Chapter 31

Planning an SRC Installation on a Solaris Platform

This chapter provides information to help you plan an SRC deployment. The chapter describes distribution scenarios for SRC components, including deployment strategies for an enterprise service portal. It also describes SRC architecture and component interactions. Topics include:

- SRC Installation Options and Configurations for Solaris Platforms on page 245
- SRC Component Distribution Scenarios on Solaris Platforms on page 246
- Distributed SRC Installation on Solaris Platforms on page 247
- Consolidated SRC Installation on Solaris Platforms on page 252
- Single-Host SRC Installation for Demonstration on page 254

SRC Installation Options and Configurations for Solaris Platforms

Before you install SRC software components on a Solaris platform, plan your implementation. The SRC software comprises a set of interacting software modules that you can install on different hosts and that you can connect to other internetworking devices and applications through a range of standard interfaces.

When you plan your implementation, consider that you can deploy the SAE on one host, a directory on another host, and Policy Editor on a third host. You might want to install only the components needed by an administrator on some hosts, and the components needed by developers on others. For a list of the components you can install and recommended sets of components for different purposes, see *Chapter 33, Installing the SRC Software on a Solaris Platform*.

Juniper Networks Professional Services can assist you in determining the best installation scenario for your environment.

SRC Component Distribution Scenarios on Solaris Platforms

The distributed architecture of the SRC software offers high scalability and extensive flexibility that allows you to customize the SRC software for your environment. SDX releases 3.1.1 and earlier, in which the SRC software was an integrated application rather than a set of interacting modules, are fully compatible with this distributed architecture.

NOTE: This chapter describes some typical scenarios, but they are by no means the only ones; many other variations are possible.

Figure 22 shows an overview installation of all SRC components.

Figure 22: Installation of All SRC Components

This section covers the following scenarios for distributing SRC components:

■ Distributed—An installation that distributes the SRC components among several machines in several locations and provides reliability and scalability

■ Regionalized—Distribution scenario for a large service provider that allows regional autonomy

- Consolidated—Distribution scenario that consolidates network services into regional data centers

- Single host—A minimal installation that is suitable for small operations, demonstrations, and trials

Distributed SRC Installation on Solaris Platforms

Figure 23 on page 248 shows a more complicated setup that distributes the SRC components among several machines in several locations, while still providing reliability and scalability.

In the back office, there are:

- A master directory server running on dedicated hardware

- SDX Admin and Policy Editor running on as many other machines as desired

- A pair of network information collector (NIC) hosts running NIC resolvers

- A Web application server with a portal (a residential portal, an enterprise portal, or an Advanced Services Gateway application)

- Non-SRC components of the service provider's OSS, which are integrated with the SRC components through the master directory as LDAP clients

In the POPs there are primary and backup hosts that contain identical SAE, RADIUS, directory servers, and NIC hosts. The NIC hosts contain a resolver, directory agent, and SAE agent, and they communicate with the NIC hosts in the back office using Common Object Request Broker Architecture (CORBA). SAE, RADIUS, and directory server components within the hosts communicate through LDAP.

Clients of the NIC host need to determine which remote SAE is managing the subscriber sessions that they need to operate on. The NIC system collects and stores this information. At startup, the SAE stores its CORBA object reference in the directory. The NIC system collects this SAE reference, along with the keys to subscriber sessions (IP addresses and LDAP DNs of the subscriber profiles in the directory) managed by the SAE. Web applications can locate the SAE for a particular subscriber by querying the NIC system.

Figure 23: Distributed Installation for Reliability and Scalability
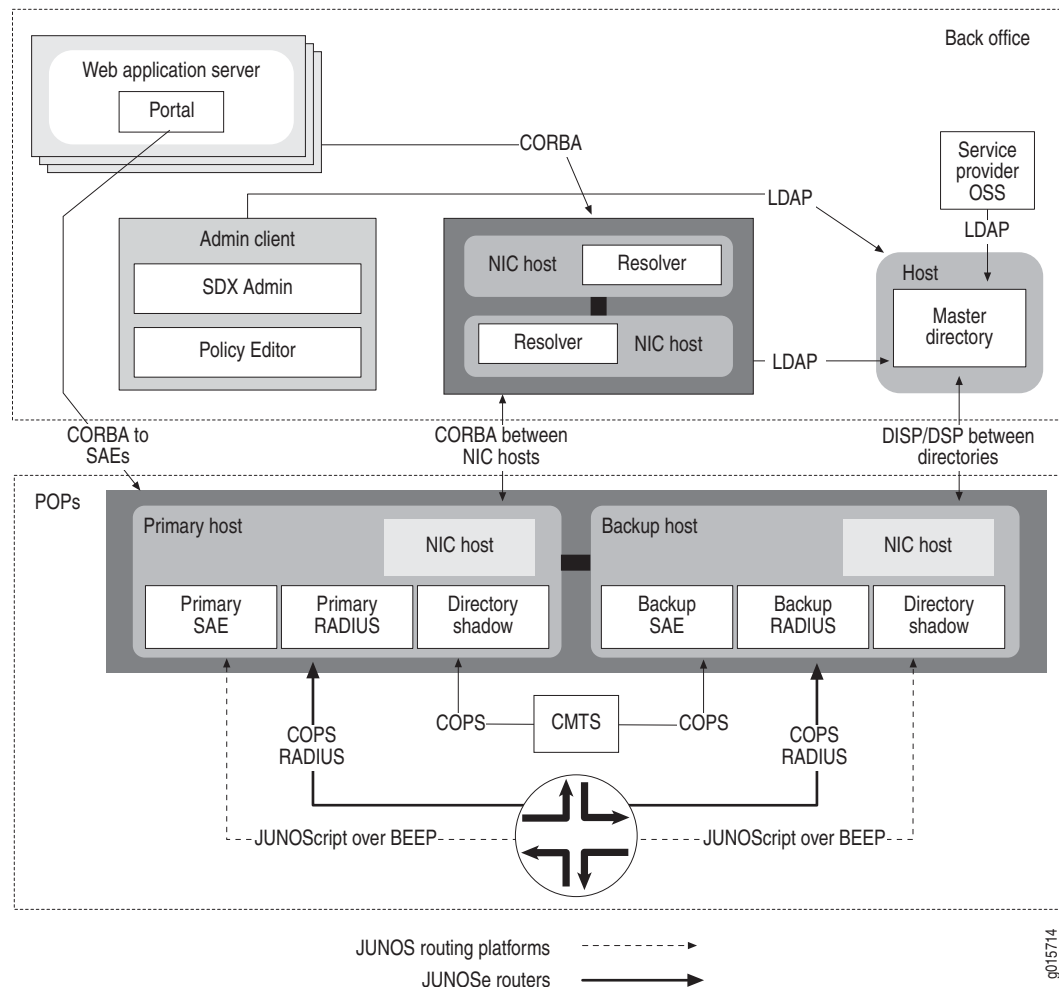
Master Directory and Directory Shadows

The master directory contains all the directory data and handles all update requests, either locally through LDAP or remotely through the Directory Service Protocol (DSP) for X.500 directories, such as DirX, or through equivalent protocols for other directory types.

The information in the master directory is copied to shadow directories in the service provider's point of presence (POP). The system uses Directory Information Shadowing Protocol (DISP) for data transfer for X.500 directories, such as DirX, and equivalent protocols for other directory transfers. This type of distribution puts the directory information for SAEs and RADIUS servers physically close to the servers. A highly reliable LAN connects the hosts and provides good performance.

It is not necessary to include all information in the directory shadows. For instance, only information relevant to a particular POP, such as the information for the subscribers who can actually connect there, may be included. Also, updates generated from an SAE in a particular POP, such as cached logins, may be mastered locally and not propagated to the directory master in the back office. Finally, attributes not relevant to SAE and RADIUS operation—for instance, the subscriber's address—may be filtered from replication to the directory shadows in the POPs.

Scalability

This setup can be scaled incrementally by replicating the pattern found in the POP as the subscriber base grows.

Reliability

To avoid a single point of failure in the POPs, the RADIUS, SAE, directory servers, and NIC hosts are installed on identical primary and backup hardware. If the primary host fails, the router switches over to the backup host. Also, the SAE and RADIUS servers (as LDAP clients) and NIC hosts can be configured to switch over to the directory server in the backup host in the POP or to the master directory in the back office. You can configure one or more backup servers for a number of primary servers; such redundancy distributes the load of the routers across several hosts and reduces failover time by limiting the number of subscribers handled by any one host.

This setup avoids service outages in the case of any single network, server, or software failure. Existing subscribers are even unaffected by long periods of disconnection between their POP and the back office. The directory server protocols ensure that all information is properly distributed regardless of the pattern of intermittent connectivity between the sites. Since relatively static directory information is cached locally in the directory shadow in the POP, very high transaction rates for SAE and the RADIUS server are achieved.

Simplified Management and Security

Additional benefits of this setup at the POP are simplified management because of the use of identical hardware and software, and an added level of security because the SAE, RADIUS, the directory, and NIC hosts are all on the same machine.

> **NOTE:** In this and subsequent scenarios, protection of the data in the back office, such as subscriber names and passwords, is a critical issue. Consequently, the back-office site is typically heavily protected by firewalls. One key advantage of this setup is that only directory protocols need be passed through firewalls, and these protocols have rich and flexible security properties.

Regionalized Installation

Figure 24 on page 251 extends the scheme shown in the last section with an additional layer of directory replication for very large service providers who partition their organization into regions with regional data centers.

A single back office still houses the master directory, some centralized management servers and clients, and a pair of NIC hosts. There are also still primary and backup hosts at the POP, with SAE and RADIUS servers and NIC hosts with a resolver, a directory agent, and an SAE agent.

In this case, there is also a middle layer of regional data centers that house the first level of replication from the master directory in the back office. The regional data centers may also contain a complete set of SRC components and other OSS management components integrated with the local directory. If the local directory fails, these regional components can switch over to the master directory in the back office and switch back once the local failure is corrected. Also, directory administrative controls can be defined to limit the access of regional management operators to an appropriate scope according to the service provider's policies.

Figure 24: Regionalized Directory Installation for Regional Autonomy
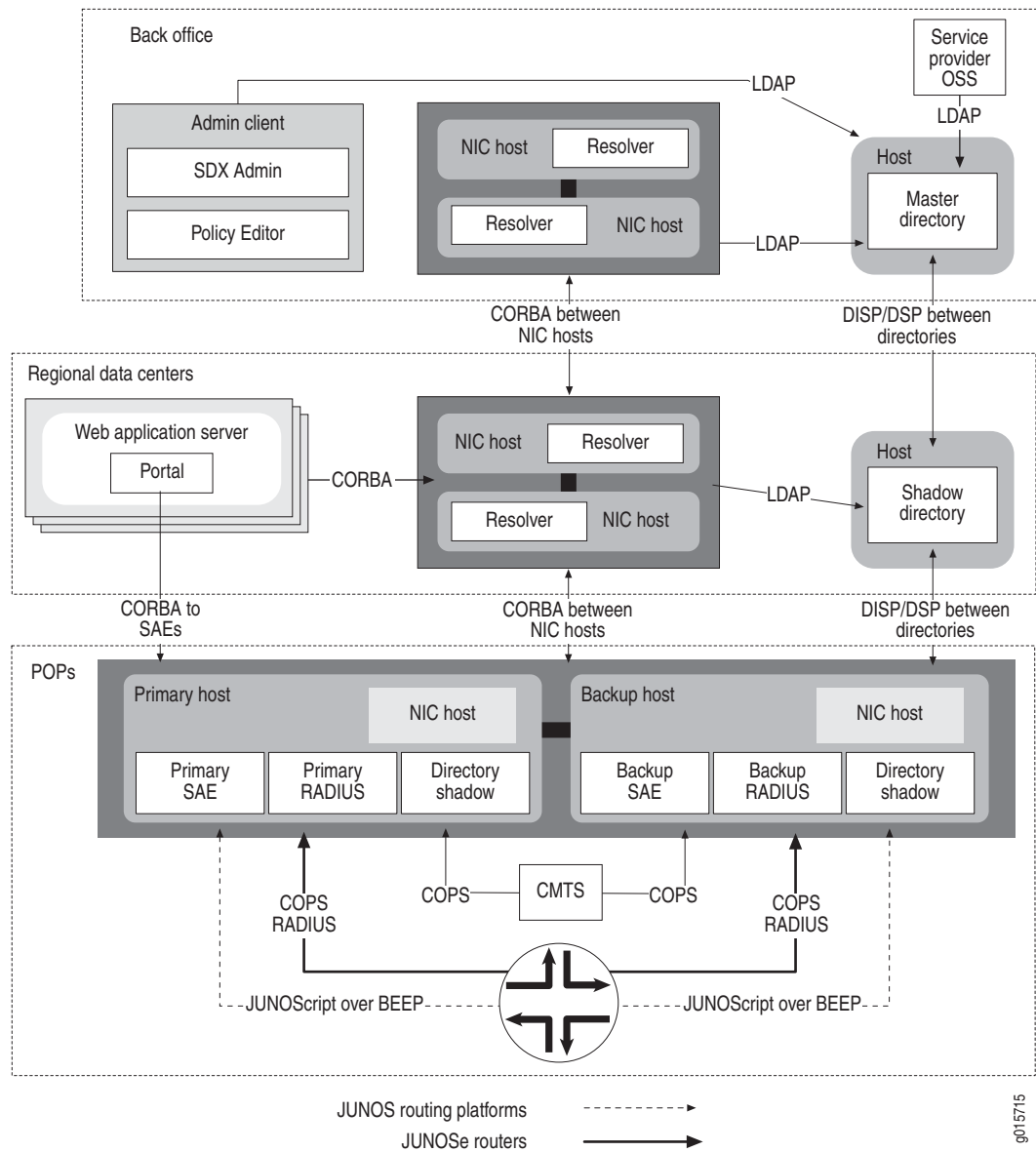
Consolidated SRC Installation on Solaris Platforms

All the previous scenarios provide top reliability because all the network services—that is, the SAE and RADIUS servers—as well as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers and NIC hosts, are at the same site as the router and are connected by a reliable LAN. However, to maintain this reliability, hardware must be dedicated to this function in every POP, no matter how small, and economies of scale cannot be achieved through consolidation in large hosts.

The SRC software also supports a deployment scenario that allows a trade-off between consolidation of components in large hosts and the risk of less reliable MAN/WAN connections between sites. This scenario, shown in Figure 25 on page 253, consolidates the network services in regional data centers. Here, the regional data center has:

- Two directory servers for reliability.

- A pair of very large SAE hosts that can be used as the primary or backup hosts for different routers in remote POPs.

- A set of RADIUS hosts that can be load balanced across the various routers and the SAEs for the region.

- A pair of NIC hosts.

- A Web application server with a portal (a residential portal, an enterprise portal, or an Advanced Services Gateway application).

Figure 25: Consolidated Network Services
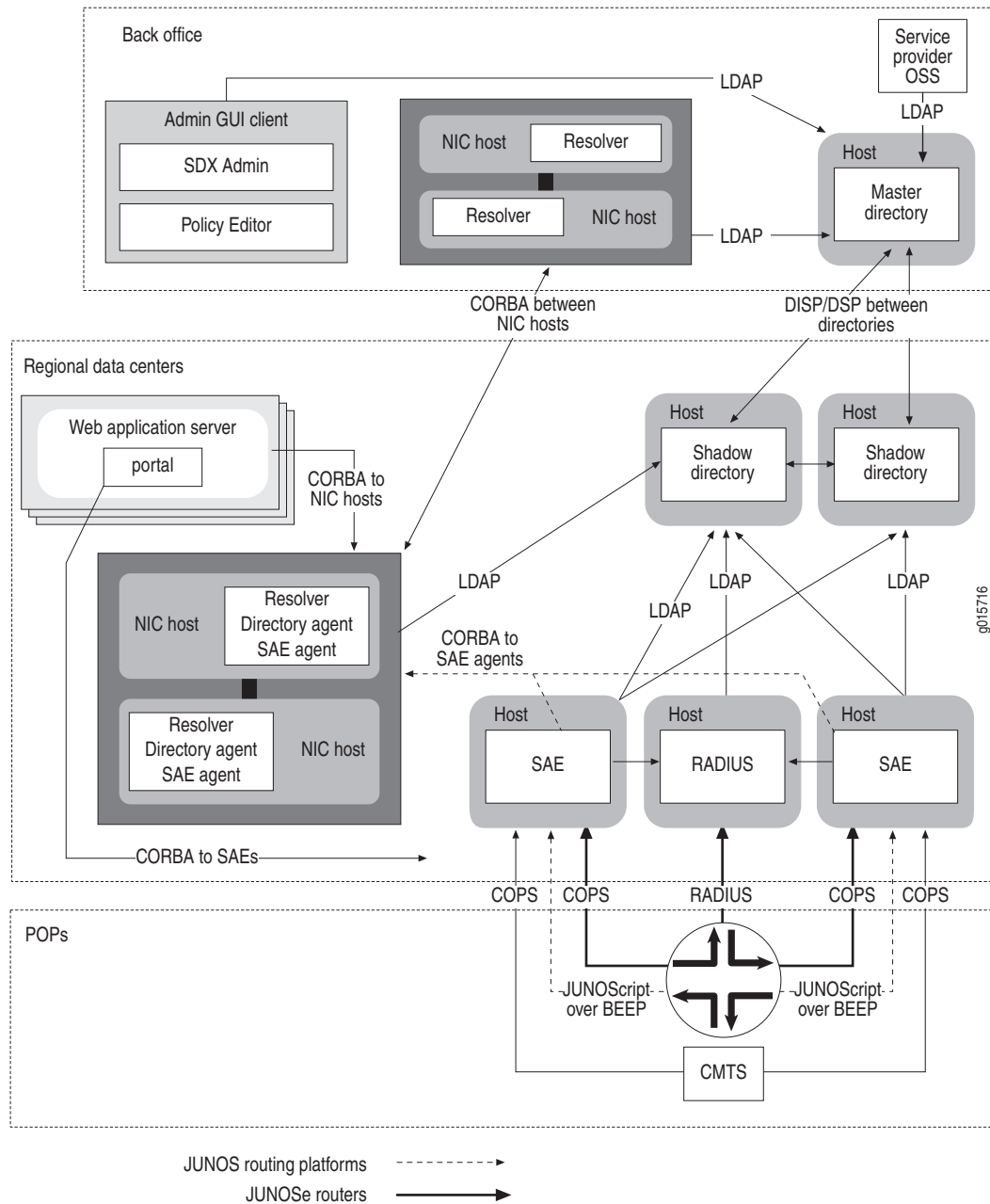
Redundancy Schemes

The N to 1 and N to M redundancy schemes are even more important in regional data centers because a server could be serving a very large number of subscribers.

RADIUS

Because RADIUS is stateless, it is enough to configure a sufficient number of RADIUS servers for the load and configure both the routers and the SAE to load balance across them.

NIC Hosts

Regional data centers may or may not have one or more NIC hosts. It is up to service providers to add enough NIC hosts to achieve the desired level of availability and performance.

COPS Connection

For the Common Open Policy Service (COPS) connection between the SAE and JUNOSe routers, special care must be taken. During a failover, existing activated services are not affected; but subscribers cannot log in, activate, or deactivate services until failover synchronization is complete. Thus, it may be desirable to configure multiple SAE machines (for example, tens) in the regional data center to limit the number of subscribers served by any one machine. The JUNOSe routers can be configured with primary, secondary, and tertiary COPS servers, so it is possible to configure many failover schemes. It is also possible for SAE servers to redirect existing and new COPS connections to other, more lightly loaded SAE servers. This COPS connection redirection can be triggered manually during a scheduled maintenance window or automatically based on SAE load monitoring.

Adding or Replacing Hardware

Startup is simplified because there is always a pool of SAE hosts to manage any new routers as they are brought online. In the case of a disastrous server failure, the offending hardware can simply be removed and replaced as time and resources allow. Also, in regularly scheduled maintenance windows, incremental software upgrades can be achieved in the same fashion.

Single-Host SRC Installation for Demonstration

Figure 26 shows a single-host installation that is suitable for demonstrations, trials, and small operations. The directory, Remote Authentication Dial-In User Service (RADIUS) server, SAE, and a Java 2 Enterprise Edition (J2EE) Web application server that contains the portal application are all installed on the same host. The SDX Admin and Policy Editor applications also run locally. The router uses the single RADIUS and SAE servers, and all SRC components act as LDAP clients to the single directory.

Figure 26: Single-Host Installation for Small Operations