eventing
   ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Setting the Timeout and Number of Events for SAE Directory Eventing

Use the following configuration statements to set the directory eventing timeout and the number of simultaneous events that the SAE can receive from the directory:

```
shared sae configuration ldap directory-eventing {
    timeout timeout;
    dispatcher-pool-size dispatcher-pool-size;
}
```

To configure the directory eventing timeout and the number of simultaneous events that the SAE can receive from the directory:

1. From configuration mode, access the configuration statement that configures SAE directory eventing. In this sample procedure, directory eventing is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration ldap directory-eventing**

2. Specify the maximum time that the directory eventing system waits for the directory to respond.

   [edit shared sae group se-region configuration ldap directory-eventing]
   user@host# **set timeout** *timeout*

3. Specify the number of events that the SAE can receive from the directory simultaneously.

   [edit shared sae group se-region configuration ldap directory-eventing]
   user@host# **set dispatcher-pool-size** *dispatcher-pool-size*

4. (Optional) Verify your configuration.

   ```
   [edit shared sae group se-region configuration ldap directory-eventing]
   user@host# show
   timeout 60;
   dispatcher-pool-size 1000;
   ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Storing Subscriber and Service Session Data

To aid in recovering from an SAE failover, the SAE stores subscriber and service session data in flat files on the SAE host. The SRC component that controls the storage of session data on the SAE is called the session store. The session store queues data and then writes the data to session store files on the SAE host's disk. After the data has been written to disk, it can survive a server reboot.

You can configure how the SAE stores session data for JUNOSe routers, JUNOS routing platforms, simulated routers, and *PacketCable Multimedia Specification* (PCMM) devices.

Session Store Files

Session store files are numbered flat files. Session store files are located in a directory on the SAE host. You can configure the size of session store files. After the maximum size has been reached, the session store creates a new file and begins writing data to the new file.

Store operations, such as adding a session to the store (put store operations) or removing a session from the store (remove store operations), are queued in a buffer before they are written to the session store file. You can configure parameters that determine when the session store writes a queue to a session store file.

Session store files are deleted if they have not been modified and if no session activity has taken place for one week. All the data files that contain the sessions associated with a particular virtual router are deleted at the same time.

Active and Passive Session Stores

You can have a community of SAEs and duplicate session store data on each SAE in the community in case of an SAE failover. SAE communities are made up of SAEs that you configure as connected SAEs for a virtual router object.

SAEs in a community are given the role of either active SAE or passive SAE. The active SAE keeps session data up to date within the community. Each active session store opens a Transmission Control Protocol (TCP) connection to its passive SAE. The TCP connection triggers the creation of a passive session store in that SAE. When the active session store writes operations to the session store file, it passes them to passive session stores on all SAEs in the community.

When you modify a community, wait for passive session stores on the new community members to be updated before you shut down the currently active SAE. Otherwise, if you add a new member to a community, and then a failover from the current active SAE to the new member is triggered immediately, the new member's session store may not have received all data from the active SAE's session store.

Standby SAEs

In a community of SAEs, one SAE can provide redundancy for the active SAE. The redundant (standby) SAE connects to the active SAE through a COPS-PR connection. State as well as session data is replicated from the active SAE to the standby SAE to reduce the failover time from one SAE to another.

A standby SAE can respond to SAE failures and connection failures between an SAE and a JUNOSe router. Connection failures between an active SAE and a standby SAE may not be immediately detected, because each SAE continues to function for a period of time. When a standby SAE does detect that state information is different on the two SAEs, it resynchronizes data between the two.

NOTE: We recommend that you use a highly reliable and available connection between an active SAE and a standby SAE to ensure availability of the two SAEs.

Session Store File Rotation

The session store periodically rotates the session store files. During rotation, the session store copies put store operations for live sessions from the oldest file to the end of the newest file. (Live sessions are sessions that have been created but not yet deleted.) It then deletes the oldest file. Sessions are rotated in batches, and you can configure the number of sessions that are rotated at the same time, and how much disk space is used by live sessions before files are rotated. No session store activity can take place while a batch of sessions is rotated.

Configuring the Session Store Feature

You can configure three things for the session store feature:

- Configure session store parameters for a router or device driver. See *Configuring Session Store Parameters for a Device Driver* on page 24.

- Configure global session store parameters that are shared by all session store instances (active or passive) on the SAE. See *Configuring Global Session Store Parameters* on page 27.

- Reduce the size of session objects that the SAE sends across the network for the session store feature. See *Reducing the Size of Objects for the Session Store Feature* on page 28.

Configuring Session Store Parameters for a Device Driver

Use the following configuration statements to configure session store parameters within a device driver configuration:

shared sae configuration driver (junos | junose | pcmm | simulated | third-party) session-store {

```
        maximum-queue-age maximum-queue-age;
        maximum-queued-operations maximum-queued-operations;
        maximum-queue-size maximum-queue-size;
        maximum-file-size maximum-file-size;
        minimum-disk-space-usage minimum-disk-space-usage;
        rotation-batch-size rotation-batch-size;
        maximum-session-size maximum-session-size;
        disk-load-buffer-size disk-load-buffer-size;
        network-buffer-size network-buffer-size;
        retry-interval retry-interval;
        communications-timeout communications-timeout;
        load-timeout load-timeout;
        idle-timeout idle-timeout;
        maximum-backlog-ratio maximum-backlog-ratio;
        minimum-backlog minimum-backlog;
}
```

To configure session store parameters within a device driver configuration:

1. From configuration mode, access the configuration statement that configures the session store for your device driver. In this sample procedure, the session store for a JUNOS device driver is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration driver junos session-store**

2. (Optional) Specify the maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

   [edit shared sae group se-region configuration driver junos session-store]
   user@host# **set maximum-queue-age** *maximum-queue-age*

3. (Optional) Specify the number of buffered store operations that are queued before the queue is written to a session store file.

   [edit shared sae group se-region configuration driver junos session-store]
   user@host# **set maximum-queued-operations** *maximum-queued-operations*

4. (Optional) Specify the maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

   [edit shared sae group se-region configuration driver junos session-store]
   user@host# **set maximum-queue-size** *maximum-queue-size*

5. (Optional) Specify the maximum size of session store files.

   [edit shared sae group se-region configuration driver junos session-store]
   user@host# **set maximum-file-size** *maximum-file-size*

6. (Optional) Specify the percentage of space in all session store files that is used by live sessions.

   [edit shared sae group se-region configuration driver junos session-store]
   user@host# **set minimum-disk-space-usage** *minimum-disk-space-usage*

7. (Optional) Specify the number of sessions that are rotated from the oldest file to the newest file at the same time that the oldest session store file is rotated.

[edit shared sae group se-region configuration driver junos session-store]
user@host# **set rotation-batch-size** *rotation-batch-size*

8. (Optional) Specify the maximum size of a single subscriber or service session.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set maximum-session-size** *maximum-session-size*

9. (Optional) Specify the size of the buffer that is used to load all of a session
    store's files from disk at startup.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set disk-load-buffer-size** *disk-load-buffer-size*

10. (Optional) Specify the size of the buffer that holds messages or message
    segments that are waiting to be sent to passive session stores.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set network-buffer-size** *network-buffer-size*

11. (Optional) Specify the time interval between attempts by the active session
    store to connect to missing passive session stores.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set retry-interval** *retry-interval*

12. (Optional) Specify the amount of time that a session store waits before closing
    when it is blocked from reading or writing a message.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set communications-timeout** *communications-timeout*

13. (Optional) Specify the time that an active session store waits for a passive
    session store or a passive session store waits for an active session store to load
    its data from disk before it closes the connection to the session store.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set load-timeout** *load-timeout*

14. (Optional) Specify the time that a passive session store waits for activity from
    the active session store before it closes the connection to the active session
    store.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set idle-timeout** *idle-timeout*

15. (Optional) Specify when the active session store closes the connection to a
    passive session store because of a backlog of messages waiting to be sent.

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set maximum-backlog-ratio** *maximum-backlog-ratio*

    [edit shared sae group se-region configuration driver junos session-store]
    user@host# **set minimum-backlog** *minimum-backlog*

16. (Optional) Verify your configuration.

```
[edit shared sae group se-region configuration driver junos session-store]
user@host# show
maximum-queue-age 5000;
maximum-queued-operations 50;
maximum-queue-size 51050;
maximum-file-size 25000000;
minimum-disk-space-usage 25;
rotation-batch-size 50;
maximum-session-size 10000;
disk-load-buffer-size 1000000;
network-buffer-size 51050;
retry-interval 5000;
communications-timeout 60000;
load-timeout 420000;
idle-timeout 3600000;
maximum-backlog-ratio 1.5;
minimum-backlog 5000000;
```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Configuring Global Session Store Parameters

This section describes how to configure global session store parameters that are shared by all session store instances (active or passive) on the SAE. You can also configure session store parameters within a device driver configuration. See *Configuring Session Store Parameters for a Device Driver* on page 24.

Use the following configuration statements to configure global session store parameters.

```
shared sae configuration driver session-store {
    ip-address ip-address;
    port port;
    root-directory root-directory;
}
```

To configure global session store parameters:

1. From configuration mode, access the configuration statement that configures the global session store parameters. In this sample procedure, the global session store is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration driver session-store**

2. (Optional) Specify the IP address or hostname that the session store infrastructure on this SAE uses to listen for incoming TCP connections from active session stores.

   [edit shared sae group se-region configuration driver session-store]
   user@host# **set ip-address** *ip-address*

3. (Optional) Specify the TCP port number on which the session store infrastructure on this SAE listens for incoming connections from active session stores.

   [edit shared sae group se-region configuration driver session-store]
   user@host# **set port** *port*

4. (Optional) Specify the root directory in which the session store creates files.

   [edit shared sae group se-region configuration driver session-store]
   user@host# **set root-directory** *root-directory*

5. (Optional) Verify your configuration.

   ```
   [edit shared sae group se-region configuration driver session-store]
   user@host# show
   ip-address 10.10.70.0;
   port 8820;
   root-directory var/sessionStore;
   ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Reducing the Size of Objects for the Session Store Feature

You can use serialized data compression to reduce the size of sessions objects that the SAE sends across the network for the session store feature. Enabling this property reduces the size of objects, but increases the CPU load on the SAE.

Use the following configuration statement to specify whether or not session objects are compressed.

```
shared sae configuration {
    compress-session-data;
}
```

To specify whether or not session objects are compressed:

1. From configuration mode, access the sae configuration. In this sample procedure, data compression is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration**

2. Enable reducing the size of session objects (subscriber and service sessions) that the SAE sends across the network for the session store feature.

   [edit shared sae group se-region configuration]
   user@host# **set compress-session-data**

3. (Optional) Verify your configuration.

   ```
   [edit shared sae group se-region configuration]
   user@host# show compress-session-data
   compress-session-data;
   ```

Related Topics

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 21, Setting Up an SAE with the SRC CLI.*

Configuring the Number of Threads for Sessions

Use the following configuration statement to set the number of threads used for session-related activity.

```
shared sae configuration session-job-manager {
    number-of-threads number-of-threads;
}
```

To configure the number of threads used to handle session-related activity:

1. From configuration mode, access the session job manager configuration. In this sample procedure, the number of threads is configured in the se-region group.

   user@host# **edit shared sae group se-region configuration session-job-manager**

2. Specify the number of threads used for session-related activity.

   [edit shared sae group se-region configuration session-job-manager]
   user@host# **set number-of-threads** *number-of-threads*

3. (Optional) Verify your configuration.

   ```
   [edit shared sae group se-region configuration session-job-manager]
   user@host# show
   number-of-threads 10;
   ```