Chapter 23

Configuring and Starting the SNMP Agent with the SRC CLI

This chapter describes how to use the SRC CLI to configure and run the SDX Simple Network Management Protocol (SNMP) agent in the SRC environment. The SNMP agent monitors host resources and the SRC components that use the host resources. You can use the CLI to configure the SNMP agent on a Solaris platform or on a C-series platform.

You can also use SRC configuration applications to configure the SNMP agent on a Solaris platform. See *Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

Topics in this chapter include:

For more information about the SNMP agent, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 8, Configuring the SNMP Traps with the SRC CLI*.

Configuration Statements for the SDX SNMP Agent

Use the following configuration statements to configure the SDX SNMP agent at the [edit] hierarchy level.

```
snmp agent {
    trap-history-limit trap-history-limit;
    component-polling-interval component-polling-interval;
    protocol-log-level protocol-log-level;
}

snmp agent initial {
    base-dn base-dn;
    host-id host-id;
}

snmp agent initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}

snmp agent initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}

snmp agent java {
    heap-size heap-size;
}
```

```
snmp agent logger name ...

snmp agent logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}

snmp agent logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring the SDX SNMP Agent

The SNMP agent obtains most of its information from the directory, but you configure the local properties that cannot be stored in the directory.

To configure the local properties for the SDX SNMP agent:

1. Configure general properties for the SDX SNMP agent, including trap history limit, component polling interval, and protocol log level.

   See *Configuring General Properties for the SDX SNMP Agent* on page 200.

2. Configure initial properties for the SDX SNMP agent, including the connection from the SDX SNMP agent to the directory and directory monitoring properties.

   See *Configuring Initial Properties for the SDX SNMP Agent* on page 201.

   See *Configuring Directory Connection Properties for the SDX SNMP Agent* on page 202.

   See *Configuring Directory Monitoring Properties for the SDX SNMP Agent* on page 202.

3. Configure logging destinations for the SDX SNMP agent.

   See *Configuring Logging Destinations for the SDX SNMP Agent* on page 203.

4. (Optional) Configure the Java heap memory for the SDX SNMP agent.

   See *Configuring JRE Properties* on page 204.

After you configure the local properties for the SDX SNMP agent, you can configure the SNMP agent. See *Configuring the SNMP Agent* on page 206.

Configuring General Properties for the SDX SNMP Agent

Use the following configuration statements to configure general properties for the SDX SNMP agent:

```
snmp agent {
    trap-history-limit trap-history-limit;
    component-polling-interval component-polling-interval;
    protocol-log-level protocol-log-level;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent
   ```

2. (Optional) Specify the maximum number of elements stored in the SNMP trap history table.

   ```
   [edit snmp agent]
   user@host# set trap-history-limit trap-history-limit
   ```

3. (Optional) Specify the interval at which an SRC component is polled.

   ```
   [edit snmp agent]
   user@host# set component-polling-interval component-polling-interval
   ```

4. (Optional) Specify the log level for SNMP requests and responses received from the master agent.

   ```
   [edit snmp agent]
   user@host# set protocol-log-level protocol-log-level
   ```

   To enable packet-level logging, set the protocol-log-level option to 9 or less.

5. (Optional) Verify your configuration.

   ```
   [edit snmp agent]
   user@host# show
   ```

   The output indicates the trap history limit, the component polling interval, the protocol log level, the initial properties, the logging destinations, and the Java heap size.

Configuring Initial Properties for the SDX SNMP Agent

Use the following configuration statements to configure initial properties for the SDX SNMP agent:

```
snmp agent initial {
    base-dn base-dn;
    host-id host-id;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent initial
   ```

2. Specify the DN of the directory used for the SNMP agent configuration data.

   ```
   [edit snmp agent initial]
   user@host# set base-dn base-dn
   ```

3. Identifies the system management configuration in the directory server that provides the remaining configuration for the SNMP agent.

   ```
   [edit snmp agent initial]
   user@host# set host-id host-id
   ```

   If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.

4. (Optional) Verify your configuration.

   ```
   [edit snmp agent initial]
   user@host# show
   base-dn o=UMC;
   host-id POP-ID;
   directory-connection {
     url ldap://127.0.0.1:389/;
     principal cn=sysman,ou=components,o=operators,<base>;
     credentials ********;
   }
   directory-eventing {
     eventing;
   }
   ```

Configuring Directory Connection Properties for the SDX SNMP Agent

Use the following configuration statements to configure directory connection properties for the SDX SNMP agent:

```
snmp agent initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

To configure directory connection properties:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent initial directory-connection
   ```

2. Specify the directory connection properties.

   ```
   [edit snmp agent initial directory-connection]
   user@host# set ?
   ```

   For more information about the directory connection properties, see *SRC-PE Getting Started Guide, Chapter 25, Configuring Local Properties with the SRC CLI*.

3. (Optional) Verify your configuration.

   ```
   [edit snmp agent initial directory-connection]
   user@host# show
   url ldap://127.0.0.1:389/;
   principal cn=sysman,ou=components,o=operators,<base>;
   credentials ********;
   ```

Configuring Directory Monitoring Properties for the SDX SNMP Agent

Use the following configuration statements to configure directory monitoring properties for the SDX SNMP agent:

```
snmp agent initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent initial directory-eventing
   ```

2. Specify the properties for the SDX SNMP agent.

   ```
   [edit snmp agent initial eventing]
   user@host# set ?
   ```

   For more information about the directory monitoring properties, see *SRC-PE Getting Started Guide, Chapter 25, Configuring Local Properties with the SRC CLI*.

3. (Optional) Verify your configuration.

   ```
   [edit snmp agent initial directory-eventing]
   user@host# show
   eventing;
   ```

Configuring Logging Destinations for the SDX SNMP Agent

Use the following configuration statement to configure logging destinations for the SDX SNMP agent:

snmp agent logger *name* ...

To configure logging destinations:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent
   ```

2. Specify the name and type of logging destination.

   For file-based logging:

   ```
   [edit snmp agent]
   user@host# set logger name file
   ```

   For syslog-based logging:

   ```
   [edit snmp agent]
   user@host# set logger name syslog
   ```

For more information about logging, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SRC Components* and *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI*.

Configuring JRE Properties

Use the following configuration statements to configure Java Runtime Environment (JRE) properties for the SDX SNMP agent:

```
snmp agent java {
    heap-size heap-size;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent java
   ```

2. (Optional) Specify the maximum amount of memory available to the JRE.

   ```
   [edit snmp agent java]
   user@host# set heap-size heap-size
   ```

   Do not change this value unless instructed to do so by Juniper Networks.

3. (Optional) Verify your configuration.

   ```
   [edit snmp agent java]
   user@host# show
   heap-size 160m;
   ```

Configuration Statements for the SNMP Agent

Use the following configuration statements to configure the SNMP agent at the [edit] hierarchy level.

```
snmp {
    contact contact;
    name name;
    location location;
    description description;
    address [address...];
}

snmp community community {
    authorization (read-only|read-write);
    clients clients;
    oid oid;
}

snmp notify target target-name {
    address address;
    port port;
    community community;
    type (trapv1|trapv2|inform);
}
```

```
snmp v3 snmp-community community-index {
    community-name community-name;
    security-name security-name;
    address address;
}

snmp v3 usm local-engine user username ...

snmp v3 usm local-engine user username authentication-md5 {
    authentication-password authentication-password;
}

snmp v3 usm local-engine user username authentication-sha {
    authentication-password authentication-password;
}

snmp v3 usm local-engine user username privacy-aes {
    privacy-password privacy-password;
}

snmp v3 usm local-engine user username privacy-des {
    privacy-password privacy-password;
}

snmp v3 vacm access group group-name ...

snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) ...

snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) security-level (authentication|none|privacy) {
    read-view read-view;
    write-view write-view;
}

snmp v3 vacm security-to-group security-model (v1|v2c|usm) ...

snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name
security-name {
    group-name group-name;
}

snmp view view-name ...

snmp view view-name oid oid {
    (include|exclude);
}
```

For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring the SNMP Agent

To configure the SNMP agent to control its operation:

1. Configure information supplied by the SNMP agent, including the listening address and system information.

   See *Configuring System Information for the SNMP Agent* on page 206.

2. Configure access control for the SNMP agent, including access for SNMPv3 users, SNMPv1 and SNMPv2 communities (traditional access control), and the view-based access control model (VACM).

   See *Configuring Access Control for SNMPv3 Users* on page 207.

   See *Configuring Access Control for Communities* on page 209.

   See *Configuring Access Control for the VACM* on page 210.

3. Configure active monitoring.

   See *Configuring Notification Targets* on page 215.

Configuring System Information for the SNMP Agent

Use the following configuration statements to configure information supplied by the SNMP agent:

```
snmp {
    contact contact;
    name name;
    location location;
    description description;
    address [address...];
}
```

To configure properties for the SNMP agent:

1. From configuration mode, access the configuration statement that configures the SNMP agent.

   ```
   [edit]
   user@host# edit snmp
   ```

2. (Optional) Specify the adminstrative contact for the system being managed by SNMP.

   ```
   [edit snmp]
   user@host# set contact contact
   ```

3. (Optional) Specify the name of the system being managed by SNMP.

   ```
   [edit snmp]
   user@host# set name name
   ```

4. (Optional) Specify the location of the system being managed by SNMP.

   ```
   [edit snmp]
   user@host# set location location
   ```

5. (Optional) Specify the description of the system being managed by SNMP.

   ```
   [edit snmp]
   user@host# set description description
   ```

6. (Optional) Specify the listening address on which to receive incoming SNMP requests.

   ```
   [edit snmp]
   user@host# set address [address...]
   ```

   To list more than one IP address, enter the addresses separated by spaces within brackets. By default, the SNMP agent listens on all IPv4 interfaces.

7. (Optional) Verify your configuration.

   ```
   [edit snmp]
   user@host# show
   ```

   If you did not configure the SNMP agent, the command displays only the SDX SNMP agent configuration.

Configuring Access Control for SNMPv3 Users

Use the following configuration statements to configure access control for SNMPv3 users:

```
snmp v3 usm local-engine user username ...

snmp v3 usm local-engine user username authentication-md5 {
    authentication-password authentication-password;
}

snmp v3 usm local-engine user username authentication-sha {
    authentication-password authentication-password;
}

snmp v3 usm local-engine user username privacy-aes {
    privacy-password privacy-password;
}

snmp v3 usm local-engine user username privacy-des {
    privacy-password privacy-password;
}
```

To configure access control for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the access control for SNMPv3 users.

   [edit]
   user@host# **edit snmp v3 usm local-engine user** *username*

   Username is the user-based security model (USM) username. By default, no authentication or encryption is specified for the SNMPv3 user.

2. (Optional) Specify the authentication type.

   See *Configuring Authentication* on page 208.

3. (Optional) Specify the encryption.

   See *Configuring Encryption* on page 209.

NOTE: Before you configure encryption, you must configure the authentication type.

4. (Optional) Verify your configuration.

   ```
   [edit snmp v3 usm local-engine user username]
   user@host# show
   ```

Configuring Authentication

To configure the authentication type for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the authentication type.

   To configure MD5 authentication:

   user@host# **edit snmp v3 usm local-engine user** *username* **authentication-md5**

   To configure SHA authentication:

   user@host# **edit snmp v3 usm local-engine user** *username* **authentication-sha**

2. Specify the authentication password.

   user@host# **set authentication-password** *authentication-password*

   The password must be at least eight characters.

Configuring Encryption

Before you configure encryption, you must configure the authentication type. See *Configuring Authentication* on page 208.

To configure encryption for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the encryption.

   To configure AES encryption:

   user@host# **edit snmp v3 usm local-engine user** *username* **privacy-aes**

   To configure DES encryption:

   user@host# **edit snmp v3 usm local-engine user** *username* **privacy-des**

2. Specify the privacy password.

   user@host# **set privacy-password** *privacy-password*

   The password must be at least eight characters.

Configuring Access Control for Communities

Use the following configuration statements to configure community strings for traditional access control:

```
snmp community community {
    authorization (read-only|read-write);
    clients clients;
    oid oid;
}
```

To configure community strings:

1. From configuration mode, access the configuration statement that configures the community string. Community names must be unique.

   [edit]
   user@host# **edit snmp community** *community*

2. (Optional) Specify the authorization level.

   To specify read-only access:

   [edit snmp community *community*]
   user@host# **set authorization read-only**

   To specify read and write access:

   [edit snmp community *community*]
   user@host# **set authorization read-write**

3. Specify the IP address or subnet of the SNMP client hosts that are authorized to use this community.

   [edit snmp community *community*]
   user@host# **set clients** *clients*

   By default, all clients are allowed.

4. (Optional) Specify the object identifier used to represent a subtree of MIB object to which access is allowed.

   [edit snmp community *community*]
   user@host# **set oid** *oid*

5. (Optional) Verify your configuration.

   ```
   [edit snmp community community]
   user@host# show
   ```

Configuring Access Control for the VACM

To configure the access control for the view-based access control model (VACM):

1. Map an SNMPv1 or SNMPv2c community name to a security name.

   See *Associating Security Names with a Community* on page 210.

2. Define a named view.

   See *Defining Named Views* on page 211.

3. Map from a group of users or communities to a view.

   See *Defining Access Privileges for an SNMP Group* on page 212.

4. Map a security name into a named group.

   See *Assigning Security Names to Groups* on page 214.

Associating Security Names with a Community

For SNMPv1 or SNMPv2c packets, you must assign security names to groups at the [edit snmp v3 vacm security-to-group] hierarchy level and you must associate a security name with an SNMP community.

Use the following configuration statements to configure SNMPv1 or SNMPv2c communities for the VACM:

```
snmp v3 snmp-community community-index {
    community-name community-name;
    security-name security-name;
    address address;
}
```

To configure the community:

1. From configuration mode, access the configuration statement that configures the community.

   [edit]
   user@host# **edit snmp v3 snmp-community** *community-index*

   Unique index that identifies an SNMP community.

2. (Optional) Specify the community string for the SNMPv1 or SNMPv2c community.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **set community-name** *community-name*

   If a community name is not specified, the community index is used.

3. Specify the VACM security name to associate with the community string.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **set security-name** *security-name*

4. (Optional) Specify the IP address or subnet of the SNMP clients that are authorized to use this community.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **set address** *address*

   If an address is not specified, all clients are authorized to use the community.

5. (Optional) Verify your configuration.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **show**

Defining Named Views

Use the following configuration statements to define named views:

```
snmp view view-name ...

snmp view view-name oid oid {
    (include|exclude);
}
```

To configure named views:

1. From configuration mode, access the configuration statement that configures the named views.

   [edit]
   user@host# **edit snmp view** *view-name*

   The view name identifies a group of MIB objects for which to define access.

2. Specify the object identifier (OID) that represents a subtree of MIB objects for the view and whether the OID is included in or excluded from the view.

   To include the OID in the view:

   [edit snmp view *view-name*]
   user@host# **set oid** *oid* **include**

   To exclude the OID from the view:

   [edit snmp view *view-name*]
   user@host# **set oid** *oid* **exclude**

3. (Optional) Verify your configuration.

   [edit snmp view *view-name*]
   user@host# **show**

Defining Access Privileges for an SNMP Group

Use the following configuration statements to define access privileges for SNMP groups:

snmp v3 vacm access group *group-name* ...

snmp v3 vacm access group *group-name* default-context-prefix security-model (any|v1|v2c|usm) ...

```
snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) security-level (authentication|none|privacy) {
    read-view read-view;
    write-view write-view;
}
```

To configure MIB views with a group for the VACM:

1. From configuration mode, access the configuration statement that configures the VACM group.

   [edit]
   user@host# **edit snmp v3 vacm access group** *group-name*

   The group name is the name for a collection of SNMP security names that belong to the same SNMP access policy.

2. Specify the security model for access privileges.

   [edit snmp v3 vacm access group *group-name*]
   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)

   To specify any security model:

   user@host# **set default-context-prefix security-model any**

To specify the SNMPv1 security model:

user@host# **set default-context-prefix security-model v1**

To specify the SNMPv2c security model:

user@host# **set default-context-prefix security-model v2c**

To specify the SNMPv3 user-based security model (USM):

user@host# **set default-context-prefix security-model usm**

3. Specify the security level for access privileges.

   [edit snmp v3 vacm access group *group-name*]
   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   security-level (authentication|none|privacy)

   To specify a security level that provides authentication but no encryption:

   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   security-level authentication

   To specify a security level that provides no authentication and no encryption:

   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   security-level none

   For SNMPv1 or SNMPv2c access, specify none as the security level.

   To specify a security level that provides authentication and encryption:

   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   security-level privacy

4. (Optional) Specify the view used for SNMP read access. You must specify the read-view option or the write-view option.

   [edit snmp v3 vacm access group *group-name* default-context-prefix security-model (any|v1|v2c|usm) security-level (authentication|none|privacy)]
   user@host# **set read-view** *read-view*

5. (Optional) Specify the view used for SNMP write access. You must specify the read-view option or the write-view option.

   [edit snmp v3 vacm access group *group-name* default-context-prefix security-model (any|v1|v2c|usm) security-level (authentication|none|privacy)]
   user@host# **set write-view** *write-view*

Assigning Security Names to Groups

For SNMPv1 or SNMPv2c packets, you must assign security names to groups and you must associate a security name with an SNMP community at the [edit snmp v3 snmp-community *community-index*] hierarchy level.

Use the following configuration statements to assign security names to groups:

```
snmp v3 vacm security-to-group security-model (v1|v2c|usm) ...

snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name
security-name {
    group-name group-name;
}
```

To map security names to groups for the VACM:

1. From configuration mode, access the configuration statement that configures the security model for a group.

   user@host# **edit snmp v3 vacm security-to-group security-model** (v1|v2c|usm)

   To specify the SNMPv1 security model:

   user@host# **edit snmp v3 vacm security-to-group security-model v1**

   To specify the SNMPv2c security model:

   user@host# **edit snmp v3 vacm security-to-group security-model v2c**

   To specify the SNMPv3 user-based security model (USM):

   user@host# **edit snmp v3 vacm security-to-group security-model usm**

2. Specify the security name.

   user@host# **edit snmp v3 vacm security-to-group security-model** (v1|v2c|usm) **security-name** *security-name*

   If the security model is USM, the security name is the username configured at the [edit snmp v3 usm local-engine user] hierarchy level.

3. Specify the group to which the security name is assigned.

   [edit snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name *security-name*]
   user@host# **set group-name** *group-name*

Configuring Notification Targets

Use the following configuration statements to configure notification targets:

```
snmp notify target target-name {
    address address;
    port port;
    community community;
    type (trapv1|trapv2|inform);
}
```

To configure notification targets:

1. From configuration mode, access the configuration statement that configures the notification target.

   ```
   [edit]
   user@host# edit snmp notify target target-name
   ```

   Specify the notification target name.

2. Specify the IPv4 or IPv6 address of the system to receive notifications.

   ```
   [edit snmp notify target target-name]
   user@host# set address address
   ```

3. (Optional) Specify the SNMP trap port number.

   ```
   [edit snmp notify target target-name]
   user@host# set port port
   ```

4. Specify the community string used when sending traps.

   ```
   [edit snmp notify target target-name]
   user@host# set community community
   ```

5. Specify the notification types as traps or informs. Traps are unconfirmed notifications. Informs are confirmed notifications.

   To specify the notification type as an SNMPv1 trap:

   [edit snmp notify target *target-name*]
   user@host# **set type trapv1**

   To specify the notification type as an SNMPv2 trap:

   [edit snmp notify target *target-name*]
   user@host# **set type trapv2**

   To specify the notification type as an SNMPv2 inform:

   [edit snmp notify target *target-name*]
   user@host# **set type inform**

6. (Optional) Verify your configuration.

   [edit snmp notify target *target-name*]
   user@host# **show**

Operating the SNMP Agent

You must configure the SNMP agent and then manually start the agent. If you attempt to manually start the SNMP agent before it is configured, the software displays a message that the agent has not been configured and cannot start.

The SNMP agent automatically restarts in the event of a host reboot or process failure that stops the agent.

Starting the SDX SNMP Agent

Before you start the SDX SNMP agent:

1. Perform the initial configuration tasks.

   See *Chapter 4, Configuring a C-series Platform*.

2. Configure the SDX SNMP agent.

   See *Configuring the SDX SNMP Agent* on page 199.

Manually start the SDX SNMP agent the first time it runs. Thereafter, the agent automatically restarts.

To start the SNMP agent:

user@host> **enable component agent**

The system responds with a start message. If the SNMP agent is already running, the system responds with a warning message indicating that fact.

Stopping the SDX SNMP Agent

To stop the SNMP agent:

user@host> **disable component agent**

The system responds with a stop message. If the SNMP agent is not running when you issue the command, the software responds with a warning message indicating that fact.

Monitoring the SDX SNMP Agent

To display the SDX SNMP agent status:

user@host> **show component**

The system responds with a status message.