Sun Java System Communications Services 6 2005Q4 Delegated Administrator Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–2658
October 2005

050921@13215

Contents

Tables

Figures

Preface

This guide explains how to configure and administer Sun ™Sun Java System Communications Services Delegated Administrator. This guide also describes the Delegated Administrator commands, providing syntax and examples.

Delegated Administrator consists of a console (graphical user interface) and a set of command-line tools for provisioning users, groups, domains, and resources for Sun Java System Messaging Server and Sun Java System Calendar Server using Sun Java System Access Manager.

Topics covered in this chapter include:

Who Should Use This Book

You should read this book if you are responsible for administering, configuring, and deploying Delegated Administrator at your site.

Before You Read This Book

This book assumes that you are responsible for administering the software and that you have a general understanding of the following:

- The Internet and the World Wide Web
- Messaging Server protocols
- Sun Java System Administration Server
- Sun Java System Directory Server and LDAP
- Sun Java System Console
- System administration and networking on the following platforms:
  - Solaris 8 for SPARC and x86
  - Solaris 9 for SPARC and x86
  - Solaris 10 for SPARC and x86
  - HP-UX 11.x
  - Windows 2000

  General deployment architectures

How This Book Is Organized

The following table summarizes the content of this book.

TABLE P–1 How This Book Is Organized

Chapter	Description
Chapter 1	Describes the directory organizations, administrator roles, and service packages provided by Delegated Administrator
Chapter 2	Describes the steps necessary to install and configure Sun Java System Communications Services Delegated Administrator.
Chapter 3	Describes and steps through the configuration program for Delegated Administrator.

TABLE P–1 How This Book Is Organized *(Continued)*

Chapter	Description
Chapter 4	Describes how to customize Delegated Administrator—for example, to change the look and feel of the console.
Chapter 5	Describes the `commadmin` utility, providing syntax and examples.
Appendix A	Describes the Service Provider Administrator role and provider and business organizations managed by the Service Provider Administrator.
Appendix B	Lists attribute values and time zone values for specific command-line options.
Appendix C	Lists log files that can be examined to debug Delegated Administrator.
Appendix D	Offers tuning tips for Delegated Administrator, the Web containers, and Directory Server that improve Delegated Administrator performance.
Appendix E	Describes how to consolidate ACIs and remove unused ACIs from the directory.

Related Books

The `http://docs.sun.com`SM web site enables you to access Sun technical documentation online. You can browse the archive or search for a specific book title or subject.

Messaging Server Documents

Use the following URL to see all the Messaging Server documentation:

`http://docs.sun.com/coll/1312.1`

The following documents are available:

- *Sun Java™System Messaging Server Administration Guide*
- *Sun Java™ System Messaging Server Administration Reference*
- *Sun Java™ System Messaging Server MTA Developer's Reference*
- *Sun Java™ System Messenger Express Customization Guide*

The Messaging Server product suite contains other products such as Sun Java™ System Directory Server and Administration Server. Documentation for these and other products can be found at the following URL:

`http://docs.sun.com/db/prod/sunone`

In addition to the software documentation, see the Messaging Server Software Forum for technical help on specific Messaging Server product questions. The forum can be found at the following URL:

`http://swforum.sun.com/jive/forum.jsp?forum=15`

Calendar Server Documents

Use the following URL to see all the Calendar Server documentation:

`http://docs.sun.com/coll/1313.1`

The following documents are available:

- *Sun Java™ System Calendar Server Administration Guide*
- *Sun Java™ System Calendar Server Developer's Guide*

Communications Services Documents

Use either one of the following URLs to see the documentation that applies to all Communications Services products:

`http://docs.sun.com/coll/1312.1`

or

`http://docs.sun.com/coll/1313.1`

The following documents are available:

- *Sun Java™ System Communications Services Release Notes*
- *Sun Java™ System Communications Services Delegated Administrator Guide*
- *Sun Java™ System Communications Services Deployment Planning Guide*
- *Sun Java™ System Communications Services Schema Migration Guide*
- *Sun Java™ System Communications Services Schema Reference*
- *Sun Java™ System Communications Services Event Notification Service Guide*
- *Sun Java™ System Communications Express Administration Guide*
- *Sun Java™ System Communications Express Customization Guide*

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

Sun Function	URL	Description
Documentation	`http://www.sun.com/documentation/`	Download PDF and HTML documents, and order printed documents
Support and Training	`http://www.sun.com/supportraining/`	Obtain technical support, download patches, and learn about Sun courses

Accessing Sun Resources Online

For product downloads, professional services, patches and support, and additional developer information, go to the following:

- Download Center `http://wwws.sun.com/software/download/`
- Professional Services `http://www.sun.com/service/sunps/sunone/index.html`
- Sun Enterprise Services, Solaris Patches, and Support `http://sunsolve.sun.com/`

- Developer Information
  `http://developers.sun.com/prodtech/index.html`

Contacting Sun Technical Support

If you have technical questions about this product that are not answered in the product documentation, go to `http://www.sun.com/service/contacting`.

Typographic Conventions

The following table describes the typographic changes that are used in this book.

TABLE P–2 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. Perform a *patch analysis*. Do *not* save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–3 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

Symbols

The following table describes the symbol conventions used in this book.

TABLE P–4 Symbol Conventions

Symbol	Description	Example	Meaning
`[ ]`	Contains optional command options.	`ls [-l]`	The `-l` option is not required.
`{ | }`	Contains a set of choices for a required command option.	`-d {y|n}`	The `-d` option requires that you use either the `y` argument or the `n` argument.
-	Joins simultaneous multiple keystrokes.	Control-A	Press the Control key while you press the A key.
+	Joins consecutive multiple keystrokes.	Ctrl+A+N	Press the Control key, release it, and then press the subsequent keys.
>	Indicates menu item selection in a graphical user interface.	File > New > Templates	From the File menu, choose New. From the New submenu, choose Templates.

Default Paths and File Names

The following table describes the default paths and file names used in this book.

TABLE P–5 Default Paths and File Names

Term	Description
msg_svr_base	Represents the base installation directory for Messaging Server. The default value of the *msg_svr_base* installation is as follows: Solaris ™ systems: `/opt/SUNWmsgsr` Linux systems: `/opt/sun/messaging`
da_base	Represents the base installation directory for Delegated Administrator. The default value of the *da_base* installation is as follows: Solaris ™ systems: `/opt/SUNWcomm` Linux systems: `/opt/sun/comms/commcli`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions.

To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title of this book is *Sun Java System Communications Services 2005Q4 Delegated Administrator Guide*, and the part number is 819-2658.

CHAPTER 1

Delegated Administrator Overview

The Communications Services Delegated Administrator utility and console let you provision users, groups, domains, and resources in an LDAP directory used by Communications Services applications such as Messaging Server and Calendar Server.

This chapter describes the following topics:

Introduction

With Delegated Administrator, you can distribute provisioning tasks to lower-level administrators who have the authority to manage specified organizations in the LDAP directory. The power to delegate user administration offers the following advantages:

- Distributes among many administrators the potentially time-consuming responsibility for provisioning a large directory. Tens or hundreds of administrators can manage organizations within a directory that may include thousands or millions of users.
- Allows you to create organizations in the directory structure that can be managed and provisioned as distinct (or unique) units. These organizations can contain users belonging to customer businesses, corporate departments, or other groups.

Delegated Administrator provides two interfaces for provisioning users and organizations in the directory:

- "Delegated Administrator Console" on page 22

These interfaces are summarized in the sections that follow.

Delegated Administrator Utility

The Delegated Administrator utility is a set of command-line tools for provisioning Messaging Server and Calendar Server organizations, users, groups, and Calendar resources.

Note – The Delegated Administrator utility provides the command-line functions that were available in previous releases of Communications Services products (Messaging Server 6 2005Q1 and Calendar Server 6 2005Q1). The Delegated Administrator utility does not offer commands for creating the Service Provider roles and organizations described in this book. To create and manage these new roles and organizations, you must use the Delegated Administrator console.

You invoke the utility with the `commadmin` command.

For information about the syntax and options available with the `commadmin` utility, see Chapter 5

Delegated Administrator Console

The Delegated Administrator console is a graphical user interface (GUI) for provisioning Messaging Server and Calendar Server organizations, users, groups, and Calendar resources.

For information on how to use the console, see the Delegated Administrator console online help.

Delegated Administrator and the LDAP Directory

Delegated Administrator enables you to provision users by modifying the LDAP directory. You do not need to modify the directory directly. However, it can be useful to understand the Delegated Administrator attributes added to user entries and higher-level nodes in the directory.

For information about the LDAP schema object classes and attributes that support Delegated Administrator, see "Chapter 5: Communications Services Delegated Administrator Classes and Attributes (Schema 2)" in the *Sun Java System Communications Services Schema Reference*.

Scenarios for Provisioning Users

Depending on your business needs, you can create a simple directory structure managed by a single administrator or a multi-tiered directory hierarchy in which provisioning and management tasks are delegated to lower-level administrators.

This section summarizes three scenarios of increasing complexity. It then describes the administrator roles and directory structures Delegated Administrator provides to support the requirements of these scenarios.

One-Tiered Hierarchy

In this scenario, a company or organization might support hundreds or thousands of employees or users. All users are grouped in a single organization. A single administrator role views and manages the entire group. There is no delegation of administrative tasks.

Figure 1–1 shows an example of the administrator role in a single-organization, one-tiered hierarchy.

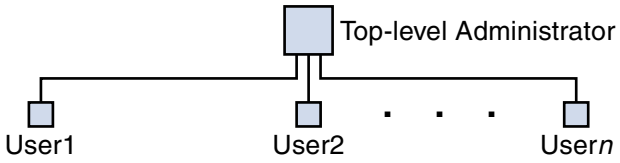

FIGURE 1–1 Administrator Role in a One-Tiered Hierarchy

In this one-tiered hierarchy, the administrator is called the Top-Level Administrator (TLA).

In the example shown in Figure 1–1, the TLA directly manages and provisions the users (User1, User2, up to Usern).

If you have one organization in your directory, the TLA is the only administrator you need.

For more information, see the following sections:

- "Directory Structure Supporting a One-Tiered Hierarchy" on page 26
- "Top-Level Administrator Role" on page 28.

Two-Tiered Hierarchy

In this scenario, a large company such as an Internet Service Provider (ISP) provides services to businesses. Each business has its own unique domain, which may contain thousands or tens of thousands of users.

Instead of relying on a single Top-Level Administrator (TLA) to manage and provision all the domains, this scenario supports the delegation of tasks to lower-level administrators.

In a two-tiered hierarchy, the directory contains multiple organizations. A separate organization is created for each hosted domain.

Each organization is assigned to an Organization Administrator (OA). The OA is responsible for the users in that organization. An OA cannot view or modify directory information outside the OA's own organization.

Figure 1–2 shows an example of the administrator roles in a two-tiered hierarchy.

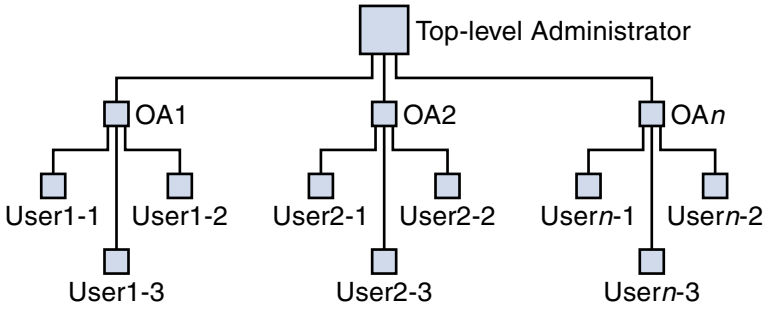

FIGURE 1–2 Administrator Roles in a Two-Tiered Hierarchy

In the example shown in Figure 1–2, the TLA creates and manages OA1, OA2, up to OAn. Each OA manages the users in one organization.

If you need multiple organizations in your directory, you should create the TLA and OAs to administer the organizations and their users.

For more information, see the following sections:

- "Directory Structure Supporting a Two-Tiered Hierarchy" on page 28
- "Top-Level Administrator Role" on page 28
- "Organization Administrator Role" on page 29.

Three-Tiered Hierarchy

In this scenario, a company such as an ISP offers services to hundreds or thousands of small businesses, each of which requires its own organization.

The ISP may support millions of end-users requiring mail services. Moreover, the ISP may work with third-party resellers who manage the end-user businesses.

Each day, dozens of new organizations might have to be added to the directory.

In a two-tiered hierarchy, the TLA would have to create all these new organizations.

In a three-tiered hierarchy, management tasks are delegated to a second level of administrators. This second level of delegation can ease the management of a large customer base supported by a large LDAP directory.

To support this hierarchy, Delegated Administrator introduces a new role, the Service Provider Administrator (SPA).

The SPA's scope of authority lies between that of the Top-Level Administrator (TLA) and the Organization Administrator (OA).

Figure 1–3 shows an example of the administrator roles in a three-tiered hierarchy.

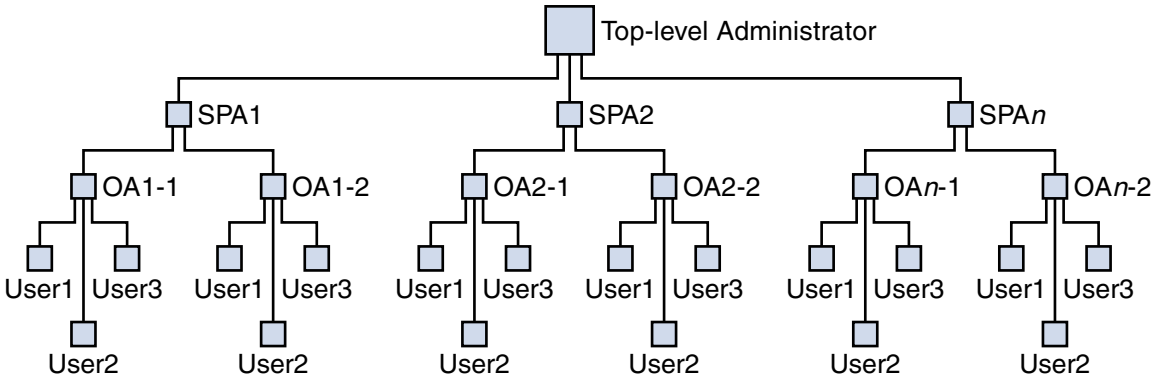

FIGURE 1–3 Administrator Roles in a Three-Tiered Hierarchy

In a three-tiered hierarchy, the TLA delegates administrative authority to Service Provider Administrators (SPAs). The SPAs can create subordinate organizations for new customers and assign Organization Administrators (OAs) to manage users in those organizations.

If you need multiple organizations that are themselves divided into subgroups or organizations, you can use a three-tiered hierarchy that implements the TLA, SPA, and OA roles.

For information about the SPA role, see Appendix A.

Administrator Roles and the Directory Hierarchy

This section shows sample Directory Information Trees that implement one- and two-tiered hierarchies. It then describes the tasks that can be performed by the Top-Level Administrator and Organization Administrator.

Directory Structure Supporting a One-Tiered Hierarchy

When you configure Delegated Administrator by running the configuration program, `config-commda`, you create a Top-Level Administrator (TLA) and a default organization.

One-Tiered Hierarchy: Default Organization Under the Root Suffix

By default, the configuration program places the default organization under the root suffix.

The Directory Information Tree will look similar to the one shown in Figure 1–4.

Figure 1–4 shows a sample Directory Information Tree organized in a one-tiered hierarchy (default configuration).

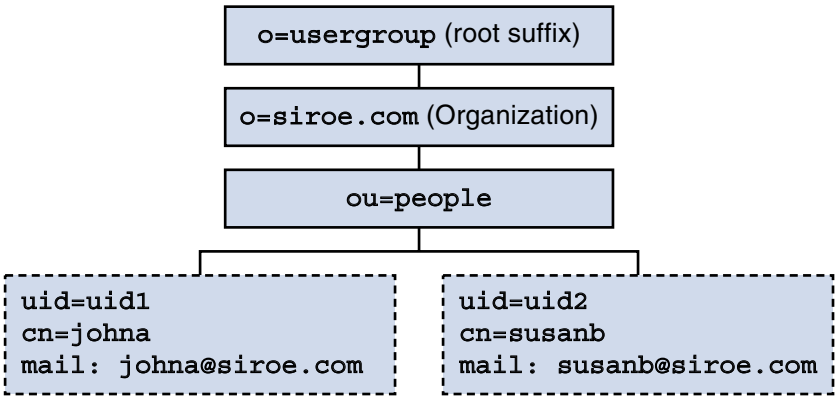

FIGURE 1–4 One-Tiered Hierarchy: Sample Directory Information Tree (default)

One-Tiered Hierarchy: Default Organization at the Root Suffix

When you run the configuration program, `config-commda`, you can choose to create the default organization at the root suffix instead of under it. For configuration details, see "Configuring the Delegated Administrator Server" on page 68 in Chapter 3.

In this situation, the Directory Information Tree will look similar to the one shown in Figure 1–5.

However, if you create the default organization at the root suffix, this configuration of the LDAP directory cannot support multiple hosted domains. To support hosted domains, the default organization must be under the root suffix.

Figure 1–5 shows a sample one-tiered hierarchy in which the default organization is created at the root suffix.

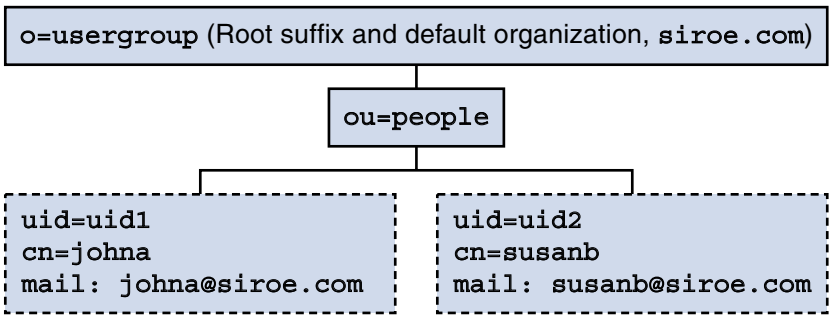

FIGURE 1–5 One-Tiered Hierarchy: Default Organization at Root Suffix

Directory Structure Supporting a Two-Tiered Hierarchy

After Delegated Administrator has been configured with the `config-commda` program, the TLA can create additional organizations, as shown in Figure 1–6.

Figure 1–6 shows a sample Directory Information Tree organized in a two-tiered hierarchy.

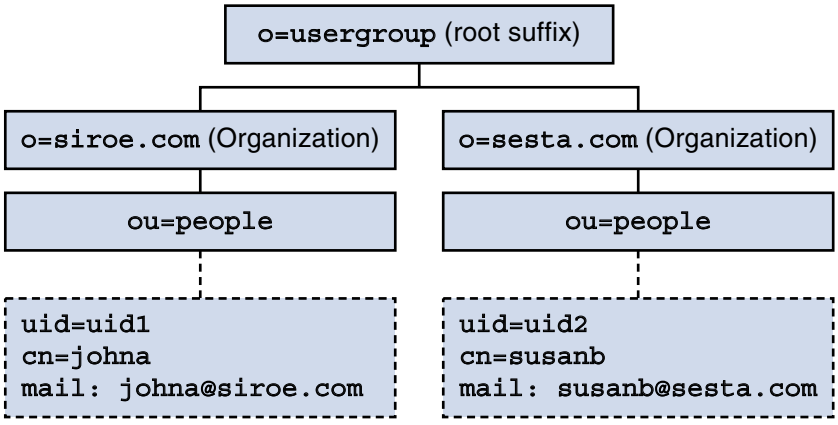

FIGURE 1–6 Two-Tiered Hierarchy: Sample Directory Information Tree

Top-Level Administrator Role

The TLA has the authority to perform the following tasks:

- Create, delete, and modify organizations.

In the example shown in Figure 1–6, the TLA can modify or delete `siroe.com` or `sesta.com` and can create additional organizations.

Note that in this example, the two organizations are also unique (hosted) domains.

- Create, delete, and modify users.
- Create, delete, and modify groups.
- Create, delete, and modify Calendar resources.
- Assign OA roles to users. For example, the TLA could assign an OA role to the user `johna` in the `siroe.com` organization.

  The TLA also can remove the OA role from a user.
- Assign TLA roles to other users. The TLA also can remove the TLA role from a user.
- Assign service packages to organizations.

  For information about service packages, see "Service Packages" on page 31, later in this overview.

  The TLA can assign specified types of service packages to an organization and determine the maximum number of each package that can be used in that organization.

  For example, the TLA could assign the following service packages:

  - In the `siroe.com` organization:

    ```
    1,000 gold packages
    500 platinum packages
    ```
  - In the `sesta.com` organization:

    ```
    2,000 silver packages
    1,500 gold packages
    100 platinum packages
    ```

    The TLA can perform the preceding tasks by using the Delegated Administrator console or by executing Delegated Administrator utility (`commadmin`) commands.

    For a description of the `commadmin` commands, see Table 5–1 in Chapter 5.

Organization Administrator Role

The OA has the authority to perform the following tasks within the OA's organization:

- Create, delete, and modify users.

  In the example shown in Figure 1–6, if the user `johna` is assigned the OA role in the `siroe.com` organization, `johna` can manage users in `siroe.com`.
- Create, delete, and modify groups.
- Create, delete, and modify Calendar resources.

- Assign the OA role to other users.
- Assign and remove service packages for users.

The OA cannot perform any of these tasks for users, groups, or resources outside the OA's organization.

For example, if `johna` is the OA for `siroe.com` in Figure 1–6, `johna` cannot manage users, groups, or resources in `sesta.com`.

The OA can perform the preceding tasks by using the Delegated Administrator console or by executing Delegated Administrator utility (`commadmin`) commands.

For a description of the `commadmin` commands available to the OA, see Table 5–1 in Chapter 5.

For Former Users of iPlanet Delegated Administrator

Communications Services Delegated Administrator is designed for provisioning users in an LDAP Schema 2 directory.

Users of previous versions of Messaging Server who have an LDAP Schema 1 directory may have used iPlanet Delegated Administrator, a deprecated tool. If you still have a Schema 1 directory, you should use iPlanet Delegated Administrator to provision users.

iPlanet Delegated Administrator uses slightly different terms for the administrator roles than those currently used by Communications Service Delegated Administrator.

Table 1–1 lists and defines the administrator roles in each version of Delegated Administrator.

TABLE 1–1 Administrator Roles in iPlanet Delegated Administrator and Communications Services Delegated Administrator

iPlanet Delegated Administrator	Communications Services Delegated Administrator Utility	Communications Services Delegated Administrator Console	Definition
Site Administrator	Top-Level Administrator (TLA)	Top-Level Administrator (TLA)	Manages the entire directory supported by Delegated Administrator, including the organizations and users*.

TABLE 1–1 Administrator Roles in iPlanet Delegated Administrator and Communications Services Delegated Administrator *(Continued)*

iPlanet Delegated Administrator	Communications Services Delegated Administrator Utility	Communications Services Delegated Administrator Console	Definition
(None)	(None in this release)	Service Provider Administrator (SPA)	Manages a provider organization, the shared and full business organizations under the provider organization, and users in those business organizations.
Domain Administrator	Organization Administrator (OA)	Organization Administrator (OA)	Manages one organization and the users in that organization.
* In this release of Delegated Administrator, the TLA cannot create provider organizations or business organizations under a provider organization.			

Service Packages

A service package is implemented by the Class-of-Service mechanism in the LDAP directory. This mechanism lets you set values for predefined attributes that are installed in the directory when you configure Delegated Administrator. A service package adds the characteristics of the service to user or group entries.

Delegated Administrator provides sample Class-of-Service templates.

You can also create your own service packages.

In the Delegated Administrator console, you can assign the sample packages and your own packages to users or groups.

Types of Service Packages

A service package includes the following components:

- Access Manager service

- Service bundle (mail service and/or calendar service)
- LDAP object (users or groups)

Delegated Administrator automatically provides Access Manager service with every service definition. When you assign a service package to a user or group, Delegated Administrator takes the Access Manager object classes and attributes from the service definition and adds them to the LDAP entry.

Do not change or delete the Access Manager portion of any service package.

When you create a service package, you can configure its service bundle and LDAP object.

Service Bundles

Delegated Administrator provides two types of service: mail service and calendar service.

A service package bundles one or more services, together with a set of attributes associated with that service. Thus, an individual service package can contain the following combinations of services:

- Mail service only
- Calendar service only
- Mail and calendar service

Note – Only mail service has LDAP attributes in its Class-of-Service definition. Calendar service has no attributes associated with it.

Packages Defined for Particular LDAP Objects

A service package is defined either for users or for groups. You cannot assign the same service package to a user and a group.

Delegated Administrator provides service packages with the following service bundles and LDAP objects:

- User mail service
- User calendar service
- User mail and calendar service
- Group mail service

Note – Only mail service can be assigned to groups. In this release of Delegated Administrator, a group cannot have calendar service.

About Groups

In Delegated Administrator, a group is an entry in the LDAP directory that comprises a list of users. Characteristics of the group are not passed on to the users who are members of the group. For example, when you assign a service package to a group, the service package attributes are not inherited by the users who are members of the group.

When a mail service package is assigned to a group, the group becomes a mailing list, which is used by Messaging Server.

Service Packages Provided by Delegated Administrator

When you configure Delegated Administrator, you can choose to install a set of predefined, sample Class-of-Service templates. The Delegated Administrator console displays these templates.

(When you run the configuration program, select **Load sample service packages** in the **Service Package and Organization Samples** panel.) The configuration program adds the `cos.sample.ldif` file to the LDAP directory.

You can use the sample templates to provide services and mail attributes to users and groups. For a list of the templates with their attribute values, see "Sample Class-of-Service Templates" on page 37.

If you do not intend to use the sample Class-of-Service templates, you can remove them from the LDAP directory and the console display by modifying a skeleton ldif file. For details, see XX.

Figure 1–7 shows the user service package templates.

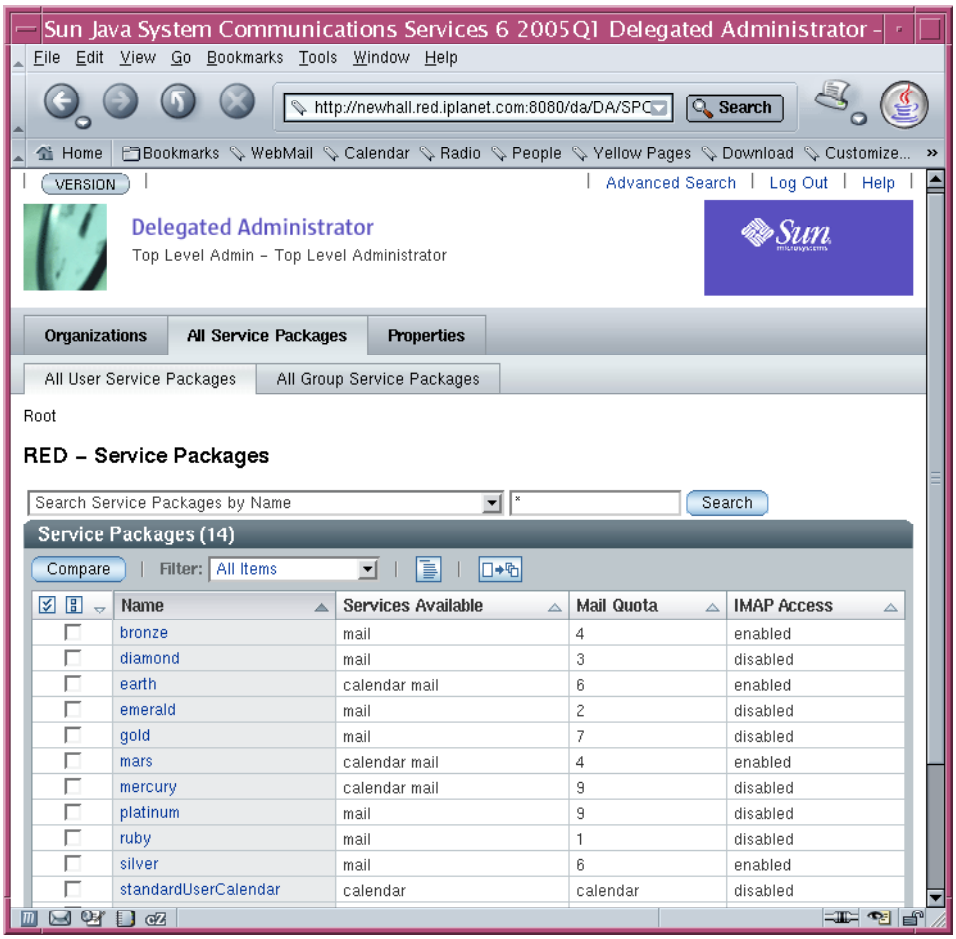

FIGURE 1–7 All User Service Packages page — sample templates displayed

Figure 1–8 shows the group service package templates.

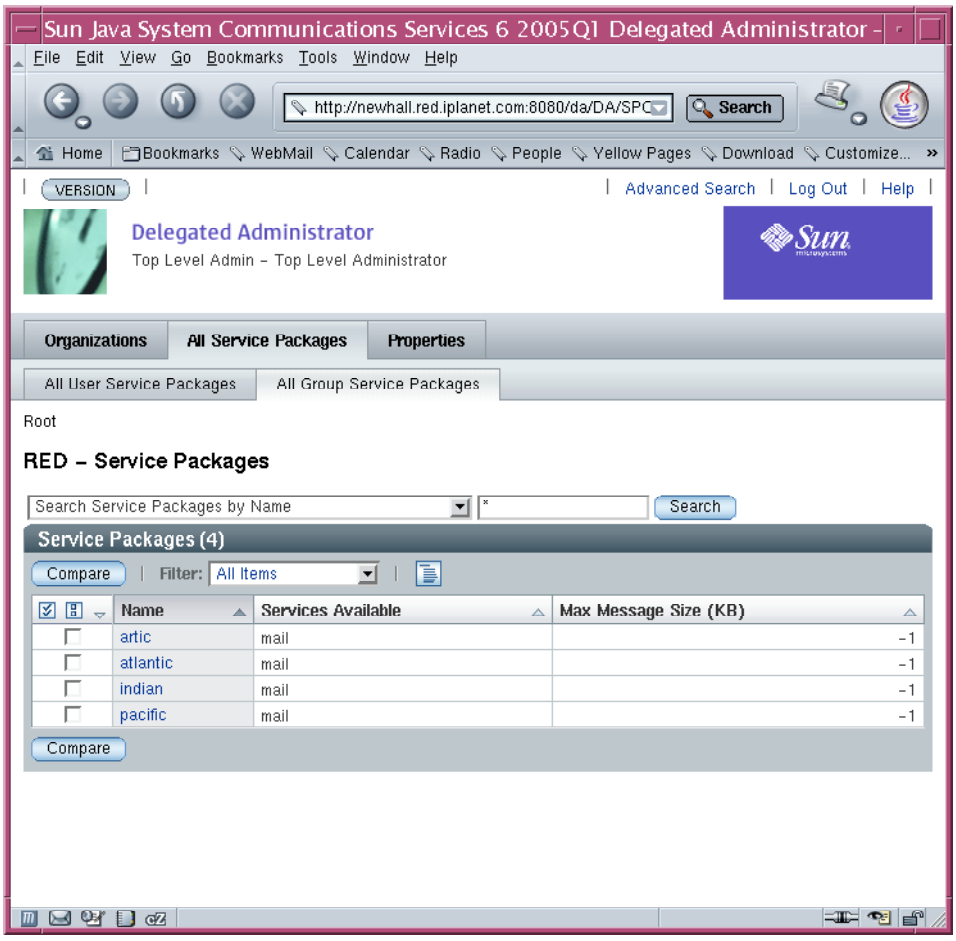

FIGURE 1–8 All Group Service Packages page — sample templates displayed

Service-Package Tasks

In the Delegated Administrator console, you perform the following service-package tasks:

- Allocate service packages to organizations. By allocating some (or all) packages to an organization, you make those packages available to users or groups in the organization.

  For each package, you allocate a specified number of packages.

  For example, for the ABC organization, you might allocate 5,000 gold service packages, 10,000 venus service packages, and 500 atlantic service packages.

- Assign service packages to users.
- Assign service packages to groups.

Guidelines for Assigning Service Packages

- The service packages allocated to an organization make up the pool from which service packages can be assigned to users or groups in the organization.
- You can assign multiple service packages to a user or group.
- When you assign a service package to a user or group, all the attributes and values in the service package are automatically assigned to the user or group.
- To assign only calendar service to a user, use the standardUserCalendar service package. Calendar service does not have any associated attributes.

  Assigning the standardUserCalendar service package is equivalent to using the `-s cal` option in the `commadmin user create` or `commadmin user modify` command.

For instructions on how to allocate and assign service packages, see the Delegated Administrator console online help.

Creating Your Own Service Packages

The Class-of-Service templates described in this chapter are meant to be examples. Most likely you will want to create your own service packages with attribute values appropriate for the users and groups in your installation.

To create your own service packages, you can use a Class-of-Service template stored in the `da.cos.skeleton.ldif` file. This file was created specifically for use as a template for writing service packages. It is not installed in the LDAP directory when Delegated Administrator is configured.

You can copy and edit the `da.cos.skeleton.ldif` file and use an LDAP directory tool such as `ldapmodify` to install your customized Class-of-Service templates in the directory.

The Delegated Administrator console displays your customized templates along with the sample templates. In the console, the Class-of-Service template is called a service package. When you can assign a service package either to a user or to a group, Delegated Administrator populates the user or group LDAP entry with a complete service package, including Access Manager service.

For instructions on using the `da.cos.skeleton.ldif` file to configure your own service packages, see "Create Service Packages" on page 76 in Chapter 3.

Limitations in Viewing an Extended Service Package

You can extend the Delegated Administrator service package definition by adding any attribute to the definition entry.

However, in this release of Delegated Administrator, the console allows you to view only the predefined attributes provided when Delegated Administrator is configured. The Delegated Administrator console does not display any attributes you add to a service package definition.

In this release, you also should not remove the predefined attribute definitions from the Class-of-Service definitions provided by Delegated Administrator.

Sample Service Package Assigned to an LDAP Entry

When you use Delegated Administrator to assign a service package to a user or group, a single attribute (`inetCOS`) is added to the user or group entry in the LDAP directory. The value of the `inetCOS` attribute assigns the entire service package to the user or group, including the service and any attributes associated with that service. (`inetCOS` is a multi-valued attribute.)

For example, suppose you assign the platinum package to a user. The following attribute is added to the user entry:

```
inetCOS: platinum
```

The platinum package provides mail service to the user. The package also contains the following values for mail attributes. Thus, assigning the platinum package has the effect of adding these attributes to the user entry:

```
mailMsgMaxBlocks: 800
mailQuota: 10000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
```

The Access Manager service definition provides the object classes and attributes required for the mail and/or calendar service. When you assign the service package, Delegated Administrator adds these object classes and attributes to the user or group entry.

Sample Class-of-Service Templates

This section lists the sample Class-of-Service templates and mail attribute values provided by the templates.

These templates are contained in the `cos.sample.ldif` file.

Mail Service Attributes

Mail service includes LDAP attributes defined for mail users. Table 1–2 defines these attributes.

TABLE 1–2 Mail service attributes that can be used in a service package

Attribute	Definition
`mailMsgMaxBlocks`	Size in units of MTA blocks of the largest message that can be sent to the user or group.
`mailAllowedServiceAccess`	Filter specifying the available client access to specified services. For example: `+imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL`
`mailMsgQuota`	Maximum number of messages permitted for a user (including all user folders).
`mailQuota`	Disk space (in bytes) allowed for the user's mailbox.

For more information about these attributes, see "Chapter 3: Messaging Server and Calendar Server Attributes" in the *Sun Java System Communications Services Schema Reference*.

User Mail Sample Templates

Platinum

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Gold

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Silver

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Bronze

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Ruby

```
mailMsgMaxBlocks: 600
mailquota: 1048576
mailmsgquota: 2000
mailAllowedServiceAccess: +pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Emerald

```
mailMsgMaxBlocks: 600
mailquota: 2097152
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Diamond

```
mailMsgMaxBlocks: 5000
mailquota: 3145728
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Topaz

```
mailMsgMaxBlocks: 3000
mailquota: 4194304
mailmsgquota: 2000
mailAllowedServiceAccess: +imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

User Calendar Sample Templates

None (standardUserCalendar)

There is no predefined Class-of-Service template that provides calendar service and contains attribute values. Calendar service is provided without associated attributes.

Because no sample template exists, Delegated Administrator generates a default service package, without a template, directly from the User Calendar Class-of-Service definition. Its name is the same as that of the Class-of-Service definition: standardUserCalendar.

This service package provides calendar service only.

User Mail and Calendar Sample Templates

The following sample templates apply both mail and calendar service.

Mercury

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Venus

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Earth

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Mars

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Group Mail Sample Templates

Atlantic

```
mailMsgMaxBlocks: 800
daServiceType: mail group
```

Pacific

```
mailMsgMaxBlocks: 900
daServiceType: mail group
```

Indian

```
mailMsgMaxBlocks: 1000
daServiceType: mail group
```

Arctic

```
mailMsgMaxBlocks: 1200
daServiceType: mail group
```

Class-of-Service Definitions

This release of Delegated Administrator provides a Class-of-Service definition for each type of service package:

- User mail service
- User calendar service
- User mail and calendar service
- Group mail service

When you configure Delegated Administrator, the Class-of-Service definitions are installed in the directory.

In each definition, the `daServiceType` attribute determines the type of service package with the following syntax:

`daServiceType: <`*service type*`> <`*target*`>`

where *service type* is mail service, calendar service, or both, and *target* is either user or group.

Mail Service for Users

The user mail service is defined in a Class-of-Service definition called `standardUserMail`:

```
#
#  Definition for user mail service bundle
#
dn: cn=standardUserMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: mail user


NOTE: When the Delegated Administrator configuration program installs the
standardUserMail definition in the directory, the variable
<ugldapbasedn>, shown above, is replaced by your root suffix
(such as o=usergroup).
```

The `daServiceType` attribute defines this as a mail service for users.

Calendar Service for Users

The user calendar service is defined in a Class-of-Service definition called `standardUserCalendar`:

```
#
#  Definition for user calendar service bundle
#
dn: cn=standardUserCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
daServiceType: calendar user


NOTE: When the Delegated Administrator configuration program installs the
standardUserCalendar definition in the directory, the variable
<ugldapbasedn>, shown above, is replaced by your root suffix
(such as o=usergroup).
```

The daServiceType attribute defines this as a calendar service for users.

Note – Note that the calendar service definition also includes calendar attributes such as icsPreferredHost.

However, Delegated Administrator does not provide service-package templates that specify values for these attributes. The Delegated Administrator console provides one service package with calendar service only: the standardUserCalendar service package. This package does not include calendar attributes.

Mail and Calendar Service for Users

The user mail and calendar service is defined in a Class-of-Service definition called standardUserMailCalendar:

```
#
#  Definition for user mail and user calendar service bundle
#
dn: cn=standardUserMailCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
cosAttribute: icsQuota
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: calendar user
daServiceType: mail user


NOTE: When the Delegated Administrator configuration program installs the
standardUserMailCalendar definition in the directory, the variable
<ugldapbasedn>, shown above, is replaced by your root suffix
(such as o=usergroup).
```

The two daServiceType attribute entries define this as a calendar service and mail service for users.

Mail Service for Groups

The group mail service is defined in a Class-of-Service definition called standardGroupMail:

```
#
#  Definition for group mail service bundle
#
dn: cn=standardGroupMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailMsgMaxBlocks
daServiceType: mail group
```

```
NOTE: When the Delegated Administrator configuration program installs the
standardGroupMail definition in the directory, the variable <ugldapbasedn>,
shown above, is replaced by your root suffix (such as o=usergroup).
```

The `daServiceType` attribute defines this as a mail service for groups.

Location of Class-of-Service Definitions and Packages

In the LDAP Directory Information Tree (DIT), the Class-of-Service definitions are located in a node directly under the root suffix. Because they are stored at the top of the DIT, the service packages can be assigned to all user entries in the directory.

Figure 1–9 shows the location of the service definitions and packages in the DIT.

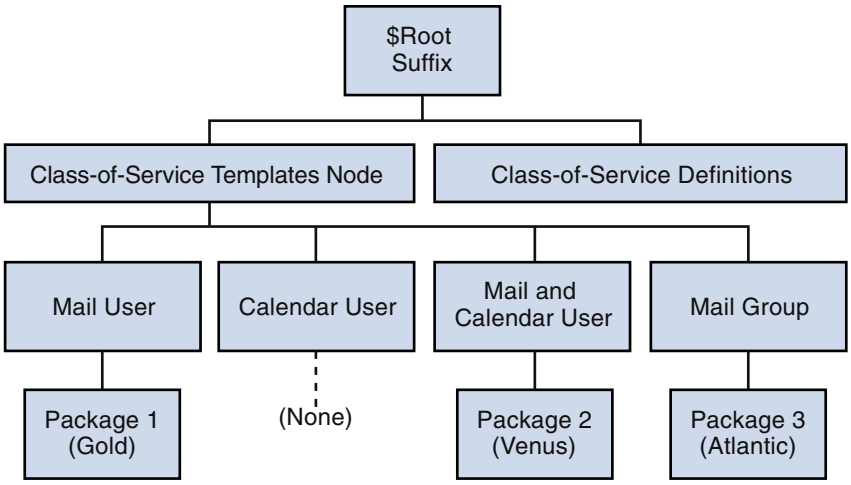

FIGURE 1–9 Location of Class-of-Service Definitions and Packages in the Directory Tree

Each type of Class-of-Service template is located under its own node. Thus, a template providing mail service to users is located under the Mail User node. This structure enables Delegated Administrator to use the correct Class-of-Service definition (such as `standardUserMail`) when it assigns a service package to a user or group.

Delegated Administrator uses the classic Class-of-Service definition.

For more information about the Class-of-Service mechanism, see the *Sun Java System Directory Server Administration Guide*. Specifically, see "Defining Class-of-Service (CoS)" in "Chapter 5: Managing Identity and Roles."

The *Sun Java System Directory Server Administration Guide* also describes related topics such as determining which service attribute value takes precedence if an attribute defined in a service package assigned to a user already exists in that individual user entry.

CHAPTER 2

Planning for Installation and Configuration

To install Sun Java System Communications Services Delegated Administrator on Solaris systems, you must use the Sun Java Enterprise System installer, which also installs other Sun component products.

To install and configure Delegated Administrator, follow these steps:

1. "Gather Your Delegated Administrator Configuration Information" on page 47
2. "Run the Java Enterprise System Installer" on page 51
3. "Run the Directory Server Setup Script" on page 52
4. "Configure Delegated Administrator" on page 53
5. "Configure Messaging Server and Calendar Server" on page 54

   For the most recent information about Delegated Administrator, see the *Sun Java System Communications Services Release Notes*.

Gather Your Delegated Administrator Configuration Information

Delegated Administrator Components

Delegated Administrator comprises the following components:

- **Delegated Administrator Utility (client)**—the command-line interface invoked with `commadmin`.

  Required. You must configure the utility on all machines on which you install Delegated Administrator.

- **Delegated Administrator Server**—the Delegated Administrator server components needed to run the Delegated Administrator utility and console.

  Required. You must configure the Delegated Administrator server on at least one machine.
- **Delegated Administrator Console**—the Delegated Administrator graphical user interface (GUI).

  Optional. If you want to use only the Delegated Administrator utility, you do not have to configure the console.

Web Containers

In addition, the Delegated Administrator server and console must be deployed to a Web container. You can configure the Delegated Administrator console and server on

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

Follow these guidelines:

- The Delegated Administrator server must be deployed to the Web container used by Access Manager.
- You can deploy the Delegated Administrator console and server on two different Web containers, on two different instances of the Web container, or on the same Web container.

Configuration Information

Before configuring Delegated Administrator, you should gather configuration information.

Table 2–1 lists the configuration options required for Delegated Administrator.

Table 2–2 lists the configuration options for deploying on Web Server.

Table 2–3 lists the configuration options for deploying on Application Server 7.*x*.

Table 2–4 lists the configuration options for deploying on Application Server 8.*x*.

TABLE 2–1 Delegated Administrator: Required Configuration Options

Option	Description
Configuration Directory	Directory to store configuration and data files.

TABLE 2–1 Delegated Administrator: Required Configuration Options *(Continued)*

Option	Description
Access Manager Host name	Host name where Access Manager is installed. The Delegated Administrator server should be installed on the same server.
Access Manager port number	Port number of Access Manager. Should be the same port number as Web Server port number.
Default domain	The default domain of the Top-Level Administrator. This is the domain used when a domain is not explicitly specified by the `-n` option when executing the `commadmin` command-line utility.
Default SSL port	The SSL port that is used by the Delegated Administrator client.
Access Manager Base Directory	The directory where Access Manager is installed. The default directory is `/opt/SUNWam`.
LDAP URL	User and Group Directory Server LDAP URL.
Bind as	User and Group Directory Server Directory Manager. For example “cn=Directory Manager”.
LDAP password	User and Group Directory Manager Password.
Access Manager Top-level administrator user ID and password	User ID and password for the Access Manager Top-level Administrator
Password for the Access Manager Internal LDAP authentication user	User created by Access Manager. This is the BindDN user for the LDAP service.
Organization name	Used to name the LDAP subtree under which all email users and groups that belong to the default email domain are located.
Top-level administrator for default organization user ID and password	User ID and password for the Top-Level Administrator that will be created in the default organization.
Preferred mail host for sample organizations	Name of the machine on which Messaging Server is installed. If you choose to install sample organizations in your directory, you must enter the preferred mail host.

TABLE 2–2 Web Server Configuration Options

Option	Description
Web Server root (instance) directory	Directory where the Web Server instance resides. Files for the Web Server instance are stored in the `https-`*host*`.`*domain* directory under the Web Server installation directory.
Web Server instance identifier	Fully qualified domain name for the Web Server instance. This can be specified by a *host.domain* name such as `west.sesta.com`.

TABLE 2–2 Web Server Configuration Options *(Continued)*

Option	Description
Virtual server identifier	Specified by a `https-`*host.domain* name such as `https-west.sesta.com`.
HTTP port number	HTTP port number for the Web Server.

TABLE 2–3 Application Server 7.*x* Configuration Options

Option	Description
Application Server installation directory	Directory where Application Server 7.*x* is installed. By default, this directory is `/opt/SUNWappserver7`.
Application Server domain directory	By default, this directory is `/var/opt/SUNWappserver7/domains/domain1`.
Application Server document root directory	By default, this directory is `/var/opt/SUNWappserver7/ \ domains/domain1/server1/docroot`
Application Server instance name	Name of the instance. For example: `server1`.
Virtual server identifier	Name of the Application Server virtual server identifier. For example: `server1`.
Application Server instance HTTP port number	HTTP port number for the Application Server instance.
Administration Server port number	Port number for the Administration Server instance for Application Server 7.*x*. For example: `4848`.
Administration Server administrator user ID and password.	User ID and password for the Administration Server administrator. User ID example: `admin`
HTTP or HTTPS access to Administration Server instance	You will need to specify whether the HTTP access to the Administration Server instance is secure or not.

TABLE 2–4 Application Server 8.*x* Configuration Options

Option	Description
Application Server installation directory	Directory where Application Server 8.*x* is installed. By default, this directory is `/opt/SUNWappserver/appserver`.
Application Server domain directory	By default, this directory is `/var/opt/SUNWappserver/domains/domain1`.
Application Server document root directory	By default, this directory is `/var/opt/SUNWappserver/domains/domain1/docroot`

TABLE 2–4 Application Server 8.*x* Configuration Options *(Continued)*

Option	Description
Application Server target name	Name of the instance. For example: `server`.
Virtual server identifier	Name of the Application Server virtual server identifier. For example: `server`.
Application Server target HTTP port number	HTTP port number for the Application Server target.
Administration Server port number	Port number for the Administration Server instance for Application Server 8.*x*. For example: `4849`.
Administration Server administrator user ID and password.	User ID and password for the Administration Server administrator. User ID example: `admin`
HTTP or HTTPS access to Administration Server instance	You will need to specify whether the HTTP access to the Administration Server instance is secure or not.

Run the Java Enterprise System Installer

The Java Enterprise System installer program installs a series of products, shared components, and libraries that interoperate with one another.

To successfully install and configure Delegated Administrator, you need to install the following components by running the Java Enterprise System installer:

- Sun Java System Directory Server 5.x
- Sun Java System Access Manager 7.0

  Access Manager 7 has two installation types: Legacy Mode (the default) and Realm Mode. Legacy Mode is compatible with Delegated Administrator.

  When you run the Java Enterprise System installer, in the first Access Manager panel, you must choose Legacy mode as the Install type. Do not choose Realm mode.

  Because Delegated Administrator requires you to use LDAP Schema 2 to provision your users and groups, you need to install Access Manager.
- One of the following Web containers:
  - Sun Java System Web Server 6.1
  - Sun Java System Application Server 7.*x*
  - Sun Java System Application Server 8.*x*

(The Java Enterprise System installer also checks to make sure you have installed Directory Server 5.x and one of the Web containers listed above.)

One or both of Sun Java System Messaging Server and Sun Java System Calendar Server.

Delegated Administrator is a provisioning tool for Messaging Server and Calendar Server. Therefore, to use Delegated Administrator successfully, you should install either or both of these applications.

Note – It is *not* recommended that Messaging Server or Calendar Server be installed on the same system as Access Manager.

See the *Sun Java System Messaging Server Administration Guide* for instructions on configuring Messaging Server. See the *Sun Java System Calendar Server Administration Guide* for instructions on configuring Calendar Server.

- Delegated Administrator

  A panel in the Java Enterprise System installer asks whether to install Delegated Administrator. In this panel, specify that you want to install Delegated Administrator.

  (In earlier releases, Delegated Administrator was installed automatically with Access Manager.)

  The installer installs Delegated Administrator in a directory referred to as the *da_base* (for example, the default is `/opt/SUNWcomm`).

For information about the Java Enterprise System installer, refer to the *Sun Java Enterprise System Installation Guide*.

Note – If you are upgrading Delegated Administrator from a previous Sun Java System version, see the chapter called "Upgrading Delegated Administrator" in the *Sun Java Enterprise System Upgrade and Migration Guide*.

Run the Directory Server Setup Script

Before configuring Delegated Administrator, Messaging Server, or Calendar Server, the Directory Server Preparation Tool script (`comm_dssetup.pl`) must be run. You only need to run the `comm_dssetup.pl` script once.

This script configures your LDAP Directory Server to work with Delegated Administrator, Messaging Server, or Calendar Server configurations. The `comm_dssetup.pl` script prepares the Directory Server by setting up new schema, index, and configuration data.

See the *Sun Java System Messaging Server Administration Guide* or the *Sun Java System Calendar Server Administration Guide* for instructions and options for the `comm_dssetup.pl` script.

In order to run Delegated Administrator, you must select the "Schema 2" schema type when running the `comm_dssetup.pl` script.

Consolidating ACIs in the Directory

For large-scale installations with Access Manager, Messaging Server, and an LDAP Schema 2 directory, you might want to consolidate the Access Control Instructions (ACIs) in your directory.

When you install Access Manager with Messaging Server, a large number of ACIs initially are installed in the directory. Many default ACIs are not needed or used by Messaging Server. You can improve the performance of Directory Server and, consequently, of Messaging Server look-ups, by consolidating and reducing the number of default ACIs in the directory.

For information about how to consolidate and discard unused ACIs, see Appendix E later in this guide.

Configure Delegated Administrator

After you install Delegated Administrator, run the Delegated Administrator configuration program using the information from "Gather Your Delegated Administrator Configuration Information" on page 47

For information about running the configuration program, see Chapter 3.

Configure Messaging Server and Calendar Server

See the *Sun Java System Messaging Server Administration Guide* for instructions on configuring Messaging Server. See the *Sun Java System Calendar Server Administration Guide* for instructions on configuring Calendar Server.

CHAPTER 3

Configuring Delegated Administrator

The Delegated Administrator configuration program (`config-commda`) creates a new configuration with your specific requirements. This initial runtime configuration program performs minimal configuration.

After you run the program, complete the initial configuration by following the steps described in "Post-Configuration Tasks" on page 75.

You can further customize your Delegated Administrator configuration by performing the tasks described in Chapter 4.

You might need to perform additional configuration, as described in the *Sun Java System Messaging Server Administration Guide*.

The following topics are described in this chapter:

If You Are Upgrading from a Previous Release of Delegated Administrator

If you are configuring Delegated Administrator for the first time, you can skip this section and go directly to the section, "Choose Which Components to Configure" on page 59.

If you are upgrading to this release of Delegated Administrator from an earlier Java Enterprise System release, you might have to perform the following tasks before you configure Delegated Administrator:

- "Preserve an Existing Configuration" on page 56
- "Upgrade Customized Service Packages" on page 57

For instructions on how to upgrade Delegated Administrator from a previous Sun Java System version, see the chapter called "Upgrading Delegated Administrator" in the *Sun Java Enterprise System Upgrade Guide*.

Preserve an Existing Configuration

This section concerns you only if you previously have installed and configured Delegated Administrator and have customized the Delegated Administrator configuration.

If you have a customized configuration and you rerun the Delegated Administrator configuration program, `config-commda`, the properties in the configuration files are reset to their default values. These files are listed below, in "Delegated Administrator Properties Files" on page 56.

For information about how you can customize Delegated Administrator, see Chapter 4.

You should preserve your customized configuration before you upgrade Delegated Administrator or rerun the Delegated Administrator configuration program for any other reason.

Delegated Administrator Properties Files

Delegated Administrator installs the following properties files:

- `resource.properties`

  Default location:

  da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet`
- `daconfig.properties`

  Default location:

  da_base`/data/WEB-INF/classes/com/sun/comm/da/resources`
- `cli-usrprefs.properties`

  Default location: `/var/opt/SUNWcomm/config`
- `security.properties`

  Default location:
  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

- `Resources.properties`

  Default location:

  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`
- `logger.properties`

  Default location:

  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

▼ To Preserve an Existing Configuration

Steps

1. **Back up the properties files you have customized.**

   For a list of the properties files and their default locations, see "Delegated Administrator Properties Files" on page 56.

2. **Run the `config-commda` program, as described in the following sections.**

   The remaining steps use the `resource.properties` file as an example. Repeat these steps for each file you have customized.

3. **Edit the new `resource.properties` file created by the `config-commda` program, as follows:**

   a. **Open the new `resource.properties` file.**

   b. **Open your back-up copy of the `resource.properties` file.**

   c. **Locate the properties that were customized in the back-up copy. Apply the customized values to the corresponding properties in the new `resource.properties` file.**

      Do not simply overwrite the new `resource.properties` file with the entire back-up copy. The new file may contain new properties created to support this release of Delegated Administrator.

Upgrade Customized Service Packages

This section concerns you only if you are upgrading from Communications Services 6 2005Q1 Delegated Administrator to Communications Services 6 2005Q4 Delegated Administrator, and you created customized service packages in the previous release (6 2005Q1).

In the current (6 2005Q4) release of Delegated Administrator, service packages can provide calendar service and mail service, and they are targeted either at users or at groups. In the previous (6 2005Q1) release, service packages provided mail service to users only. Service package definitions include a new attribute to support the new functions.

Sample Class-of-Service Templates

When you run the Delegated Administrator configuration program, the previously installed sample Class-of-Service templates installed by the Delegated Administrator configuration program are upgraded automatically. (In the configuration program, you should select **Load sample service packages** in the **Service Package and Organization Samples** panel.)

If you use only the sample templates to assign service packages to users and groups, no action is required.

Customized Service Packages

The configuration program does not upgrade customized service packages created in the 6 2005Q1 release. You must upgrade your customized service packages manually.

For information on how customized service packages are created, see "Creating Your Own Service Packages" on page 76.

▼ To Upgrade Customized Service Packages

Steps

1. **Edit each customized service package by adding the following line to the ldif file defining the service package:**

   ```
   daServiceType: mail user
   ```

   The `daServiceType` attribute defines the type of service (mail or calendar) and the target (users or groups).

   Service packages created in the previous release only provided mail service to users. Thus, the value of `daServiceType` should be `mail user`.

   The following example shows what the edited ldif file might look like:

   ```
   dn: cn=myservicepackage,o=cosTemplates,o=mycompanysuffix
   changetype: modify
   replace: daServiceType
   daServiceType: mail user
   ```

2. **Use the LDAP directory tool `ldapmodify` to update the service package in the directory.**

   For example, you could run the following command:

   ```
   ldapmodify -D <directory manager> -w <password> -f
   myservicepackage
   ```

   where

   `<directory manager>` is the name of the Directory Server administrator.

`<password>` is the password of the Directory Service administrator.

`myservicepackage` is the name of the ldif file defining the customized service package.

Choose Which Components to Configure

The third panel in the configuration program asks which Delegated Administrator components you want to configure:

- **Delegated Administrator Utility (client)**—the command-line interface invoked with `commadmin`.
- **Delegated Administrator Server**—the Delegated Administrator server components required to run the Delegated Administrator utility and console.
- **Delegated Administrator Console**—the Delegated Administrator graphical user interface (GUI).

The configuration program displays different panels depending on which components you select.

The following steps summarize the configuration choices. Each summary step (below) links you to a section (later in this chapter) that walks you through the actual configuration panels.

▼ Summary of Configuration Choices

Steps

1. **"Starting the Configuration" on page 61**

   Enter the information requested in these panels to begin the configuration.

2. **"Configuring the Delegated Administrator Utility" on page 62**

   These panels follow directly after the **Select Components to Configure** panel. They ask for information used to configure the Delegated Administrator utility.

   The Delegated Administrator utility is required and must be configured on all machines on which you install a Delegated Administrator component (server or console).

   Therefore, you always must enter the information in these panels.

3. **"Configuring the Delegated Administrator Console" on page 63**

   These panels follow the panels that configure the utility.

You can choose whether or not to configure the Delegated Administrator console.

- If you deploy the Delegated Administrator console and server on the same machine, you would select both the console and the server in **Select Components to Configure** panel.
- You also can deploy the Delegated Administrator console and server on different machines.

  On the machine on which you deploy the console, you would select only the console on the **Select Components to Configure** panel. (The utility is always selected.)

  In this case, you must run the configuration program again on the machine on which you deploy the server.

  If you deploy the console and server on different machines, the utility is configured on *both* machines.

The configuration program displays different panels depending on which Web container you select for the console. You can deploy to one of the following Web containers:

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

If you are configuring the Delegated Administrator server and console on one machine, you will go through these instructions *twice* (once for the server, once for the console).

4. **"Configuring the Delegated Administrator Server" on page 68**

   These panels follow the panels that configure the console.

   You can choose whether or not to configure the Delegated Administrator server on a given machine.

   If you do not choose to configure the server on a given machine, the configuration program warns you that you must configure it on another machine. The server component is required for running the utility and console.

   All other considerations for deploying the server are the same as those for the console, as(described in "Configuring the Delegated Administrator Console" on page 63.

   Note also that the server uses the same Web container as Access Manager. (The configuration program asks for Web container information after it asks for Access Manager base directory.)

5. **"Completing the Configuration" on page 71**

   Enter the information requested in these panels to complete the configuration.

Run the Configuration Program

The steps described in this section walk you through configuring Delegated Administrator.

Launching the Configuration Program

To run the configuration program, log in as (or become) root and go to the `/opt/SUNWcomm/sbin` directory. Then enter the command:

```
# ./config-commda
```

Once you run the `config-commda` command, the configuration program starts.

The sections that follow lead you through the configuration panels.

Starting the Configuration

You must enter the information requested in the first configuration-program panels.

▼ To start the configuration

Steps

1. **Welcome**

   The first panel in the configuration program is a copyright page. Click **`Next`** to continue or **`Cancel`** to exit.

2. **Select directory to store configuration and data files**

   Select the directory where you want to store the Delegated Administrator configuration and data files. The default configuration directory is `/var/opt/SUNWcomm`. This directory should be separate from the *da_base* directory (`/opt/SUNWcomm`).

   Enter the name of the directory, or keep the default and click **`Next`** to continue.

   If the directory does not exist, a dialog appears asking if you want to create the directory or choose a new directory. Click **`Create Directory`** to create the directory or **`Choose New`** to enter a new directory.

   A dialog appears indicating that the components are being loaded. This may take a few minutes.

3. **Select components to configure**

   Select the component or components you want to configure on the Components Panel.

- **Delegated Administrator Utility (client)**—the command-line interface invoked with `commadmin`. This component is required and is selected by default. It cannot be deselected.
- **Delegated Administrator Server**—the Delegated Administrator server components required to run the Delegated Administrator console.
- **Delegated Administrator Console**—the Delegated Administrator graphical user interface (GUI).

Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

For more information about how to choose components, see "Choose Which Components to Configure" on page 59

If you choose not to configure the Delegated Administrator server, a dialog box cautions you that you must configure the Delegated Administrator Server on another machine. The server must be configured to enable the Delegated Administrator utility and console to work.

Configuring the Delegated Administrator Utility

You must configure the Delegated Administrator utility on all machines on which you install a Delegated Administrator component (server or console).

▼ To configure the Delegated Administrator Utility

Steps

1. **Access Manager host name and port number**

   Enter the Access Manager (formerly called Identity Server) host name and port number. If you are installing the Delegated Administrator server component, you must install it on the same host as Access Manager.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

2. **Default domain**

   Enter the default domain for the Top-Level administrator. This is the domain used when a domain is not explicitly specified by the `-n` option when executing the `commadmin` command-line utility. This is also known as the default organization. If the domain specified does not exist in the directory, it will be created.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

3. **Default SSL port for client**

   Enter the default SSL port that the Delegated Administrator utility uses.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

4. **If you chose to configure only the Delegated Administrator utility, go on to**
   "Completing the Configuration" on page 71

   If you chose to configure both the Delegated Administrator console and the server, or if you chose to configure the console only, go on to

   "Configuring the Delegated Administrator Console" on page 63

   If you chose to configure the Delegated Administrator server only (together with the required Delegated Administrator utility), go on to

   "Configuring the Delegated Administrator Server" on page 68

Configuring the Delegated Administrator Console

The configuration program now displays the following panel:

Select a Web Container for Delegated Administrator

Select the Web container on which you will deploy the Delegated Administrator console. You can configure Delegated Administrator on

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

This panel and the panels that follow gather information about the Web container for the Delegated Administrator console. Follow the instructions in the appropriate section:

- "Web Server Configuration" on page 64
- "Application Server 7.*x* Configuration" on page 65
- "Application Server 8.*x* Configuration" on page 67

You can deploy the Delegated Administrator console and server on two different Web containers, on two different instances of the Web container, or on the same Web container.

If you chose to configure both the Delegated Administrator console and Delegated Administrator server in Panel 3, a second series of panels will ask for Web container information for the server.

Thus, you will see the Web container configuration panels twice. Follow the appropriate instructions for deploying each of the Delegated Administrator components.

When you complete the Web container configuration panels:

- If you chose to configure both the Delegated Administrator console and the server, go on to

  "Configuring the Delegated Administrator Server" on page 68
- If you chose to configure the Delegated Administrator console only (together with the required Delegated Administrator utility), go on to

  "Completing the Configuration" on page 71

Web Server Configuration

If you are deploying the Delegated Administrator server or console on Web Server, follow the steps described in this section.

▼ To Configure Web Server

Steps

1. **Web Server Configuration Details**

   The panel text tells you if you are providing Web Server configuration information for the Delegated Administrator server or console.

   Enter the Web Server root directory. You can browse to select the directory.

   Enter the Web Server instance identifier. This is can be specified by a *host.domain* name such as `west.sesta.com`.

   Enter the virtual server identifier. This can be specified by a `https-`*host.domain* name such as `https-west.sesta.com`.

   For more information about the Web Server instance identifier and virtual server identifier, see the Web Server documentation.

   Files for the Web Server instance are stored in the `https-`*host*`.`*domain* directory under the Web Server installation directory, for example `/opt/SUNWwbsvr/https-west.sesta.com`.

   Enter the HTTP port number for the Web Server.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

   The configuration program checks if the values you specified are valid. If a directory or identifier is invalid or does not exist, a dialog box tells you to choose a new value.

   Next, the configuration program checks if a Web Server instance connection is alive. If not, a dialog box warns you that the configuration program could not connect to the specified instance and your configuration may not be completed. You can accept the specified values or choose new Web Server configuration values.

2. **Default Domain Separator**

   This panel appears only if you are configuring the Delegated Administrator console. The domain separator is needed to configure the console; this information is not related to the Web container.

   Enter the default domain separator to be used for authentication when the user logs on. For example: `@`.

   The domain separator value is contained in the `daconfig.properties` file. You can edit this property value after the configuration program runs. For more information, see Chapter 4.

3. **If you are configuring the Delegated Administrator console:**

   - If you chose to configure both the Delegated Administrator console and the server, go on to

     "Configuring the Delegated Administrator Server" on page 68
   - If you chose to configure the Delegated Administrator console only (together with the required Delegated Administrator utility), go on to

     "Completing the Configuration" on page 71

   If you are configuring the Delegated Administrator server:

   Go on to

   Step 3 in "Configuring the Delegated Administrator Server" on page 68.

Application Server 7.*x* Configuration

If you are deploying the Delegated Administrator server or console on Application Server 7.*x*, follow the steps described in this section.

▼ To configure Application Server 7.*x*

Steps

1. **Application Server 7.x Configuration Details**

   The panel text tells you if you are providing Application Server 7.*x* configuration information for the Delegated Administrator server or console.

   Enter the Application Server installation directory. By default, this directory is `/opt/SUNWappserver7`.

   Enter the Application Server domain directory. By default, this directory is `/var/opt/SUNWappserver7/domains/domain1`.

   Enter the Application Server document root directory. By default, this directory is`/var/opt/SUNWappserver7/domains/domain1/server1/docroot`.

You can browse to select any of these directories.

Enter the Application Server instance name. For example: `server1`.

Enter the Application Server virtual server identifier. For example: `server1`.

Enter the Application Server instance HTTP port number.

Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

The configuration program checks if the directories you specified are valid. If a directory is invalid or does not exist, a dialog box tells you to choose a new directory.

Next, the configuration program checks if an Application Server instance connection is alive. If not, a dialog box warns you that the configuration program could not connect to the specified instance and your configuration may not be completed. You can accept the specified values or choose new Application Server configuration values.

2. **Application Server 7.x: Administration Instance Details**

   Enter the Administration Server port number. For example: `4848`

   Enter the Administration Server administrator user ID. For example: `admin`

   Enter the administrator user password.

   If you are using a secure Administration Server instance, check the **Secure Administration Server Instance** box. If you are not, leave the box unchecked.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

3. **Default Domain Separator**

   This panel appears only if you are configuring the Delegated Administrator console. The domain separator is needed to configure the console; this information is not related to the Web container.

   Enter the default domain separator to be used for authentication when the user logs on. For example: `@`.

4. **If you are configuring the Delegated Administrator console:**

   - If you chose to configure both the Delegated Administrator console and the server, go on to

     "Configuring the Delegated Administrator Server" on page 68
   - If you chose to configure the Delegated Administrator console only (together with the required Delegated Administrator utility), go on to

     "Completing the Configuration" on page 71

   If you are configuring the Delegated Administrator server:

Go on to

Step 3 in "Configuring the Delegated Administrator Server" on page 68.

Application Server 8.*x* Configuration

If you are deploying the Delegated Administrator server or console on Application Server 8.*x*, follow the steps described in this section.

▼ To configure Application Server 8.*x*

Steps

1. **Application Server 8.x Configuration Details**

   The panel text tells you if you are providing Application Server 8.*x* configuration information for the Delegated Administrator server or console.

   Enter the Application Server installation directory. By default, this directory is `/opt/SUNWappserver/appserver`.

   Enter the Application Server domain directory. By default, this directory is `/var/opt/SUNWappserver/domains/domain1`.

   Enter the Application Server document root directory. By default, this directory is `/var/opt/SUNWappserver/domains/domain1/docroot`.

   You can browse to select any of these directories.

   Enter the Application Server target name. For example: `server`.

   Enter the Application Server virtual server identifier. For example: `server`.

   Enter the Application Server target HTTP port number.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

   The configuration program checks if the directories you specified are valid. If a directory is invalid or does not exist, a dialog box tells you to choose a new directory.

   Next, the configuration program checks if an Application Server target connection is alive. If not, a dialog box warns you that the configuration program could not connect to the specified target and your configuration may not be completed. You can accept the specified values or choose new Application Server configuration values.

2. **Application Server 8.x: Administration Instance Details**

   Enter the Administration Server port number. For example: `4849`

Enter the Administration Server administrator user ID. For example: `admin`

Enter the administrator user password.

If you are using a secure Administration Server instance, check the **Secure Administration Server Instance** box. If you are not, leave the box unchecked.

Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

3. **Default Domain Separator**

   This panel appears only if you are configuring the Delegated Administrator console. The domain separator is needed to configure the console; this information is not related to the Web container.

   Enter the default domain separator to be used for authentication when the user logs on. For example: `@`.

4. **If you are configuring the Delegated Administrator console:**

   - If you chose to configure both the Delegated Administrator console and the server, go on to

     "Configuring the Delegated Administrator Server" on page 68
   - If you chose to configure the Delegated Administrator console only (together with the required Delegated Administrator utility), go on to

     "Completing the Configuration" on page 71

   If you are configuring the Delegated Administrator server:

   Go on to

   Step 3 in "Configuring the Delegated Administrator Server" on page 68.

Configuring the Delegated Administrator Server

If you chose to configure the Delegated Administrator server, the configuration program displays the following panels.

▼ To configure Delegated Administrator Server

Steps

1. **Access Manager base directory**

   Enter the Access Manager Base Directory. The default directory is `/opt/SUNWam`.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

   The configuration program checks if a valid Access Manager base directory is specified. If not, a dialog box displays indicating that an existing Access Manager base directory must be selected.

2. **Next, a Web container Configuration Details panel appears.**

   If you chose to configure the console and server, this is the second time a Web container **Configuration Details** panel appears.

   The Delegated Administrator server is deployed to the same Web container as Access Manager. (You cannot choose a Web container for the Delegated Administrator server.)

   Follow the instructions in the appropriate section:

   - "Web Server Configuration" on page 64
   - "Application Server 7.*x* Configuration" on page 65
   - "Application Server 8.*x* Configuration" on page 67

3. **Directory (LDAP) Server**

   This panel asks for information about connecting to the LDAP Directory Server for the user/group suffix.

   Enter the User and Group Directory Server LDAP URL (**LdapURL**), Directory Manager (**Bind As**), and password in the text boxes.

   The Directory Manager has overall administrator privileges on the Directory Server and all Sun Java System servers that make use of the Directory Server (for example, Delegated Administrator) and has full administration access to all entries in the Directory Server. The default and recommended Distinguished Name (DN) is `cn=Directory Manager`.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

4. **Access Manager Top Level Administrator**

   Enter the user ID and password for the Access Manager Top-Level Administrator. The user ID and password are created when Access Manager is installed. The default user ID is `amadmin`.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

5. **Access Manager internal LDAP authentication password**

   Enter the password for the Access Manager Internal LDAP authentication user.

   The authentication user name is hard-coded as `amldapuser`. It is created by the Access Manager installer and is the Bind DN user for the LDAP service.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

6. **Organization Distinguished Name (DN)**

   Enter the Organization DN for the default domain. For example, if your organization DN is `o=siroe.com`, all the users in that organization will be placed under the LDAP DN `o=siroe.com, o=usergroup`, where `o=usergroup` is your root suffix.

By default, the configuration program adds the default domain under the root suffix in the LDAP directory.

If you want to create the default domain at the root suffix (not underneath it), delete the organization name from the DN that appears in the **Organization Distinguished Name (DN)** text box.

For example, if your organization DN is `o=siroe.com` and your root suffix is `o=usergroup`, delete `"o=siroe.com"` from the DN in the text box; leave only `o=usergroup`.

If you choose to create the default domain at the root suffix, and if you later decide to use hosted domains, it can be difficult to migrate to the hosted-domain configuration. The `config-commda` program displays the following warning:

"The Organization DN you chose is the User/Group Suffix. Although this is a valid choice, if you ever decide to use hosted domains, there will be difficult migration issues. If you do wish to use hosted domains, then specify a DN one level below the User/Group suffix."

For more information, see "Directory Structure Supporting a One-Tiered Hierarchy" on page 26.

Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

7. **Top-Level Administrator for the default organization**

   Enter the user ID and password for the Top-Level Administrator that is to be created in the default domain (organization).

   A **Confirm Password**field asks you to enter the password a second time.

   Click **`Next`** to continue, **`Back`** to return to the previous panel, or **`Cancel`** to exit.

8. **Service Package and Organization Samples**

   You can choose to add sample service packages and sample organizations to your LDAP directory.

   Load sample service packages. Select this option if you want to use or modify sample service package templates to create your own Class-of-Service packages.

   Load sample organizations. Select this option if you want your LDAP directory tree to contain sample provider organization nodes and subordinate organization nodes.

   You can select

   - Both the sample service packages and the sample organizations
   - Only one of these options
   - Neither option

   Preferred Mailhost for Sample. Enter the name of the machine on which Messaging Server is installed.

For example: `mymachine.siroe.com`

If you chose to load the sample organizations into your LDAP directory, you must enter a preferred mail host name for these samples.

For information about service packages and organizations, see Chapter 2: "Delegated Administrator Overview."

After you run the configuration program, you must modify the service package templates to create your own Class-of-Service packages. For information about this post-configuration task, see "Create Service Packages" on page 76.

Completing the Configuration

Take the steps described in this section to finish running the configuration program.

▼ To complete the configuration

Steps

1. **Ready to Configure**

   The verification panel displays the items that will be configured.

   Click **`Configure Now`** to begin the configuration, **`Back`** to return to any previous panel to change information, or **`Cancel`** to exit.

2. **Task Sequence**

   A sequence of tasks being performed is displayed on the Task Sequence Panel. This is when the actual configuration takes place.

   When the panel displays "All Tasks Passed" you can click **`Next`** to continue or **`Cancel`** stop the tasks from being performed and exit.

   A dialog box appears reminding you to restart the Web container in order for configuration changes to take effect.

3. **Installation Summary**

   The Installation Summary panel displays the product installed and a **`Details...`** button that displays more information about this configuration.

   A log file for the `config-commda` program is created in the `/opt/SUNWcomm/install` directory. The name of the log file is `commda-config_`*YYYYMMDDHHMMSS*`.log`, where *YYYYMMDDHHMMSS* identifies the 4-digit year, month, date, hour, minute, and second of the configuration.

   Click **`Close`** to complete the configuration.

Restarting the Web Container

After you complete the Delegated Administrator configuration, you must restart the Web container to which Delegated Administrator is deployed (one of the following):

- Web Server
- Application Server 7.x
- Application Server 8.x

Configuration and Log Files Created by the `config-commda` Program

Configuration Files

Using the information you provided in the panels, the `config-commda` program creates the following configuration files for the three Delegated Administrator components:

- Delegated Administrator utility:

  Configuration file name: `cli-usrprefs.properties`

  Default location: `/var/opt/SUNWcomm/config`
- Delegated Administrator server:

  Configuration file name: `resource.properties`

  Default location:

  `/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet`

  or

  `/var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet`
- Delegated Administrator console:

  Configuration file name: `daconfig.properties`

  Default location:

  `/opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources`

  or

  `/var/opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources`

For information about these files, the properties they contain, and how to edit these properties to customize your configuration, see Chapter 4.

Log Files

The Delegated Administrator console creates a runtime log file:

Default log file name: `da.log`

Default location: `/opt/SUNWcomm/log`

For more information about this and other Delegated Administrator log files, see Appendix C.

Perform Silent Installation

The Delegated Administrator utility initial runtime configuration program automatically creates a silent installation state file (called `saveState`). This file contains internal information about the configuration program, and is used for running silent installs.

The silent installation `saveState` file is stored in the `/opt/SUNWcomm/data/setup/commda-config_`*YYYYMMDDHHMMSS*`/` directory, where *YYYYMMDDHHMMSS* identifies the 4-digit year, month, date, hour, minute, and second of the `saveState` file.

For example, once you have run the `config-commda` program once, you can run it in silent install mode:

```
da_base/sbin/config-commda -nodisplay -noconsole -state
 fullpath/saveState
```

The *fullpath* variable is the full directory path of where the `saveState` file is located.

Run Delegated Administrator Console and Utility

Launching the Console

The Delegated Administrator console is launched by accessing the Web container to which it is deployed.

▼ To launch the Delegated Administrator console

Steps

1. **Go to the following url:**

   `http://`*host*`:`*port*`/da/DA/Login`

   where

   host is the Web container host machine

   port is the Web container port

   For example:

   `http://siroe.com:8080/da/DA/Login`

   The Delegated Administrator console log-in window appears.

2. **Log in to the Delegated Administrator console.**

   You could use the Top-Level Administrator (TLA) user ID and password specified in the Delegated Administrator configuration program. This information was requested in the following panel:

   Top-Level Administrator for the default organization

Note – Values set in Access Manager can determine session time-outs when you are running the Delegated Administrator console. For information on the session time-out values, see "Session Service Attributes," in the *Sun Java System Access Manager Administration Guide*. For information on viewing these values in the Access Manager console, see "Current Sessions" in the *Sun Java System Access Manager Administration Guide*.

Running the Command-Line Utility

You can run the Delegated Administrator utility by entering the command name, `commadmin`, from a terminal window.

▼ To run the command-line utility

Steps

1. **Go to the** *da_base*`/bin/` **directory. For example, go to** `/opt/SUNWcomm/bin/`**.**

2. **Enter the** `commadmin` **command.**

Example 3–1 Using `commadmin` to search for users

The following command searches for users in the `varrius.com` domain:

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

For details about this `commadmin` command, see "commadmin user search" on page 137.

More Information `commadmin` Return Codes

Tip – When a `commadmin` operation success, an OK message is displayed on the command line.

If a failure occurs, the following message appears:

```
FAIL
```

<*message*>

Where <*message*> displays the error text.

Post-Configuration Tasks

After you run the Delegated Administrator configuration program, you should perform the following tasks:

- "Add Mail and Calendar Services to the Default Domain" on page 75
- "Create Service Packages" on page 76

Perform the following task only if you are using an LDAP directory in Schema 2 compatibility mode:

- "Add ACIs for Schema 2 Compatibility Mode" on page 81

Add Mail and Calendar Services to the Default Domain

The `config-commda` program creates a default domain.

If you want to create users with mail service or calendar service in the default domain, you first must add mail service and calendar service to the domain.

To perform this task, use the `commadmin domain modify` command with the `-S mail` and `-S cal` options.

The following example shows how you can use `commadmin domain modify` to add mail and calendar services to the default domain:

```
commadmin domain modify -D chris -w bolton -n sesta.com -d siroe.com
 -S mail,cal -H test.siroe.com
```

For `commadmin` command syntax and details, see Chapter 5.

Create Service Packages

Each user and group provisioned in the LDAP directory with Delegated Administrator should have a service package. A user or group can have more than one service package.

Predefined Class-of-Service Templates

When you run the Delegated Administrator configuration program (`config-commda`), you can choose to have the `config-commda` program install sample Class-of-Service templates in the directory.

For information about the sample Class-of-Service templates and the available mail attributes in a service package, see "Service Packages" on page 31 in Chapter 1.

You can use the sample Class-of-Service templates to create and assign service packages. However, the sample templates are meant to be examples.

Creating Your Own Service Packages

Most likely you will want to create your own service packages based on customized Class-of-Service templates with attribute values appropriate for the users and groups in your installation.

To create your own service packages, use the Class-of-Service templates stored in the `da.cos.skeleton.ldif` file.

This file was created specifically for use as a template for writing customized Class-of-Service templates. It is not installed in the LDAP directory when Delegated Administrator is configured.

The `da.cos.skeleton.ldif` file contains four parameterized templates, one for each Class-of-Service definition provided by Delegated Administrator:

- `standardUserMail`

- standardUserCalendar
- standardUserMailCalendar
- standardGroupMail

You can create your own Class-of-Service templates by using one or more of the parameterized templates in the `da.cos.skeleton.ldif` file.

The Class-of-Service templates in the `da.cos.skeleton.ldif` file are as follows:

```
# Templates for creating COS templates for service packages.
#
# There are four COS definitions :
#   standardUserMail
#   standardUserCalendar
#   standardUserMailCalendar
#   standardGroupMail
#
# Each definition can have zero or more COS templates which
# define specific values for the attributes listed in the
# COS definition.
#
# Each COS definition points to a corresponding subdirectory
# in which COS templates for that definition (and no other
# definition) are found.  The templates directory structure
# is as follows:
# standardUserMail          => o=mailuser,o=costemplates,<ugldapbasedn>
# standardUserCalendar      => o=calendaruser,o=costemplates,
#                                <ugldapbasedn>
# standardUserMailCalendar  => o=mailcalendaruser,o=costemplates,
#                                <ugldapbasedn>
# standardGroupMail          => o=mailgroup,o=costemplates,
#                                <ugldapbasedn>
#
# Thus, all COS templates for the user mail service are found in the
# o=mailuser,o=costemplates,<ugldapbasedn> directory, etc.
#
# It is not necessary to have any templates for a given definition.
# In that case default values are assumed for those attributes defined
# in the COS definition.
#
# If a template is created for a definition there should be at least
# one attribute with a defined value.
#
# Consult documentation for values for the attributes.
# Documentation includes units and default values.
#
# The finished COS derived from this skeleton is added to the
# directory with the following command:
#
# ldapmodify -D <directory manager> -w <password>
# -f <cos.finished.template.ldif>
#
#
################################################################
#
```

```
#    standardMailUser COS template
#
################################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailuser,o=cosTemplates,<rootSuffix>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailQuota: <ma:ilQuotaValue>
mailMsgQuota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
#
#
################################################################
#
#    standardCalendarUser COS template
#
################################################################
# There must be a least one of the following attributes:
# - icsPreferredHost
# - icsDWPHost
# - icsFirstDay
#
dn: cn=<service package name>,o=calendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
icsPreferredHost: <preferredHostValue>
icsDWPHost: <dwpHostValue>
icsFirstDay: <firstDayValue>
daServiceType: calendar user
#
#
################################################################
#
#    standardMailCalendarUser COS template
#
################################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
```

```
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailcalendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailquota: <mailQuotaValue>
mailmsgquota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
daServiceType: calendar user
daServiceType: mail user
#
#
###############################################################
#
#    standardMailGroup COS template
#
###############################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
#
#
dn: cn=<service package name>,o=mailgroup,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
daServiceType: mail group
```

▼ To create your own service packages

Steps

1. **Copy and rename one of the parameterized templates in the `da.cos.skeleton.ldif` file.**

   When you install Delegated Administrator, the `da.cos.skeleton.ldif` file is installed in the following directory:

   da_base`/lib/config-templates`

   Choose one of these templates in the `da.cos.skeleton.ldif` file to copy and rename:

   ```
   standardUserMail
   standardUserCalendar
   ```

```
standardUserMailCalendar
standardGroupMail
```

2. **Edit the following parameters in your copy of the template:**

   - `<ugldapbasedn>`

     Change the root suffix parameter,`<rootSuffix>`, to your root suffix (such as `o=usergroup`).

     The `<ugldapbasedn>` parameter appears in the DN.

   - `<service package name>`

     Change the `<service package name>` parameter to your own service package name.

     The `<service package name>` parameter appears in the DN and the `cn`.

   - Mail attribute values:

     ```
     <mailMsgMaxBlocksValue>
     <mailQuotaValue>
     <mailMsgQuotaValue>
     <mailAllowedServiceAccessValue>
     ```

     Edit these values to your specifications.

     For example, you could enter the following values for the mail attributes:

     ```
     mailMsgMaxBlocks: 400
     mailQuota: 400000000
     mailMsgQuota: 5000
     mailAllowedServiceAccess: imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
     ```

   - Calendar attribute values:

     ```
     <preferredHostValue>
     <dwpHostValue>
     <firstDayValue>
     ```

     These parameters represent values for the `icsPreferredHost`, `icsDWPHost`, and `icsFirstDay` LDAP attributes.

     Edit these values to your specifications.

   For definitions and descriptions of these attributes, see "Chapter 3: Messaging Server and Calendar Server Attributes" in the *Sun Java System Communications Services Schema Reference*.

   You must use at least one attribute in a customized Class-of-Service template. You do not have to use all four mail attributes in a custom template. You can delete one or more attributes from the service package.

3. **Use the LDAP directory tool `ldapmodify` to install the service package in the directory.**

   For example, you could run the following command:

```
ldapmodify -D <directory manager> -w <password> -f
<cos.finished.template.ldif>
```

where

<directory manager> is the name of the Directory Server administrator.

<password> is the password of the Directory Service administrator.

<cos.finished.template.ldif> is the name of the edited ldif file to be installed as a service package in the directory.

Add ACIs for Schema 2 Compatibility Mode

If you are using an LDAP directory in Schema 2 compatibility mode, you must manually add ACIs to the directory to enable Delegated Administrator to provision in your directory. Take the following steps:

▼ To add ACIs for Schema 2 compatibility mode

Steps 1. **Add the following two ACIs to the OSI root. You can find the following two ACIs in the `usergroup.ldif` file, located in the `/opt/SUNWcomm/config` directory.**

Be sure to replace ugldapbasedn with your usergroup suffix. Add the edited usergroup.ldif into the LDAP directory.

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <local.ugldapbasedn>
########################################
dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read
to org node";
allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

2. **Add the following two ACIs to the DC Tree root suffix. You can find the following two ACIs in the `dctree.ldif` file, located in the `/opt/SUNWcomm/config` directory.**

   Be sure to replace *dctreebasedn* with your DC Tree root suffix and *ugldapbasedn* with your usergroup suffix. Add the edited `dctree.ldif` into the LDAP directory.

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <dctreebasedn>
########################################
dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to dc node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to dc
node"; allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

3. **Add the following additional ACIs to the DC Tree root suffix. (These ACIs are not in the `dctree.ldif` file.)**

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Proxy user rights"; allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix"; allow (all) userdn ="ldap:///cn=dsameuser,ou=DSAME
Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all) roledn = "ldap:///cn=Top-level Admin
Role,<ugldapbasedn>";)
```

4. **Set the `com.iplanet.am.domaincomponent` property in the `AMConfig.properties` file to your DC Tree root suffix.**

   For example, modify the following lines in the *<AM_base_directory>*`/lib/AMConfig.properties` file:

   from

   ```
   com.iplanet.am.domaincomponent=o=isp
   ```

   to

   ```
   com.iplanet.am.domaincomponent=o=internet
   ```

5. **Enable Access Manager (formerly called Identity Server) to use compatibility mode.**

   In the Access Manager Console, in the Administration Console Service page, check (enable) the **Domain Component Tree Enabled** check box.

6. **Add the `inetdomain` object class to all the DC Tree nodes (such as `dc=com,o=internet`), as in following example:**

   ```
   /var/mps/serverroot/shared/bin 298% ./ldapmodify
   -D "cn=Directory Manager" -w password
   dn: dc=com,o=internet
   changetype: modify
   add: objectclass
   objectclass: inetdomain
   ```

7. **Restart the Web container.**

CHAPTER 4

Customizing Delegated Administrator

After you have installed and configured Delegated Administrator with the configuration program (`config-commda`), you can customize your configuration to meet your particular needs. This chapter offers examples of how to customize certain Delegated Administrator features.

You should back up any existing Delegated Administrator configuration file before you begin customizing it.

Also, customized configuration data can be lost when you upgrade Delegated Administrator. Therefore, you should preserve your customized configuration before you upgrade Delegated Administrator or rerun the Delegated Administrator configuration program. For more information, see "Preserve an Existing Configuration" on page 56.

This chapter describes the following topics:

Configuring the Preferred Mail Host Using the Service-Wide Default

If you want the Preferred Mail Host and Preferred Mail Store to be set using the server-wide default, you can perform the tasks described in this section.

If you need to remove the Preferred Mail Host field from the Console (specifically, from the New Organization Wizard and Organization Properties screens), you can should take the following steps:

- Edit the `Security.properties` file. This step is described in this section.
- Enable the MailHostStorePlugin. This step is described in the following section, "Adding Plug-ins for Delegated Administrator" on page 87.

The `Security.properties` file lets you customize the Delegated Administrator Console for all or for individual roles.

The `Security.properties` file is located in the directory *da_base*`/da/WEB-INF/classes/com/sun/comm/da/resources`

To remove the Preferred Mail Host from the Console, add the lines shown below to the `Security.properties` file:

```
# Remove Preferred Mail Host from UI
*.NewOrganizationPage6.PreferredMailHostProperty=INVISIBLE
*.NewOrganizationSummaryPage.PreferredMailHostSummaryProperty=INVISIBLE
*.OrgProperties.MailHostName=INVISIBLE
*.OrgProperties.MailHostNameText=INVISIBLE
*.OrgProperties.MailHostValue=INVISIBLE
```

CAUTION: You may add lines to this file for your own customization, but do not edit the lines already present. Editing existing lines could result in exceptions being thrown on the Console.

The properties in the file are of the form: *Security Element Name=Permission*

A Security Element Name is of the form:*Role Name*.*Container View Name*.*Console Element Name*

A Security Element specifies the Console element and role for which the permission is being defined. If you do not know an element name, view the source of a page to match the name on the page to the Console element you are interested in.

The names on the page are fully qualified names. You need to pick up only the last two elements of the name, which form *Container View Name*.*Console Element Name*.

Valid role names for Delegated Administrator are as follows:

"ProviderAdminRole" (SPA) For information about this role, see Appendix A.

"OrganizationAdminRole" (OA)

"Top-levelAdminRole" (TLA)

"*" (applies a permission to all roles unless it is overridden for a specific role)

A permission must be one of the following strings:

- EDITABLE– indicates that the security element is editable.

- NONEDITABLE– indicates that the security element is read-only.
- VISIBLE– indicates that the security element is visible and read-only.
- INVISIBLE– indicates that the security element is invisible.

Adding Plug-ins for Delegated Administrator

You can customize Delegated Administrator to support the following plug-ins:

- `MailHostStorePlugin`

  By default, this plug-in is disabled. If no `preferredmailhost` is supplied when a business organization is created, an exception will be raised. If the plug-in is enabled, values from the flat file (described later in this section) will be used only if the corresponding attribute is absent.

- `MailDomainReportAddressPlugin`

  Uses the domain value to return the desired DSN address. The default implementation is to return the string `MAILER-DAEMON@<`*domain*`>`.

- `UidPlugin`

  Generates a unique id string. The default implementation generates a GUID to return to the caller.

Enabling the Plug-Ins

To enable these plug-ins, edit the `commcli servlet resource.properties` file, located in the following directory:

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

(By default, *da_base* is `/opt/SUNWcomm`.)

The plug-ins are located in the `resource.properties` file in a section headed as follows:

```
########################
# Plugin Configuration #
########################
```

```
Each has "plugin" as the suffix. The current list looks like:
```

```
jdapi-mailhoststoreplugin=disabled

jdapi-mailhoststorepluginclass=sun.comm.cli.server.util.MailHostStorePlugin
```

```
jdapi-mailhoststorepluginfile=/tmp/mailhostmailstore
jdapi-maildomainreportaddressplugin=enabled
jdapi-maildomainreportaddresspluginclass=sun.comm.cli.server.
  util.MailDomainReportAddressPlugin
jdapi-uidautogenerationplugin=disabled
jdapi-uidautogenerationpluginclass=sun.comm.cli.server.util.UidPlugin
```

Plug-In Format

Each plug-in has at least two lines, which take the following form:

- `jdapi-<`*name*`>plugin= "enabled" | "disabled"`
- `jdapi-<`*name*`>pluginclass=sun.comm.cli.server.util/`
  `<`*java class name*`>`

To enable a plug-in, change "`disabled`" to "`enabled`".

Plug-in classes are supplied for all the plug-ins listed in this section. The classes are located in the following directory:

da_base`/data/WEB-INF/classes/sun/comm/cli/server/util`

You do not need to do anything with these classes.

Additional Flat File Required for `MailHostStorePlugin`

The `MailHostStorePlugin` requires a flat file, which is included in a third line for the plug-in. The plug-in reads the value in the flat file and uses it to set attribute values. If the plug-in is enabled, the file must be present, or an error will occur.

- ```
  jdapi-mailhoststoreplugin
      o jdapi-mailhoststorepluginin=<full file name>
      o file has one line
      o value is that for :
          o preferredmailhost attribute
          o preferredmailmessagestore attribute
      o form
          o <mailhost>:<mailpartition>
  ```
  ```

Adding a Custom Object Class When You Create an LDAP Object

You can enable Delegated Administrator to add a custom object class to the LDAP entry of a new user, group, resource, or organization. To accomplish this task, you customize the appropriate object-creation template installed in the directory by Access Manager.

For example, the BasicUser creation template determines which object classes and attributes are added to a user entry when you create a new user. You can update the BasicUser creation template with your custom object class. Thereafter, the custom object class will be added to each new user entry together with the standard object classes.

The following procedure describes how to customize the BasicUser template. You can follow the same procedure to customize the BasicGroup, BasicResource, and BasicOrganization creation templates.

▼ To add a custom object class to the user-creation process

Steps

1. **Make sure your custom object class is defined in the directory schema.**
2. **Locate the following directory entry:**

   ```
   ou=basicuser,ou=creationtemplates,ou=templates,ou=default,
   ou=globalconfig,ou=1.0,ou=dai,ou=services,
   o=$Root_Suffix
   ```

   where *$Root_Suffix* is the root suffix of your directory.
3. **Add the following *attribute:value* to the entry:**

   ```
   sunkeyValue:required=objectClass=$Your_Custom_Objectclass.
   ```

   where *$Your_Custom_Objectclass* is your custom object class.

Customizing the User Log-In

When you run the Delegated Administrator configure program (`config-commda`), the value you use to log in to Delegated Administrator is set to be a `uid`.

For example, if you intend to log in as the TLA, and the TLA's `uid` is `john.doe`, you would use `john.doe` to log in to Delegated Administrator.

You can customize Delegated Administrator to enable you to use additional values for the user log-in. For example, you could add the mail address (`mail`).

How the User Log-In Value Is Set

The `config-commda` program sets this value to `uid` with the loginAuth-idAttr property in the `resource.properties` file, as shown in the following example:

```
loginAuth-searchBase=<$rootSuffix>
         servicepackage-cosdefbasedn = <$rootSuffix>
          loginAuth-idAttr-1=uid
```

where <*$rootSuffix*> is the root suffix in your directory.

The `resource.properties` file is located in

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

Adding a User Log-In Value

You can set additional values for the user log-in by editing the `resource.properties` file.

For example, to enable you to use a mail address (such as `john.doe@sesta.com`) to log in, you could add the following line to the `resource.properties` file:

```
loginAuth-searchBase=<$rootSuffix>
         servicepackage-cosdefbasedn = <$rootSuffix>
          loginAuth-idAttr-1=uid
          loginAuth-idAttr-2=mail
```

where <*$rootSuffix*> is the root suffix in your directory.

Note that you must add an increment to the `loginAuth-idAttr` property for each new value. In this example, a second value is added, so you add `-2` to `loginAuth-idAttr`.

You can add multiple instances of the `loginAuth-idAttr` property:

```
loginAuth-idAttr-1=uid
  loginAuth-idAttr-2=mail
  |
  loginAuth-idAttr-n=<login-in value>
```

Requiring Service Packages for New Users

By default, Delegated Administrator lets you create a new user without assigning a service package to the user.

You can change the default setting so that all new users must have at least one service package assigned to them.

▼ To require new users to have a service package assigned to them

Steps

1. **Open the `daconfig.properties` file in a text editor.**

   The `daconfig.properties` file is located by default in the following directory:

   ```
   /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/
   comm/da/resources/daconfig.properties
   ```

2. **Change the value of the `user.atleastOneServicePackage` property from `false` to `true`.**

   By default, this value is `false`.

   For example:

   ```
   user.atleastOneServicePackage=true
   ```

   After you set this value to `true`, when you use the Create New User wizard in the Delegated Administrator console, you must assign at least one service package to successfully create the new user.

Adding a New Calendar Time Zone

You can customize Delegated Administrator by adding a new Calendar Server time zone. Delegated Administrator can then provision organizations, users, groups, and resources with the new time zone.

Once the time zone has been added, you can set it as the default time zone for newly created users.

▼ To add a new time zone in Delegated Administrator

Steps

1. **Add the time zone in Calendar Server.**

   To accomplish this step, you must edit the `timezones.ics` file and other Calendar Server files. For instructions, see "Adding a New Time Zone" in the chapter, "Managing Calendar Server Time Zones" in the *Sun Java System Calendar Server Administration Guide*.

2. **Back up the `UserCalendarService.xml` and `DomainCalendarService.xml`, and `Resources.properties` files.**

   The xml files are located by default in the following directory:

   ```
   /opt/SUNWcomm/lib/services
   ```

   The `Resources.properties` file is located by default in the following directory:

   ```
   /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
   comm/da/resources
   ```

   Also be sure to preserve your customized configuration data before you upgrade Delegated Administrator or rerun the Delegated Administrator configuration program.

3. **Edit the `UserCalendarService.xml` and `DomainCalendarService.xml` files to add the new time zone in Delegated Administrator.**

   These xml files are located by default in the following directory:

   ```
   /opt/SUNWcomm/lib/services
   ```

   - In both the `UserCalendarService.xml` and `DomainCalendarService.xml` files, find the following entry heading:

     ```
     <AttributeSchema name="icstimezone"
                                type="single choice"
                                syntax="string"
     ```

```
                                    any="optional|adminDisplay">
                                    <ChoiceValues>
```

- Add the new time zone value to the list of `<ChoiceValues>`.

4. **Run the Access Manager `amadmin` utility to delete the current service and add the updated service.**

   For both the `UserCalendarService.xml` and `DomainCalendarService.xml` files, run the following `amadmin`commands:

```
./amadmin -u <admin> -w <password> -r DomainCalendarService
./amadmin -u <admin> -w <password> -s $PATH/DomainCalendarService.xml
```

Note – If you also intend to make the new time zone your default, you can run these `amadmin` commands after you have performed both tasks. (The following task describes how to change the default time zone.)

---

5. **Restart your Web container to enable the changes to take effect.**

▼ To change the default time zone in Delegated Administrator

Steps

1. **In the `UserCalendarService.xml` and `DomainCalendarService.xml` files, edit the following value:**

```
<DefaultValues>
                <Value>America/Denver</Value>
</DefaultValues>
```

   You can find `<DefaultValues>` under the following entry in the xml files:

```
<AttributeSchema name="icstimezone"
```

2. **Run the Access Manager `amadmin` utility to delete the current service and add the updated service.**

   For both the `UserCalendarService.xml` and `DomainCalendarService.xml` files, run the following `amadmin`commands:

```
./amadmin -u <admin> -w <password> -r DomainCalendarService
./amadmin -u <admin> -w <password> -s $PATH/DomainCalendarService.xml
```

3. **Restart your Web container to enable the changes to take effect.**

▼ To add the new time zone to Delegated Administrator console

Step ● **Edit the `Resources.properties` file, located under your Delegated Administrator data directory.**

The `Resources.properties` file is located by default in the following directory:

```
/var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
comm/da/resources
```

To edit `Resources.properties`, search for the `rsrc.Timezone` property and add the new time zone to the appropriate list.

After you edit this file, the new time zone will appear in the appropriate list boxes in the Delegated Administrator console.

CHAPTER 5

Command Line Utilities

The Delegated Administrator command-line utilities enable the administrators to manage different communication services for users, groups, domains, and organizations. The command line tool set used to perform bulk operations such as create, modify, delete, and search on users, groups, domains, and organizations are discussed in this chapter.

Commands

The commands are listed in the table shown below. The table consists of three columns; the first column lists the command, the second the description of the command, and the third lists the type of administrators permitted to execute the command.

The `commadmin` utility is located in the `/opt/SUNWcomm/bin` directory.

TABLE 5–1 Delegated Administrator Command Line Interfaces

Command	Description	Permission to Execute*
"commadmin admin add" on page 99	Grants Organization Administrator privileges to a user	Top-level Administrator
"commadmin admin remove" on page 101	Revokes Organization Administrator privileges from a user	Top-level Administrator

TABLE 5–1 Delegated Administrator Command Line Interfaces *(Continued)*

Command	Description	Permission to Execute*
"commadmin admin search" on page 102	Searches and displays users who have Organization Administrator privileges	Top-level Administrator, Organization Administrator
"commadmin domain create" on page 103	Creates a domain	Top-level Administrator
"commadmin domain delete" on page 106	Deletes a domain	Top-level Administrator
"commadmin domain modify" on page 107	Modifies a domain	Top-level Administrator
"commadmin domain purge" on page 110	Purges a domain	Top-level Administrator
"commadmin domain search" on page 112	Searches for a domain	Top-level Administrator
"commadmin group create" on page 113	Creates a group	Top-level Administrator, Organization Administrator and Mail list owner
"commadmin group delete" on page 116	Deletes a group	Top-level Administrator, Organization Administrator and Mail list owner
"commadmin group modify" on page 117	Modifies a group	Top-level Administrator, Organization Administrator and Mail list owner
"commadmin group search" on page 120	Searches for a group	Anyone
"commadmin resource create" on page 122	Creates a resource	Top-level Administrator, Organization Administrator
"commadmin resource modify" on page 126	Modifies a resource	Top-level Administrator, Organization Administrator
"commadmin resource delete" on page 124	Deletes a resource	Top-level Administrator, Organization Administrator
"commadmin resource search" on page 128	Searches for a resource	Anyone

TABLE 5–1 Delegated Administrator Command Line Interfaces *(Continued)*

Command	Description	Permission to Execute*
"commadmin user create" on page 129	Creates a user	Top-level Administrator, Organization Administrator
"commadmin user delete" on page 132	Deletes a user	Top-level Administrator, Organization Administrator
"commadmin user search" on page 137	Searches for a user	Anyone
"commadmin user modify" on page 134	Modifies a user	Top-level Administrator, Organization Administrator
*This release of Delegated Administrator does not support the Service Provider Administrator's use of the `commadmin` utility.		

Execution Modes

The command line execution has three possible modes:

- Execute with options specified in a file

  `commadmin` *object task* `-i` *inputfile*

  Analyzes *inputfile* and executes it.
- Interactive

  `commadmin` *object task*

  The administrator is queried for the remainder of the options and attributes.
- Immediate or shell execution

  `commadmin` *object task* [*options*]

When a `commadmin` operation succeeds, an OK message is displayed on the command line.

If a failure occurs, the following message appears:

`FAIL`

<*message*>

Where <*message*> displays the error text.

Command File Format

The options can be specified within a file, using the `-i` option.

Within the file, option names are separated from option values by white space. The option value begins with the first non-white space character and extends to the end-of-line character. Option sets are separated by blank lines.

The general syntax is:

```
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
<blank line>
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
```

The option value given in the command line becomes the default for each option set. Alternatively, these options can be specified for each option set. The value then overrides any default specified on the command line.

Following is an example of the format and syntax for the file specified by the `-i` option for the `commadmin user add` command.

```
l newuser1
F new
L user1
W secret

l newuser2
F new
L user2
W secret

l newuser3
F new
L user3
W secret

<and so forth...>
```

Command Descriptions

This section provides descriptions, syntax, and examples of the command line tools.

Mandatory commadmin Options

The following are the mandatory options used for authenticating the administrator or the user.

Options	Description
`-D` *userid*	User ID used to bind to the directory.
`-w` *password*	Password used to authenticate the userID to the directory. You may also specify *password* via a text file, *password* `.txt`.
`-n` *domain*	The domain the administrator belongs to.

The Access Manager Host (`-X`), Access Manager Port (`-p`), and the default domain (`-n`) values are specified during installation and stored in the `cli-userprefs.properties` file.

Note – If the `-X`, `-p` and `-n` options are not specified at the time when an `commadmin` command is executed, their values are taken from the `cli-userprefs.properties` file.

---

commadmin admin add

The `commadmin admin add` command grants the Organization Administrators privileges to a user for a particular domain. Only a top-level administrator or an ISP administrator can execute this command.

Syntax

```
commadmin admin add -D login -l login -n domain -w password -d domain
    [-h] [-i inputfile] [-p AM port] [-X AM host] [-?] [-s] [-v] [-V]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the top-level administrator.
`-l` *login*	The user ID of the user to whom you want to grant organization administrative privileges. The user should be present in the directory and be a part of the domain specified by the `-d` option.
`-n` *domain*	The domain of the top-level administrator. If not specified, default domain stored in the `cli-userprefs.properties` file is used.
`-w` *password*	The password of the top-level administrator.
`-d` *domain*	The domain to which you want to grant administrative privileges. If not specified, the domain specified by the `-n` option is used.

The following options are non-mandatory:

Options	Description
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Use this option to specify an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-X` *AM host*	Specify the host on which the Access Manager is running. If not specified, the default *AM host* is used
`-h`, `-?`	Prints command usage syntax.
`-V`	Prints information about the utility and its version.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.

Examples

The following grants Organization Administrator privileges to the user with the user ID `admin1`.

```
commadmin admin add -D chris -n sesta.com -w bolton -l admin1 \
-d florizel.com
```

The following grants Organization Administrator privileges to the user with the user ID `admin2` for the domain `florizel.com`.

```
commadmin add admin -D chris -w bolton -l admin2 -n varrius.com \
-d florizel.com
```

commadmin admin remove

The `commadmin admin remove` command removes the Organization Administrator privileges from an existing Organization Administrator. Only a Top-Level Administrator can execute this command.

To remove Organization Administrator privileges from multiple users, use the `-i` option.

Syntax

```
commadmin admin remove -D login -l login -n domain -w password
   -d domain name [-h] [-?] [-i inputfile] [-p AM port] [-X AM host]
   [-s] [-v] [-V]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the top-level administrator.
`-l` *login*	The user ID of the user whose administrator privileges need to be revoked.
`-n` *domain*	The domain of the top-level administrator.
`-w` *password*	The password of the top-level administrator.
-d *domain name*	The domain to which administrator privileges are revoked. If `-d` is not specified, the domain specified by `-n` is used.

The following options are non-mandatory:

Option	Description
`-h, -?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Use this option to specify an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-X` *AM host*	Specify the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.

Example

The following command removes Organization Administrator privileges from the administrator with user ID `admin5`:

```
commadmin admin remove -D chris -n sesta.com -w bolton -l admin5 -d test.com
```

commadmin admin search

The `commadmin admin search` command searches and displays a specific or all Organization Administrators of a domain.

Syntax

`commadmin admin search -D` *login* `-n` *domain* `-w` *password* `[-l` *login*`] [-d` *domain*`]`

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	The domain of the user specified with the `-D` option.
`-w` *password*	The password of the user specified with the `-D` option.

The following options are non-mandatory:

Option	Description
`-l` *login*	The user ID of the Organization Administrator searched for. If `-l` is not specified or `-l` is specified with the wildcard operator (`-l\\*` or `-l '*'`) all Organization Administrators of the domain are displayed.
`-d` *domain*	Searches for users who have Organization Administrator privileges for the specified domain. If `-d` is not specified, the domain specified by `-n` is used.

Example

To search for all Organization Administrators of the `test.com` domain:

```
commadmin admin search -D chris -n sesta.com -w bolton -d test.com
```

commadmin domain create

The `commadmin domain create` command creates a single domain on the Access Manager. To create multiple domains, use the `-i` option.

Syntax

```
commadmin domain create -D login -d domain name -n domain -w password
    [-A [+] attributename:value] [-h] [-?] [-i inputfile] [-o organization RDN]
    [-p AM port] [-s] [-v] [-V] [-X AM host]
    [-S mail -H preferred maillhost]
    [-S cal [-B backend calendar data server] [-C searchable domains] [-g access control string]
    [-P propertyname[:value]] [-R right[:value]] [-T calendar time zone string]]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the top-level administrator.
`-d` *domain name*	DNS domain name of the domain that is being created.
`-n` *domain*	The domain of the top-level administrator.
`-w` *password*	The password of the top-level administrator.

The following options are non-mandatory:

Option	Description
`-A` [+]*attributename:value*	An attribute to modify. The *attributename* is defined in the LDAP schema and the *value* specified replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes. If the action value (+), is not specified, the default action is to add the existing value.
`-h, -?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-o` *organization RDN*	Specifies the organization RDN for the domain. For example, `o=varrius.florizel.com`. If this option is not specified then the organization is created under the `osi suffix`, with `o`=the name of the domain, `o=osiSuffix`.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.

Option	Description
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-S` *service*	Specifies the service or services to be added to the domain. *service* can have the value of a single service or multiple services. The valid *service* values are `mail` and `cal`. These values are case-insensitive. If the `-S mail` option is specified, then the `-H` option must be specified. Can be listed as a comma-separated list. For Example: `-S mail,cal` A domain is created with the services mentioned depending on the value of the particular service definition present in the configuration file of the Identity Sever.
The following option is only allowed if the `-S mail` option is specified:	
`-H` *preferred mailhost*	The preferred mail host for the domain. The host must be a fully qualified host name, for example, `mailhost.sesta.com`. This option is mandatory if the `-S mail` option is specified.
The following options are only allowed if the `-S cal` option is specified:	
`-B` *backend calendar data server*	Specifies the default backend host assigned to a user or resource in a domain.
`-C` *searchable domains*	Specifies the domains to be searched when looking for calendars or users.
`-g` *access control string*	Specifies the Access Control List (ACL) for newly created user calendar.
`-P` *propertyname*[:*value*]	Sets values for multi-valued and bit oriented attributes. Refer to table "Attribute Values" on page 165 for attributes, their descriptions and values.
`-R` *right*[:*value*]	Sets calendar domain attribute `icsAllowRights`. The attribute holds a bitmap value. See "Attribute Values" on page 165 for a list of attributes, their value, and description.

Option	Description
`-T` *calendar time zone string*	Specifies the time zone ID used when importing files. See "Calendar Time Zone Strings" on page 167 for a list of the valid time zone strings.

Example

To create a new domain with mail and calendar services, enter:

```
commadmin domain create -D chris -d florizel.com -n sesta.com -w bolton \
-S mail,cal -H mailhost.sesta.com
```

commadmin domain delete

The `commadmin domain delete` command marks a single hosted domain as deleted from the server. To mark multiple hosted domains as deleted, use the `-i` option.

The "commadmin domain purge" on page 110 command will permanently remove the domain.

To disable Organization Administrators usage of a service like calendar service or mail service, use the `-S` option. Here `S` is in uppercase.

Syntax

```
commadmin domain delete -D login -d domain name -n domain -w password [-h] [-?]
   [-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the top-level administrator.
`-d` *domain name*	The DNS domain name that is being deleted. If `-d` is not specified, the domain specified by `-n` is used.
`-n` *domain*	The domain of the top-level administrator.
`-w` *password*	The password of the top-level administrator.

The following options are non-mandatory:

Option	Description
-h, -?	Prints command usage syntax.
-i *inputfile*	Reads the command information from a file instead of the command line.
-p *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured during installation.
-s	Use SSL (Secure Socket Layer) to connect to the Access Manager.
-S *service*	Modifies the value of the specified service status attribute value to "deleted'. Multiple services are separated by a comma. The valid *service* values are `mail` and `cal`. These values are case-insensitive.
-v	Enable debugging output.
-V	Prints information about the utility and its version.
-X *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To delete an existing domain:

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com
```

To delete just the mail service from the `florizel.com` domain:

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com \
-S mail
```

commadmin domain modify

The `commadmin domain modify` command modifies attributes of a single domain's directory entry. To modify multiple domains, use the `-i` option.

Syntax

```
commadmin domain modify -D login -d domain -n domain -w password
   [-A [+|-]attributename:value] [-h] [?] [-i inputfile] [-p AM port] [-s] [-v] [-V]
   [-X AM host]
   [-S mail -H preferred mailhost]
   [-S cal [-g access string] [-C cross domain search domains] [-B backend calendar data server]
   [-P [action]propertyname[:value]] [-R propertyname[:value]] [-T calendar time zone string]]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the top-level administrator.
`-d` *domain*	The DNS domain name to be modified. If `-d` is not specified, the domain specified by `-n` is used.
`-n` *domain*	The domain of the top-level administrator.
`-w` *password*	The password of the top-level administrator.

The following options are non-mandatory:

Option	Description
`-A` [`+` | `-`]*attributename*:*value*	An attribute to modify. The *attributename* is defined in the LDAP schema and value replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes. A "-" indicates removing the value. If the "-" is used, it must be preceded by two backslashes if the command is specified on the command line. If the option is provided within an input file, one backslash must precede the "-" sign. If the action value (`+` or `-`), is not specified, the default action is to replace the existing value.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.

Option	Description
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-S` *service*	Adds the specified service or services to the domain during modification. The valid *service* values are `mail` and `cal`. These values are case-insensitive. The services listed with the `-S` option are separated by a comma. If `-S mail` is specified, then the `-H` option must be specified.
When adding a service, the following option is only allowed if the `-S mail` option is specified:	
`-H` *preferred mailhost*	The preferred mailhost for the domain. This option is mandatory if the `-S mail` option is specified.
When adding a service, the following options are only allowed if the `-S cal` option is specified:	
`-B` *backend calendar data server*	The default backend host assigned to a user or resource in a domain.
`-C` *cross domain search domains*	Specifies the domains to be searched when looking for calendars or users.
`-g` *access string*	Specifies the Access Control List (ACL) for newly created user calendar.
`-P` [*action*]*propertyname*[:*value*]	Sets the values for multi-valued and bit oriented attributes. Refer to table "Attribute Values" on page 165 for the descriptions and values of *propertyname*.
`-T` *calendar time zone string*	Time zone ID used when importing files. See "Calendar Time Zone Strings" on page 167 for a list of the valid time zone strings.
`-R` *propertyname*[:*value*]	Sets calendar domain attribute `icsAllowRights`. The attribute holds a bitmap value. See "Attribute Values" on page 165 for a list property names, their value, and description.

Example

To modify an existing domain:

```
commadmin domain modify -D chris -w bolton -n sesta.com -d varrius.com \
-A preferredmailhost:test.siroe.com
```

commadmin domain purge

The `commadmin domain purge` command permanently removes all entries or service of entries that have been marked for removal. This can include domains, users, groups, and resources.

As part of periodic maintenance operations, use the `commadmin domain purge` command to remove all entries that have been deleted for a time period that is longer than the specified grace period.

You can perform a purge at any time by invoking the command manually.

When you invoke the command, the directory is searched and a list of domains is created whose entries include domains that have been marked for deletion longer than the specified grace period. The default value for the grace period is set to 5 days.

If the `-d*` option is specified, all domains are searched for users and domains that are marked as deleted. Users that are marked as deleted will be purged from their domain, but the domain will not be purged unless it is also marked as deleted. If a domain is marked as deleted, it will be purged along with all users within that domain.

After a service has been marked as deleted, a utility that removes resources such as mailboxes or calendars must be run before the service can be purged from the directory. For mail services, the program is called `msuserpurge`. Refer to the *Sun Java System Messaging Server Administration Reference* for information about the `msuserpurge` utility. For calendar services, the program is `csclean`. Refer to the *Sun Java System Calendar Server Administration Guide* for information about the `csclean` utility.

Note – The `commadmin domain purge` command must be run by the Top-level administrator.

Syntax

```
commadmin domain purge -D login -n domain -w password -d domain [-g grace] [-h]
   [-?] [-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the top-level administrator.
`-n` *domain*	Domain of the top-level administrator.
`-w` *password*	Password of the top-level administrator.
`-d` *domain*	Purge specified domain. The * operator (`-d*`) may be used to search for a pattern.

The following options are non-mandatory:

Option	Description
`-g` *grace*	Grace period in days before the domain is purged. Domains marked for deletion for less than *grace* days will not be purged. A 0 indicates purge immediately. The default value is 5 days. The default value cannot be changed permanently. You can change the grace period only by using the `-g` *grace* option in the `commadmin domain purge`command.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-S` *service*	Removes service related object classes and attributes from the domain. If the domain contains users and resources it removes the service specific data from the directory for these users and resources. The list of services is separated by the comma (,) delimiter. The valid *service* values are `mail` and `cal`. These values are case-insensitive.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.

Option	Description
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

In the following example, the `siroe.com` domain is purged and all entries within the domain are also removed:

```
commadmin domain purge -D chris -d siroe.com -n sesta.com -w bolton
```

commadmin domain search

The `commadmin domain search` command obtains all the directory properties associated with a single domain. To obtain all the directory properties for multiple domains, use the `-i` option. When `-S` is specified in this command, only the domains having active specified services are displayed.

Syntax

```
commadmin domain search -D login -n domain -w password [-d domain] [-h] [-?]
   [-i inputfile] [-p AM port] [-s] [-S service] [-t Search Template] [-v] [-V]
   [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	The domain of the user specified with the `-D` option.
`-w` *password*	The password of the user specified with the `-D` option.

The following options are non-mandatory:

Option	Description
`-d` *domain*	Search for this domain. If `-d` is not specified or `-d*` is specified, all domains are displayed.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-S` *service*	Specifies the services to be searched in the active domains. *service* can have the value of a single service or multiple services. The valid *service* values are `mail` and `cal`. These values are case-insensitive. The list of services is separated by the comma (,) delimiter. For Example: `-S mail,cal`
`-t` *Search template*	Specifies the name of the search templates to be used instead of the default search templates. Only active domains are displayed after the search.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

commadmin group create

The `commadmin group create` command adds a single group to the Access Manager. To create multiple groups, use the `-i` option.

If a group is created without any members, by default, it is a static group.

Note – Groups cannot contain both static and dynamic members.

An email distribution list is one type of group. When a message is sent to the group address, Access Manager sends the message to all members in the group.

Syntax

```
commadmin group create -D login -G groupname -n domain -w password
   [-A [+]attributename:value] [-d domain] [-f ldap-filter] [-h] [-?]
   [-i inputfile] [-m internal-member] [-p AM port] [-s] [-v] [-V] [-X AM host]
   [-S service [-H mailhost] [-E email] [-M external-member] [-o owner] [-rs moderator]]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user who has permission to execute this command.
`-n` *domain*	The domain of the user specified by the `-D` option.
`-G` *groupname*	The name of the group (for example, `mktg-list`).
`-w` *password*	The password of the user specified by the `-D` option.

The following options are non-mandatory:

Option	Description
`-A` [+]*attributename:value*	An attribute to modify. The *attributename* is defined in the LDAP schema and *value* replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes.
`-d` *domain*	The fully qualified domain name of the group (for example, `varrius.com`). The default is the local domain. If `-d` is not specified, the domain specified by `-n` is used.
`-f` *ldap-filter*	Creates dynamic groups. Setup the LDAP filter by specifying an attribute or a combination of attributes. Multiple `-f` commands can be specified to define many LDAP filters for members of a group.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.

Option	Description
`-m` *internal -member*	User ID of the internal members added to this group. To add more than one member, use multiple `-m` options. This options should be used to create static groups.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-S` *service*	Specifies the services to be added to the Group. *service* can have the value of a single service or multiple services.The valid service values are mail and cal. These values are case-insensitive. The list of services is separated by the comma (,) delimiter. For Example: `-S mail,cal`
The following options are only allowed if the `-S mail` option is specified:	
`-H` *mailhost*	The mail host to which this group responds (for example, `mailhost.varrius.com`). The default is the local mail host.
`-E` *email*	The email address of the group.
`-M` *external-member*	User ID of the external members added to this group. To add more than one member, use multiple `-M` options.
`-o` *owner*	The group owner's email address. An owner is the individual responsible for the distribution list. An owner can add or delete distribution list members.
`-r` *moderator*	The moderator's email address.

Example

To create a group `testgroup` in the domain `sesta.com`:

```
commadmin group create -D chris -n sesta.com -w bolton -G testgroup \
-d sesta.com -m lorca@sesta.com -S mail -M achiko@varrius.com
```

commadmin group delete

The `commadmin group delete` command marks a single group as deleted. To mark multiple groups as deleted, use the `-i` option.

To disable a group's usage of services such as Calendar Server or Messaging Server use the `-S` option. Here `S` is in uppercase.

Note – In order to permanently remove a group, you must run the following command: "commadmin domain purge" on page 110.

Syntax

```
commadmin group delete -D login -G groupname -n domain -w password [-d domain]
   [-h] [-?] [-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

Options

The following are mandatory options:

Option	Description
`-D` *login*	The user ID of the user who has permission to execute this command.
`-G` *groupname*	The name of the group to be marked as deleted. For example, `mktg-list`.
`-n` *domain*	The domain of the user specified by the `-D` option.
`-w` *password*	The password of the user specified by the `-D` option.

The following are non-mandatory options:

Option	Description
`-d` *domain*	The domain of the group. If `-d` is not specified, the domain specified by the `-n` option is used.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.

Option	Description
-p *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
-s	Use SSL (Secure Socket Layer) to connect to the Access Manager.
-S *service*	Modifies the value of the specified service status attribute value to ”deleted’. The services listed with the -S option are separated by a comma. The valid *service* values are mail and cal. These values are case-insensitive.
-v	Enable debugging output.
-V	Prints information about the utility and its version.
-X *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Examples

The following example marks the group testgroup@varrius.com as deleted:

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com
```

The following example marks the mail service for testgroup@varrius.com as deleted:

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com -S mail
```

commadmin group modify

The commadmin group modify command changes the attributes of a single group that already exists in the Access Manager. To change the attributes of multiple groups, use the -i option.

A mailing list is one type of group. When a message is sent to the group address, Access Manager sends the message to all members in the group.

Syntax

```
commadmin group modify -D login -G groupname -n domain -w password
    [-A [+|-]attributename:value] [-d domain] [-f [action]ldap-filter] [-h] [-?]
    [-i inputfile] [-m [+|-]internal-member] [-p AM port] [-s] [-v] [-V] [-X AM host]
    [-S mail [-o owner] [-E email] [-H mailhost] [-M external-member] [-r moderator]]
```

Options

The following are mandatory options:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-G` *groupname*	The name of the group to be modified. For example, `mktg-list`.
`-n` *domain*	The domain of the user specified by the `-D` option.
`-w` *password*	The password of the user specified by the `-D` option.

The following are non-mandatory options:

Option	Description
`-A` [`+` | `-`]*attributename:value*	An attribute to modify. The *attributename* is defined in the LDAP schema and value replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes. A "-" indicates removing the value. If the "-" is used, it must be preceded by two backslashes or enclosed in quotes if the command is specified on the command line. If the option is provided within an input file, one backslash must precede the "-" sign.
`-d` *domain*	The domain of the group. If `-d` is not specified, the domain specified by the `-n` option is used.
`- f` [*action*] *ldap-filter*	Indicates whether a ldap filter is added to or removed from the group A "+" before the *ldap-filter* indicates that it is to be added to the existing filters. A "-" indicates removing the existing filter. Type `-f-*` to remove all the filters. If the "-" is used, it must be preceded by two backslashes or enclosed in quotes if the command is specified on the command line. If *action* is not specified, by default the filter is added provided it is not already present. Otherwise an error message is displayed.
`-h`, `-?`	Prints command usage syntax.

Option	Description
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-m` [*action*] *internal -member*	Indicates whether to add or remove an internal member. The value of internal-*member* is either a mail address or user ID. An *action* value of: + adds the member to an existing list of internal members. - removes the member from an existing list of internal members. If the "-" is used, it must be preceded by two backslashes or enclosed in quotes if the command is specified on the command line. `-m-* removes all the internal members.`
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-S mail`	Adds mail service to the group during modification after validating whether the mail service already exists. If the service exists an error message is displayed. The only valid value for `-S` is `mail`.
The following options are only allowed if the `-S mail` option is specified:	
`-o` *owner*	The group owner's email address. An owner is the individual responsible for the distribution list. An owner can add or delete distribution list members.
`-E` *email*	The email address of the group.
`-H` *mailhost*	The group's mail host. The default is the local mail host.
`-M` *external -member*	Adds an external member. The value of *external-member* is the user mail address.

Option	Description
`-r` *moderator*	The moderator's user ID. Type the email address if the moderator is in a different domain. The `-S mail` option must be specified with this option.

Example

To remove an internal member (`jsmith`) from the group `testgroup` within the domain `varrius.com`:

```
commadmin group modify -D chris -d varrius.com -G testgroup -n sesta.com \
-w bolton -m \\-jsmith
```

commadmin group search

The `commadmin group search` command obtains all the directory properties associated with a single group. To obtain all the directory properties for multiple groups, use the `-i` option.

Syntax

```
commadmin group search -D login -n domain -w password [-d domain] [-E string]
    [-G string] [-h] [-?] [-i inputfile] [-p AM port] [-s] [-S service]
    [-t search template] [-v] [-V] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	The domain of the user specified by the `-D` option.
`-w` *password*	The password of the user specified by the `-D` option.

The following options are non-mandatory:

Option	Description
`-d` *domain*	The domain of the group to be searched. If `-d` is not specified, all domains are searched.
`-E` *string*	Email address of the group. The wildcard operator (*) may be used within any part of string.
`-G` *string*	The name of the group to be searched. For example, `mktg-list`. If `-G` is not specified, all groups in the domain specified by `-d` are displayed. The wildcard operator (*) may be used within any part of string.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the IS server is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-S` *service*	Specifies the service to be searched. The only valid value for *service is* `mail`. This value is case-insensitive. For Example: `-S mail` Only groups with active services are displayed.
`-t` *Search Template*	Specifies the name of the search templates to be used instead of the default search templates. This is an entry in the directory that defines the filter for the search. Only active groups are searched for.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To search for a group named `developers` under the `siroe.com` domain:

```
commadmin group search -D chris -n sesta.com -w password -G developers \
-d siroe.com
```

commadmin resource create

The `commadmin resource create` command creates a directory entry for a resource.

For instructions on creating a resource, see "Creating a Resource" on page 124.

Syntax

```
commadmin resource create -D login -n domain -w password -u identifier -N name
   -o owner [-c calendar identifier] [-A [+]attributename:value] [-C DWPHost]
   [-d domainname ] [-h] [-?] [-i inputfile][-p AM port] [-s] [-T time zone] [-v]
   [-V] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	Domain of the user specified with the `-D` option.
`-w` *password*	Password of the user specified with the `-D` option.
`-u` *identifier*	Resources' unique identifier. This *identifier* value should be unique within the domain namespace or within all the users and resources the calendar manages in the calendar mode.
`-N` *name*	Friendly name used to display the resource in the calendar GUI.
`-o` *owner*	Owner of the resource. This user ID must exist under the domain in which the resource is created.
`-c` *calendar identifier*	Identifier for this resource's calendar. The identifier value should be unique throughout all the calendars managed by the Calendar Server

The following options are non-mandatory:

Option	Description
`-A` [`+`] *attributename:value*	An attribute to modify. The *attributename* is defined in the LDAP schema and *value* replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes.
`-C` *DWPHost*	The DNS name of the back end calendar server which hosts this user's calendars. If the DNS name of the backend calendar server is not specified, the value stored in the ics.conf file of the server is used as the default value.
`-d` *domain name*	Domain of the resource. If `-d` is not specified, the domain specified by `-n` is used.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-T` *time zone*	The time zone used to display the resource's calendar in the calendar's user interface. See "Calendar Time Zone Strings" on page 167 for a list of the valid time zone strings.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To create a resource with Name `peter` in the calendar `cal.siroe.com` under the domain `varrius.com`:

```
commadmin resource create -D chris -n sesta.com -w bolton -o ownerid \
-d varrius.com -u id -c calid -N peter -C cal.siroe.com
```

Creating a Resource

A resource consists of two data descriptions: a directory entry and a calendar in the Calendar Server database. The directory entry has an attribute, `icsCalendar`, whose value is the name of the calendar associated with the resource.

You can create a resource with the two data descriptions, using either of the following methods:

- Use the `csresource` utility by itself. The `csresource` utility creates a directory entry and a calendar.

  However, using `csresource` to create both the directory entry and the calendar is only recommended if the directory is in a Schema 1 environment and you are not using Access Manager.

- Use `commadmin resource create` to create a directory entry and use the `csresource` utility to create a calendar. For example:

  Use `commadmin resource create` to create a directory entry:

  ```
  commadmin resource create -D amadmin -w ampassword -n blink.sesta.com
   -X blink -p 5555 -d varrius.com -o test1 -u resourceOne
   -N firstResource -c resourceOneCalendar
  ```

  The directory entry is as follows:

  ```
  dn: uid=resourceONE,ou=People,o=varrius,o=domainroot
  uid: resrouceONE
  objectClass: icsCalendarResource
  objectClass: top
  cn: firstResource
  icsStatus: active
  icsCalendar: test1@varrius.com:resourceOne
  ```

  Use `csresource` to create a calendar.

NOTE: When you invoke the `create` command in `csresource`, the value you enter for the name of the resource must be the same as the value used for the `-u` option in `commadmin resource create`.

You can now log in as any user and invite the resource to an event.

For a detailed description of the `csresource` utility, see the "Calendar Server Command-Line Utilities" in the *Sun Java System Calendar Server Administration Guide*.

commadmin resource delete

The `commadmin resource delete` command marks the resource as deleted.

Note – To permanently remove the resource, run the "commadmin domain purge" on page 110.

Syntax

```
commadmin resource delete -D login -u identifier -n domain -w password [-d domainname]
   [-h] [-?] [-i inputfile] [-p AM port] [-s] [-v] [-V] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	Domain of the user specified with the `-D` option.
`-w` *password*	Password of the user specified with the `-D` option.
`-u` *identifier*	Resource's unique identifier

The following options are non-mandatory:

Option	Description
`-d` *domainname*	Domain of the resource. If `-d` is not specified, the domain specified by `-n` is used.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.

Option	Description
`-X` *AM host*	Specify the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To mark a resource as deleted:

```
commadmin resource delete -D chris -n sesta.com -w bolton -u bill023
```

commadmin resource modify

The `commadmin resource modify` command modifies the resource.

Syntax

```
commadmin resource modify -D login -n domain -w password -u identifier
    [-A [+|-]attributename:value] [-d domainname ] [-h] [-?] [-i inputfile]
  [-N name] [-p AM port] [-s] [-T time zone] [-v] [-V] [-X sAM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	Domain of the user specified with the `-D` option.
`-w` *password*	Password of the user specified with the `-D` option.
`-u` *identifier*	Resources's unique identifier.

The following options are non-mandatory:

Option	Description
`-A` [`+` | `-`]*attributename*:*value*	An attribute to modify. The *attributename* is defined in the LDAP schema and value replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes. A "-" indicates removing the value. If the "-" is used, it must be preceded by two backslashes if the command is specified on the command line. If the option is provided within an input file, one backslash must precede the "-" sign.
`-d` *domainname*	Domain of the resource. If `-d` is not specified, the domain specified by `-n` is used.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-N` *name*	Common name used to display the resource in the calendar user interface.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-T` *time zone*	The time zone used to display resource's calendar in the calendar GUI. See "Calendar Time Zone Strings" on page 167 for a list of the valid time zone strings.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To modify a resource with the unique identifier `bill023` with a new common name `bjones`:

```
commadmin resource modify -D chris -n sesta.com -w bolton -d test.com \
-u bill023 -N bjones
```

commadmin resource search

The `commadmin resource search` command searches for a resource.

Syntax

```
commadmin resource search -D login -n domain -w password [-d domain] [-h] [-?]
   [-i inputfile] [-N string] [-p AM port] [-s] [-t Search Template] [-u string]
   [-V] [-v] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with the permission to execute this command.
`-n` *domain*	Domain of the user specified with the `-D` option.
`-w` *password*	Password of the user specified with the `-D` option.

The following options are non-mandatory:

Option	Description
`-d` *domain*	Domain of the resource. Search is performed only in the domain. If `-d` is not specified or `-d*` is specified, then all domains are searched.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-N` *string*	Enter the resource's common name. The wildcard operator (*) may be used within any part of string.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.

Option	Description
`-t` *Search Template*	Specifies the name of the search templates to be used instead of the default search templates. This is an entry in the directory that defines the filter for the search. Only active resources are searched for.
`-u` *string*	The resource identifier specified must be unique for the domain namespace or for all the users and resources the calendar manages. The wildcard operator (*) may be used within any part of string. If the identifier is not specified or `-l*` is specified all resources are displayed during the search.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specify the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To search for a resource `arabella` in the domain `sesta.com`:

```
commadmin resource search -D serviceadmin -w serviceadmin -n sesta.com \s
-d sesta.com -u arabella
```

commadmin user create

The `commadmin user create` command creates a single user in the Access Manager system. To create multiple users, use the `-i` option.

Syntax

```
commadmin user create -D login -F firstname -n domain -L lastname -l userid
    -w password -W password [-A [+]attributename:value] [-d domain]
    [-I initial] [-h] [-?] [-i inputfile] [-p AM port] [-s] [-v] [-V] [-X AM host]
    [-S mail [-E email] [-H mailhost]]
    [-S cal [-B DWPHost] [-E email] [-k calid_type] [-J First Day of Week] [-T time zone]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-F` *firstname*	The user's first name; must be a single word without any spaces.
`-n` *domain*	The domain of the user specified with the `-D` option.
`-l` *userid*	The user's login name.
`-w` *password*	The password of the user specified with the `-D` option.
`-W` *password*	The password of the user that is being created. You may also specify *password* via a text file, *password*`.txt`.
`-L` *lastname*	The User's lastname.

The following options are non-mandatory:

Option	Description
`-A` [`+`]*attributename*:*value*	An attribute to modify. The *attributename* is defined in the LDAP schema and *value* replaces any and all current values for this attribute in the directory. Repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes.
`-d` *domain*	Domain of the user. If `-d` is not specified, the domain specified by `-n` is used.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-I` *initial*	User's middle initial.
`-h`, `-?`	Prints command usage syntax.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.

Option	Description
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-S` *service*	Adds the specified service to the user during creation. *service* can have the value of a single service or multiple services. The valid *service* values are `mail` and `cal`. These values are case-insensitive. The list of services is separated by the comma (,) delimiter. For Example: `-S mail,cal`
The following options are only allowed if the `-S mail` option is specified:	
`-E` *email*	The email address of the user.
`-H` *mailhost*	The mail host of the user.
The following options are only allowed if the `-S cal` option is specified:	
`-B` *DWPHost*	DNS name of the back end calendar that hosts the user's calendar.
`-E` *email*	The email address of the calendar user.
`-J` *First Day of Week*	First day of the week shown when the calendar is displayed in the calendar server user interface. The valid values are 0-6 (0 is Sunday, 1 is Monday, and so on).

Option	Description
`-k` *calid_type*	Specifies the type of calendar id that is created. The accepted values are `legacy` and `hosted`. If `-k legacy` is specified, only the calendar id is used (for example, `jsmith`). If `-k hosted` is specified, the calendar id plus domain is used (for example, `jsmith@sesta.com`). If the `-k` option is not specified, the default is to use the calendar id plus domain (`hosted`). You can set the value of the calendar id type that is created if the `-k` option is not specified. To do so, add the following parameter to the `resource.properties` file: `switch-caltype=`*value* where *value* is "`hosted`"	"`legacy`". The `resource.properties` file is located in the following directory: *da_base*`/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties`
`-T` *time zone*	The time zone in which the user's calendar is displayed. See "Calendar Time Zone Strings" on page 167 for a list of the valid time zone strings.

Example

To create a new user, `smith`, enter:

```
commadmin user create -D chris -n sesta.com -w secret -F smith -l john \
-L major -W secret -S mail -H mailhost.siroe.com
```

commadmin user delete

The `commadmin user delete` command marks a single user as deleted. To mark multiple users as deleted, use the `-i` option.

No undelete utility exists. However, you can use the `ldapmodify` command to change the status attribute of a user entry to `active` at any time before the purge grace period has expired and a purge is set to run against the entry.

▼ To remove a user

Steps

1. **Mark the user as deleted by running the `commadmin user delete` command.**
2. **Remove resources from the user.**

   A resource can be a mailbox or a calendar.

   For mail services, the program is called `msuserpurge`. Refer to the *Sun Java System Messaging Server Administration Reference* for information about the `msuserpurge` utility.

   For calendar services, the program is `csclean`. Refer to the *Sun Java System Calendar Server Administration Guide* for information about the `csclean` utility.
3. **Permanently remove the user, by invoking the following command:** **"commadmin domain purge" on page 110.**

Syntax

```
commadmin user delete -D login -n domain -l login name -w password [-d domain]
   [-h] [-?] [-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with the permission to execute this command.
`-n` *domain*	The domain of the user specified with the `-D` option.
`-w` *password*	The password of the user specified with the `-D` option.
`-l` *userid*	The user ID of the user to be deleted.

The following options are non-mandatory:

Option	Description
`-d` *domain*	Domain of the user. If `-d` is not specified, the domain specified by `-n` is used.
`-h`, `-?`	Prints command usage syntax.

Option	Description
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-S` *service*	Specifies the services to be removed from the user. The user remains active, but only the specified services are deactivated. If `-S` is not specified, then the user is deleted. *service* can have the value of a single service or multiple services. The valid *service* values are `mail` and `cal`. These values are case-insensitive. The list of services is separated by the comma (,) delimiter. For Example: `-S mail,cal`
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

To mark an existing user as deleted:

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith
```

To delete the mail services only from user `smith`:

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail
```

commadmin user modify

The `commadmin user modify` command modifies attributes of a single user's directory entry. To modify multiple user, use the `-i` option.

Syntax

```
commadmin user modify -D login -n domain -l userid -w password
   [-A [+|-]attributename:value] [-d domain] [-h] [-?] [-i inputfile] [-p AM port]
   [-s] [-v] [-V] [-X AM host]
```

```
[-S mail -H mailhost [-E email]]
[-S cal [-B DWPHost] [-E email] [-k calid_type] [-J First Day of Week]
[-T time zone]]
```

Options

The following options are mandatory:

Option	Description
`-D` *login*	The user ID of the user with permission to execute this command.
`-n` *domain*	Domain of the user specified with the `-D` option.
`-w` *password*	The password of user specified with the `-D` option.
`-l` *userid*	User's login ID.

The following options are non-mandatory:

Option	Description
`-A` [`+` | `-`]*attributename*:*value*	An attribute to modify. The *attributename* is defined in the LDAP schema and value replaces any and all current values for this attribute in the directory. You can repeat this option to modify multiple attributes at the same time, or to specify multiple values for the same attribute. A "+" before the *attributename* indicates adding the value to the current list of attributes. A "-" indicates removing the value. If the "-" is used, it must be preceded by two backslashes if the command is specified on the command line. If the option is provided within an input file, one backslash must precede the "-" sign.
`-d` *domain*	Domain of the user or group. If `-d` is not specified, the domain specified by `-n` is used.
`-h`, `-?`	Prints command usage syntax.
`-i` *inputfile*	Reads the command information from a file instead of the command line.
`-p` *AM port*	Specifies an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.

Option	Description
`-s`	Use SSL (Secure Socket Layer) to connect to the Access Manager.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.
`-S` *service*	Adds the specified services to the user after validating whether the user has the service specified with `-S` option.If the user already has the service an error message is displayed. *services* can have the value of a single service or multiple services. The valid *service* values are `mail` and `cal`. These values are case-insensitive. The list of services is separated by the comma (,) delimiter. For Example: `-S mail,cal`
The following options are only allowed if the `-S mail` option is specified:	
`-E` *email*	Specifies the email address of the user.
`-H` *mailhost*	The mail host of the user. This option is mandatory if the `-S mail` option is specified.
The following options are only allowed if the `-S cal` option is specified:	
`-B` *DWPHost*	Specifies the DNS name of the backend calendar server that hosts this user's calendars. Note: This attribute can only be added and cannot be modified if it already exists.
`-E` *email*	Specifies the email address for the calendar user.
`-J` *First Day of Week*	The first day of the week shown when the calendar is displayed in the calendar server user interface. The valid values are 0-6 (0 is Sunday, 1 is Monday, and so on).

Option	Description
-k *calid_type*	Specifies the type of calendar id that is created (when adding the calendar service). The accepted values are `legacy` and `hosted`. If `-k legacy` is specified, only the calendar id is used (for example, `jsmith`). If `-k hosted` is specified, the calendar id plus domain is used (for example, `jsmith@sesta.com`). If the `-k` option is not specified, the default is to use the calendar id plus domain (`hosted`). You can set the value of the calendar id type that is created if the `-k` option is not specified. To do so, add the following parameter to the `resource.properties` file: `switch-caltype=`*value* where *value* is "`hosted`"	"`legacy`". The `resource.properties` file is located in the following directory: *da_base*`/data/WEB-INF/classes/sun/comm/cli/ \` `server/servlet/resource.properties`
-T *time zone*	A user's calendar is displayed in this time zone. See "Calendar Time Zone Strings" on page 167 for a list of the valid time zone strings.

Examples

The following example adds a mail service for the user `smith`:

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A description:"new description" -S mail -H mailhost.siroe.com
```

In this example, a mail forwarding address is added for user `smith`:

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A +mailforwardingaddress:tsmith@siroe.com
```

commadmin user search

The `commadmin user search` command obtains all the directory properties associated with a single user. To obtain all the directory properties for multiple users, use the `-i` option. Only active users are displayed after a search.

Syntax

```
commadmin user search -D login -n domain -w password [-d domain] [-E string]
   [-F string] [-h] [-?] [-i inputfile] [-L string] [-l string] [-p AM port] [-s]
```

[-S *service*] [-t *Search Template*] [-v] [-V] [-X *AM host*]

Options

The following options are mandatory:

Option	Description
-D *login*	The user ID of the user with permission to execute this command.
-n *domain*	The domain of the user specified with the -D option.
-w *password*	The password of the user specified with the -D option.

The following options are non-mandatory:

Option	Description
-d *domain*	The domain of the user. The user is searched only in the specified domain. If -d is not specified, all domains are considered for the search.
-E *string*	Searches for user's mail address. The wildcard operator (*) may be used within any part of string.
-F *string*	Searches for user's first name. The wildcard operator (*) may be used within any part of string.
-h, -?	Prints command usage syntax.
-i *inputfile*	Reads the command information from a file instead of the command line.
-L *string*	Searches for user's last name. The wildcard operator (*) may be used within any part of string.
-l *string*	Searches for user's login name. The wildcard operator (*) may be used within any part of string.
-p *AM port*	Use this option to specify an alternate TCP port where the Access Manager is listening. If not specified, the default *AM port* is used, or Port 80 is used if no default was configured at install time.
-s	Use SSL (Secure Socket Layer) to connect to the Access Manager.

Option	Description
`-S` *service*	Specifies the services to match in the user search. *services* can have the value of a single service or multiple services. The valid *service* values are `mail` and `cal`. These values are case-insensitive. The list of services is separated by the comma (,) delimiter. For Example: `-S mail,cal`
`-t` *Search template*	Specifies the name of the search templates to be used instead of the default search templates. This is an entry in the directory that defines the filter for the search. Only active users are searched for.
`-v`	Enable debugging output.
`-V`	Prints information about the utility and its version.
`-X` *AM host*	Specifies the host on which the Access Manager is running. If not specified, the default *AM host* is used, or the localhost if no default was configured at install time.

Example

The following example searches for users in the `varrius.com` domain:

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

APPENDIX **A**

Service Provider Administrator and Service Provider Organizations

The Delegated Administrator console provides a new administrator role, the Service Provider Administrator (SPA), as well as new types of organizations that can be created in the directory.

This appendix describes the following topics:

This appendix describes the Service Provider Administrator role and the new organization types and explains how to create them in Delegated Administrator.

Service Provider Administrator

The Delegated Administrator console lets you delegate administrative tasks to a new role, the Service Provider Administrator (SPA), who can create and manage new types of subordinate organizations.

The SPA's scope of authority lies between that of the Top-Level Administrator (TLA) and the Organization Administrator (OA).

With the SPA, you can create a three-tiered administrative hierarchy, as described in "Three-Tiered Hierarchy" on page 24 in Chapter 1.

This second level of delegation can ease the management of a large customer base supported by a large LDAP directory. For example, an ISP may offer services to hundreds or thousands of small businesses, each of which requires its own organization. Each day, dozens of new organizations might have to be added to the directory.

If you used a two-tiered hierarchy, the TLA would have to create all these new organizations. Now the TLA can delegate these tasks to SPAs.

The SPAs can create subordinate organizations for new customers and assign OAs to manage users in those organizations.

Figure A–1 shows a logical view of a sample three-tiered organizational hierarchy.

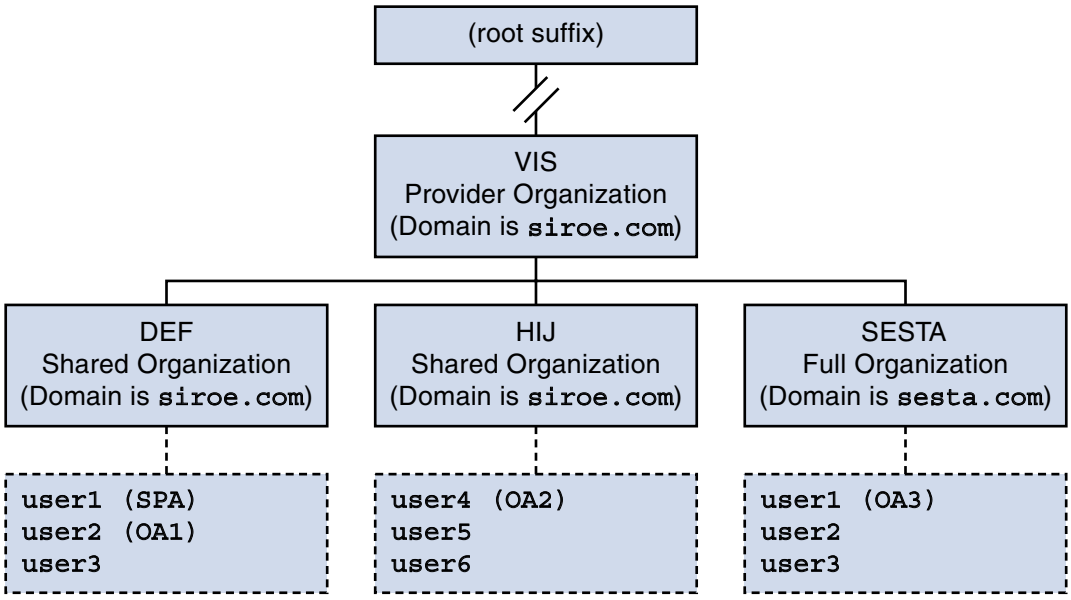

FIGURE A–1 Directory Using a Service Provider Administrator: Logical View

The example in Figure A–1 shows one provider organization. However, a directory can contain multiple provider organizations.

In this example, administrative tasks are delegated as follows:

- The SPA has the authority to manage the VIS provider organization and all organizations under it. The SPA role is assigned to `user1` in the DEF organization.
- The Organization Administrator named OA1 manages DEF, a shared organization. This OA role is assigned to `user2` in the DEF organization.
- OA2 manages HIJ, a shared organization. This OA role is assigned to `user4` in the HIJ organization.

- OA3 manages SESTA, a full organization. This OA role is assigned to `user1` in the SESTA organization.

  SESTA is a full organization and has its own unique namespace. `user1` in SESTA (in the `sesta.com` domain) has a unique user ID.

For definitions of provider and subordinate organizations, see "Organizations Managed by the Service Provider Administrator" on page 145.

Service Provider Administrator Role

The SPA can perform the following tasks:

- Create, delete, and modify shared and full organizations in the provider organization in which the SPA has administrative authority.

  In the example shown in Figure A–1, the SPA for the VIS provider organization can

  - Modify or delete the DEF, HIJ, and SESTA organizations
  - Create additional organizations under the VIS provider organization.
- Create, delete, and modify users in any organization under the provider organization.
- Create, delete, and modify groups in any organization under the provider organization.
- Create, delete, and modify Calendar resources in any organization under the provider organization.
- Assign OA roles to users.

  For example, in the sample organization shown in Figure A–1, the SPA could assign an OA role to `user2` in the SESTA organization. `user2` could then manage users in the SESTA organization.

  The SPA also can remove the OA role from a user.
- Assign the SPA role to other legitimate users under the provider organization (and remove the SPA role).
- Allocate service packages to organizations.

  For information about service packages, see "Service Packages" on page 31 in Chapter 1.

  The SPA can assign specified types of service packages to an organization and determine the maximum number of each package that can be used in that organization.

  For example, the SPA could assign the following service packages:

  - In the DEF organization:

    ```
    1,000 gold packages
    500 platinum packages
    ```
  - In the HIJ organization:

```
2,500 topaz packages
500 platinum packages
500 emerald packages
1,000 ruby packages
```

- In the SESTA organization:

  ```
  2,000 silver packages
  1,500 gold packages
  100 platinum packages
  ```

  The SPA can use the Delegated Administrator console to perform these tasks. In this release, the Delegated Administrator utility does not include command options to perform these tasks.

Note – The TLA can modify or delete any existing shared organization or full organization. The TLA also can manage users in those organizations.

The TLA can remove the SPA role from a user but cannot assign the SPA role through the console. For a list of constraints in this release of Delegated Administrator, see "Considerations for This Release" on page 144.

For a complete description of the administrative tasks performed by the TLA, see "Administrator Roles and the Directory Hierarchy" on page 26 in Chapter 1.

Assigning the SPA Role to a User

The SPA role must be assigned to a user in an organization designated for SPAs and subordinate to the provider organization that the SPA will manage.

In the example shown in Figure A–1, assume you need to create an SPA for the provider organization named VIS. You could assign the SPA role to `user1` in the organization DEF.

The SPA must reside in a subordinate organization because a provider organization node does not contain any users.

Thus, before a provider organization can be managed by an SPA, at least one organization must be created under it. This organization should be designated to hold users who are assigned the SPA role. For more information, see "Creating a Provider Organization and Service Provider Administrator" on page 146.

Considerations for This Release

In this release of Delegated Administrator, you cannot use the Delegated Administrator console or utility to create an SPA or a provider organization.

To create an SPA or provider organization, you must manually modify the custom service-provider template, `da.provider.skeleton.ldif`.

For instructions on using the custom service-provider template to perform these tasks, see "Creating a Provider Organization and Service Provider Administrator" on page 146, later in this appendix.

Organizations Managed by the Service Provider Administrator

The SPA can create, modify, and delete the following types of organizations that are subordinate to the SPA's provider organization:

- "Full Organization" on page 146
- "Shared Organization" on page 146

The provider organization, full organization, and shared organization are described in the sections that follow.

Provider Organization

A provider organization is a node in the LDAP directory that logically contains full organizations and shared organizations. The provider organization node has attributes that allow the SPA to manage subordinate organizations.

In the LDAP directory, a provider organization must be located under a mail domain. For an example, see "Sample Service-Provider Organization Data" on page 161, later in this appendix.

A provider organization cannot contain user entries. Instead, users are provisioned in the organizations created under the provider organization.

A provider organization stores directory information about the organizations created under it. For example:

- Whether the provider organization can contain shared organizations, full organizations, or both
- Domain names that can be used by the shared organizations created under this provider organization
- The types and number of Class-of-Services packages available to the organizations created under this provider organization
- The organization designated to be the home of the SPA for the provider organization.

Full Organization

A full organization has the following characteristics:

- It is subordinate to the provider organization and is created by the SPA.
- Users can be provisioned in a full organization.

  In the example shown in Figure A–1, `user2` belongs to the `sesta.com` domain and has a mail address of `user2@sesta.com`.
- As a full organization, it has its own domain that no other organization can share, and it has its own unique namespace.

  In the example shown in Figure A–1, the full organization, SESTA, has the domain name `sesta.com`.

Shared Organization

A shared organization has the following characteristics:

- It is subordinate to the provider organization and is created by the SPA.
- Users can be provisioned in a shared organization.

  In the example shown in Figure A–1, `user5` belongs to the `siroe.com` domain and has a mail address of `user5@siroe.com`.
- It uses one or more of the shared domain names from the list provided by the provider organization.

  In the example shown in Figure A–1, the shared organization DEF uses the domain name `siroe.com`.
- Other shared organizations can share the domain name used by this organization.

  In the example shown in Figure A–1, both the DEF and HIJ organizations belong to the `siroe.com` domain.
- A shared organization does not have a unique namespace.

Creating a Provider Organization and Service Provider Administrator

In this release of Delegated Administrator, you must use the custom service-provider template (`da.provider.skeleton.ldif`) provided by Delegated Administrator to create your own provider organizations and SPAs.

Note – You also can install a sample provider organization (with subordinate organizations) and a sample SPA in your directory when you run the Delegated Administrator configuration program. You do this by choosing to **Load Sample Organizations** in the configuration program.

However, the sample organization template (`da.sample.data.ldif`) is meant to be used as an example, not as a template for creating your own provider organizations. For details about this example, see "Sample Service-Provider Organization Data" on page 161, later in this appendix.

Once you have created a provider organization and an SPA, the SPA can log into the Delegated Administrator console, create and manage subordinate organizations, and assign the SPA role to other users in the SPA's organization. However, these SPAs can only manage the same provider organization.

To create another provider organization and an SPA to manage it, you should use the custom service-provider template again.

This section contains the following topics:

- "Entries Created by the Template" on page 147 shows an example of the organizations created when an edited copy of the template is installed in the directory.
- "Information Needed to Create a Provider Organization, Subordinate Organization, and SPA" on page 149 defines the parameters in the template required to create a provider organization, a subordinate shared organization, and an SPA.
- "Steps for Creating a Provider Organization and Service Provider Administrator" on page 153 explains how to edit the template and install the information in your directory.
- "Custom Service-Provider Template" on page 155 is a listing of the template.

Entries Created by the Template

When you install your edited copy of the custom service-provider template in the directory, the following entries are created:

- A provider organization
- A subordinate shared organization designated to hold the SPA user
- One user in the subordinate organization to whom the SPA role is assigned
- A placeholder node under which full organizations can be created. These full organizations will be managed by the SPA for this provider organization.

Figure A–2 shows an example of the entries created by installing the template. It is a Directory Information Tree (DIT) view of the organizations.

Figure A–2 is only an example. Your organization names, SPA user name, and DIT structure should be specific to your own installation.

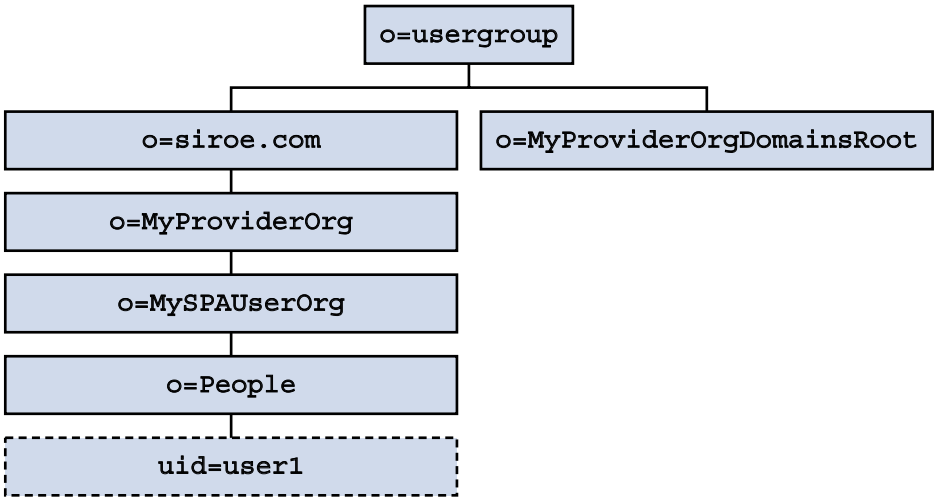

FIGURE A–2 Custom Service-Provider Template: Directory Information Tree View

Nodes in the Sample Installed Custom Service-Provider Template

The nodes in the example shown in Figure A–2 are as follows:

- `o=usergroup` - The root suffix for user/group data.
- `o=siroe.com` - The mail domain used by the provider organization.
- `o=MyProviderOrg` - The provider organization node.
- `o=MySPAUserOrg` - The subordinate shared organization designated to hold the provider organization users, including the user assigned the SPA role.
- `ou=people` - The standard LDAP organization unit required for containing users.
- `uid=user1` - The uid of the user in the MySPAUserOrg organization who is assigned to be the SPA.
- `o=MyProviderOrgDomainsRoot` - The placeholder node for holding full organizations subordinate to the MyProviderOrg provider organization.

Information Needed to Create a Provider Organization, Subordinate Organization, and SPA

To create a provider organization, one subordinate organization, and an SPA, you need to replace parameters in the custom service-provider template with information specific to your installation.

As you read about these parameters, you can look at a listing of the `da.provider.skeleton.ldif` shown in "Custom Service-Provider Template" on page 155. Or open the actual ldif file, located in the following directory:

da_base`/lib/config-templates`

For definitions of the attributes associated with these parameters, see "Chapter 5: Communications Services Delegated Administrator Classes and Attributes (Schema 2)" and "Chapter 3: Messaging Server and Calendar Server Attributes" in the *Sun Java System Communications Services Schema Reference*.

Parameters Defining the Provider and Subordinate Organization

To create a provider organization and subordinate organization, edit the following parameters:

- *ugldapbasedn*

  Root suffix of user/group data in your directory.

  Examples:

  `o=usergroup`

  `dc=red,dc=iplanet,dc=com`

- *maildomain_dn*

  Complete DN of the mail domain underneath which the provider organization will be created.

  Examples:

  `o=siroe.com, o=usergroup`

  ```
  o=sesta.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

- *maildomain_dn_str*

  The mail domain DN with all commas (,) replaced by underscores (_).

  For example, if the mail domain DN is

  ```
  o=siroe.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

  The mail domain DN string will be

```
o=siroe.com_o=SharedDomainsRoot_o=Business_dc=red_ \
dc=iplanet_dc=com
```

- *providerorg*

  Name of the provider organization. The directory node where the provider organization resides will be given this name.

  This parameter is used multiple times in the `da.provider.skeleton.ldif` template.

  Examples:

  ```
  sunProviderOrgDN: o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

  ```
  o=MyProviderOrg
  ```

  ```
  sunBusinessOrgBase: o=MyProviderOrgdomainsroot, o=usergroup
  ```

- *servicepackage*

  Name of a service package that can be assigned to users in the organizations subordinate to the provider organization. This is a multivalued parameter.

  In the "Provider Organization" section of the `da.provider.skeleton.ldif` file, you will see the following attribute:

  ```
  sunIncludeServices: <servicepackage>
  ```

  For each service package you want to include in the provider organization, add one instance of the `sunIncludeServices` attribute and *servicepackage* parameter. Only those service packages listed here can be assigned to users in subordinate organizations.

  Example:

  ```
  sunIncludeServices: gold
  sunIncludeServices: platinum
  sunIncludeServices: ruby
  sunIncludeServices: silver
  ```

  If you do not use the `sunIncludeServices` attribute (if you delete the line containing the *servicepackage* parameter), all service packages in the directory can be assigned.

- *domain_name*

  Domain name that can be assigned to subordinate organizations in the provider organization. This is a multivalued parameter.

  In the "Provider Organization" section of the `da.provider.skeleton.ldif` file, you will see the following attribute:

  ```
  sunAssignableDomains: <domain_name>
  ```

  The domain names in the `sunAssignableDomains` attribute are a subset (some or all) of the names listed in the mail domain organization's `sunPreferredDomain` and `associatedDomain` attributes. (The mail domain is the organization under which this provider organization is created.)

  For each domain name you want to include in the provider organization, add one instance of the `sunAssignableDomains` attribute and *domain_name* parameter. Only the domain names listed here can be assigned to subordinate organizations.

Example:

```
sunAssignableDomains: siroe.com
sunAssignableDomains: siroe.net
sunAssignableDomains: varrius.com
sunAssignableDomains: sesta.com
sunAssignableDomains: sesta.net
```

- *provider_sub_org*

  Name of the shared organization in which the SPA user resides. When you install the edited ldif information in the directory, this organization is created as shared and subordinate to the provider organization. It is designated as the organization that contains the SPA user. Other users who are assigned the SPA role for this provider organization must reside in this subordinate shared organization.

  In the "Provider Organization" section of the `da.provider.skeleton.ldif` file, you will see the following attribute:

  ```
  sunProviderOrgDN:
  o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
  ```

  The `sunProviderOrgDN` attribute identifies the organization designated for provider organization users, particularly the SPA user.

  Example:

  ```
  sunProviderOrgDN:
  o=MySPAUserOrg,o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

- *preferredmailhost*

  Machine name of the preferred mail host for the provider organization's subordinate organization (in which the SPA user resides). You must use a fully qualified domain name (FQDN).

  In the "Shared Subordinate Organization" section of the `da.provider.skeleton.ldif` file, you will see the following attribute:

  ```
  preferredMailHost: <preferredmailhost>
  ```

  Example:

  ```
  preferredMailHost: mail.siroe.com
  ```

- *available_domain_name*

  Domain name that can be assigned to a user in a particular subordinate organization. This is a multivalued parameter.

  The values for *available_domain_name* are a proper subset of the values given for the `sunAssignableDomains: <domain_name>` attribute and parameter. Whereas *domain_name* applies to the entire provider organization, *available_domain_name* applies to a single subordinate organization.

  In the "Shared Subordinate Organization" section of the `da.provider.skeleton.ldif` file, you will see the following attribute:

  ```
  sunAvailableDomainNames: <available_domain_name>
  ```

For each domain name you want this subordinate organization to inherit from the list of domain names in the provider organization's `sunAssignableDomains` attribute, add one instance of the `sunAvailableDomains` attribute and *available_domain_name* parameter. Only the domain names listed here can be assigned to the subordinate organization.

Example:

```
sunAvailableDomainNames: siroe.com
sunAvailableDomainNames: siroe.net
sunAvailableDomainNames: varrius.com
```

- *available_services*

  Service package available to a particular subordinate organization. This is a multivalued parameter.

  The service packages assigned to the subordinate organization are a subset of those assigned to the entire provider organization with the `sunIncludeServices` attribute.

  In the "Shared Subordinate Organization" section of the `da.provider.skeleton.ldif` file, you will see the following attribute:

  `sunAvailableServices: <available_services>`

  The format of the *available_services* parameter is

  service package name: count

  where *count* is an integer. If count is absent, the default value is an unlimited number.

  For each service package you want this subordinate organization to inherit from the service packages available in the provider organization's `sunIncludeServices` attribute, add one instance of the `sunAvailableServices` attribute and *available_services* parameter.

  Example:

  ```
  sunAvailableServices: gold:1500
  sunAvailableServices: platinum:2000
  sunAvailableServices: silver:5000
  ```

Parameters Defining the SPA

To create an SPA, edit the following parameters:

- *spa_uid*

  The user ID for the SPA user.

  Example:

  `uid: user1`

- *spa_password*

The password for the SPA user.

Example:

```
userPassword: x12P3&qrS
```

- *spa_firstname*

  The first name of the SPA user.

  Example:

  ```
  givenname: John
  ```

- *spa_lastname*

  The last name of the SPA user.

  Example:

  ```
  sn: Smith
  ```

- *spa_servicepackage*

  The service package assigned to the SPA user. For information about service packages, see "Service Packages" on page 31 in Chapter 1.

  Example:

  ```
  inetCos: platinum
  ```

- *spa_mailaddress*

  The mail address of the SPA user. The domain part of the mail address must be one of the domain values that replace the *available_domain_name* parameter. That is, it must be a domain that has been made available for use in the subordinate organization in which the SPA user resides. For more information, see "Parameters Defining the Provider and Subordinate Organization" on page 149.

  Example:

  ```
  mail: user1@siroe.com
  ```

For instructions in how to edit the custom service-provider template and install the information in your directory, see "Steps for Creating a Provider Organization and Service Provider Administrator" on page 153.

Steps for Creating a Provider Organization and Service Provider Administrator

You use an ldif file, `da.provider.skeleton.ldif`, to perform the following procedure.

▼ To create a provider organization and Service Provider Administrator

Steps

1. **Create a mail domain in the directory.**

   If you have not already done so, create a mail domain in your directory. The provider organization and its subordinate shared organizations will use this mail domain.

2. **Copy and rename the `da.provider.skeleton.ldif` file.**

   When you install Delegated Administrator, the `da.provider.skeleton.ldif` file is installed in the following directory:

   da_base`/lib/config-templates`

3. **Edit the following parameters in your copy of the `da.provider.skeleton.ldif` file. Replace the parameters with the correct values for your installation.**

   For definitions of the parameters, see "Information Needed to Create a Provider Organization, Subordinate Organization, and SPA" on page 149.

   Some parameters are used more than once in the ldif file. You must search for and replace all instances of each parameter.

   A few parameters represent values for multivalued attributes. You can copy and edit these parameters, together with their associated attribute names, to allow multiple instances of these attributes in your ldif file. Multivalued parameters are noted below.

   - `<ugldapbasedn>`
   - `<maildomain_dn>`
   - `<maildomain_dn_str>`
   - `<providerorg>`
   - `<servicepackage>` (multivalued)
   - `<domain_name>` (multivalued)
   - `<provider_sub_org>`
   - `<preferredmailhost>`
   - `<available_domain_name>` (multivalued)
   - `<available_services>` (multivalued)
   - `<spa_uid>`
   - `<spa_password>`
   - `<spa_firstname>`
   - `<spa_lastname>`
   - `<spa_servicepackage>`

- <spa_mailaddress>

  For definitions of the attributes associated with these parameters, see "Chapter 5: Communications Services Delegated Administrator Classes and Attributes (Schema 2)" and "Chapter 3: Messaging Server and Calendar Server Attributes" in the *Sun Java System Communications Services Schema Reference*.

4. **Use the LDAP directory tool `ldapmodify` to install the provider organization and SPA in the directory.**

   For example, you could run the following command:

   ```
   ldapmodify -D <directory manager> -w <password> \
   -f <da.provider.finished.ldif>
   ```

   where

   <directory manager> is the name of the Directory Server administrator.

   <password> is the password of the Directory Service administrator.

   <da.provider.finished.ldif> is the name of the edited ldif file to be installed as a new provider organization and SPA in the directory.

Custom Service-Provider Template

The template (da.provider.skeleton.ldif) contains parameters that you must modify to create a new provider organization and SPA.

The listing below shows the sections of the ldif file that have parameters. The listing does not include the entire file. Entries and ACIs required to support Access Manager are not included here.

You should only modify the parameters in the ldif file. Do not modify the sections of the file related to Access Manager.

da.provider.skeleton.ldif File (Relevant Sections)

```
#
# The following parameterized values must be replaced.
#
# <ugldapbasedn>          :: Root suffix for user/group data
# <maildomain_dn>         :: Complete dn of the mail domain underneath
#                            which the provider organization will be
#                            created.
# <maildomain_dn_str>     :: The maildomain dn with all ',' replaced
#                                      by '_'. E.g.
#                            dn --\> o=siroe.com,o=SharedDomainsRoot,
#                            o=Business,dc=red,dc=iplanet,dc=com
#                            dn_str --> o=siroe.com_o=SharedDomainsRoot_
```

```
#                              o=Business_dc=red_dc=iplanet_dc=com
# <providerorg>             : Organization value for provider node.
# <servicepackage>         :: One for each service package to include.
#                              All service packages in the system
#                              may be assigned by leaving this value empty.
# <domain_name>            :: One for each DNS name which may be assigned
#                              to a subordinate organization.
#                              These names form a proper subset (some or
#                              all) of the names listed in the <maildomain>
#                              organization's sunpreferreddomain
#                              and associateddomain attributes.
# <provider_sub_org>       :: Organization value for the shared subordinate
#                              organization in which the Provider
#                              Administrator resides.
# <preferredmailhost>      :: Name of the preferred mail host for the
#                              provider's subordinate organization.
# <available_domain_name> :: one for each DNS name that an organization
#                              allows an organization admin to use when
#                              creating a user's mail address.  This is
#                              a proper subset of the values given for
#                              <domain_name> (sunAssignableDomains attribute).
# <available_services>     :: One for each service packags available to an
#                              organization (sunAvailableServices attribute).
#                              These service packages form a proper subset
#                              of the ones assigned to a provider organization
#                              - <servicepackage> (sunIncludeServices
#                              attribute).  Form is
#                              <service package name>:<count>
#                              where count is an integer.  If count is absent
#                              then default is unlimited.
# <spa_uid>                :: The uid for the service provider administrator.
# <spa_password>           :: The password for the service provider
#                              administrator.
# <spa_firstname>          :: First name of the service provider
#                              administrator.
# <spa_lastname>           :: Last name of the service provider
#                              administrator.
# <spa_servicepackage>     :: Service package assigned to the service
#                              provider administrator.
# <spa_mailaddress>        :: The spa's mail address. The domain part of the
#                              mail address must be one of the values used for
#                              <available_domain_name>.
#


#
# Provider Organization
#
dn: o=<providerorg>,<maildomain_dn>
changetype: add
o: <providerorg>
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunmanagedorganization
objectClass: organization
```

```
objectClass: sunManagedProvider
sunAllowBusinessOrgType: full
sunAllowBusinessOrgType: shared
sunBusinessOrgBase: o=<providerorg>domainsroot,<ugldapbasedn>
sunIncludeServices: <servicepackage>
sunAssignableDomains: <domain_name>
sunAllowMultipleDomains: true
sunAllowOutsideAdmins: false
sunProviderOrgDN: o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Full Organizations node
#
dn: o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
o: <providerorg>DomainsRoot
objectClass: top
objectClass: organization
objectClass: sunmanagedorganization
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Provider Admin Role shared organizations
#
dn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Provider Admin Role full organizations
#
dn: cn=Provider Admin Role,o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
```

```
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Shared Subordinate Organization. Includes 1 user who is
# the Provider Administrator.
#
dn: o=<provider_sub_org>,=<providerorg>,<maildomain_dn>
changetype: add
preferredMailHost: <preferredmailhost>
sunNameSpaceUniqueAttrs: uid
o: <provider_sub_org>
objectClass: inetdomainauthinfo
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunnamespace
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunDelegatedOrganization
objectClass: sunMailOrganization
sunAvailableDomainNames: <available_domain_name>
sunAvailableServices: <available_services>
sunOrgType: shared
sunMaxUsers: -1
sunNumUsers: 1
sunMaxGroups: -1
sunNumGroups: 0
sunEnableGAB: true
sunAllowMultipleServices: true
inetDomainStatus: active
sunRegisteredServiceName: GroupMailService
sunRegisteredServiceName: DomainMailService
sunRegisteredServiceName: UserMailService
sunRegisteredServiceName: iPlanetAMAuthService
sunRegisteredServiceName: UserCalendarService
sunRegisteredServiceName: iPlanetAMAuthLDAPService
sunRegisteredServiceName: DomainCalendarService
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

dn: ou=People,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: People
objectClass: iplanet-am-managed-people-container
objectClass: organizationalUnit
objectClass: top

dn: ou=Groups,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: Groups
objectClass: iplanet-am-managed-group-container
objectClass: organizationalUnit
```

```
objectClass: top
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# User - provider administrator
#
dn: uid=<spa_uid>,ou=People,o=<provider_sub_org>,o=<providerorg>, \
        <maildomain_dn>
changetype: add
sn: <spa_lastname>
givenname: <spa_firstname>
cn:  <spa_firstname> <spa_lastname>
uid: <spa_uid>
iplanet-am-modifiable-by: cn=Top-level Admin Role,<ugldapbasedn>
objectClass: inetAdmin
objectClass: top
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: iPlanetPreferences
objectClass: person
objectClass: organizationalPerson
objectClass: inetuser
objectClass: inetOrgPerson
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: inetSubscriber
objectClass: userPresenceProfile
objectClass: icsCalendarUser
mailhost: <preferredmailhost>
mail: <spa_mailaddress>
maildeliveryoption: mailbox
mailuserstatus: active
inetCos: <spa_servicepackage>
inetUserStatus: Active
nsroledn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
userPassword: <spa_password>
```

Creating Shared and Full Subordinate Organizations

Once you have created a provider organization and an SPA, the SPA can create and manage both shared and full organizations subordinate to the provider organization. The SPA uses the Delegated Administrator console to accomplish these tasks.

The following task outlines the key steps in creating a shared organization or a full organization. This task does not describe how to enter all the information displayed when you create an organization with the Create New Organization wizard. For detailed descriptions of the Create New Organization wizard, see the Delegated Administrator console online help.

▼ To create a shared or full subordinate organization

Steps

1. **Launch the Delegated Administrator console.**
   Go to the following url:

   `http://`*host*`:`*port*`/da/DA/Login`

   where

   host is the Web container host machine

   port is the Web container port

   For example:

   `http://siroe.com:8080/da/DA/Login`

   The Delegated Administrator console log-in window appears.

2. **Log in to the Delegated Administrator console using the SPA login ID and password.**
   The preceding section, "Creating a Provider Organization and Service Provider Administrator" on page 146, describes how to create an SPA.

   The Service Provider Administrator page appears. The Organizations tab is selected by default. The page displays the organizations subordinate to the SPA's provider organization.

3. **Click New Organization.**
   The Create New Organization wizard appears. For details about entering and selecting information in the Create New Organization wizard, see the Delegated Administrator console online help.

4. **Enter information in the Organization Information panel and click Next.**
   The Contact Information panel appears.

5. **Enter information in the Contact Information panel and click Next.**
   The Account Information panel appears.

6. **Choose whether to create a shared organization or full organization.**
   In the Account Information panel, you determine whether the new organization will be shared or full.

A shared organization uses an existing domain shared with other organizations.

A full organization has its own unique domain.

- To create a shared organization, click the **Select from available domains** radio button.

  From the drop-down list, choose a domain.

  Note – When you create a shared organization, the Calendar service details are inherited from the existing parent domain. Therefore, you will not enter Calendar service information for the new organization. The Calendar Service Details panel will not appear in the Create New Organization wizard. Furthermore, after the shared organization is created, Calendar Service Details do not appear in the organization's Properties page.

- To create a full organization, click the **New domain** radio button.

  In the text box, enter a new mail domain name. For example: `siroe.com`.

  If you wish, enter alias names for the new domain in the **Alias Names for the New Domain** text box.

7. **Enter information in the remaining panels of the Create New Organization wizard.**

   For details about these panels, see the Delegated Administrator console online help.

Sample Service-Provider Organization Data

You can choose to install sample organization data (defined in an ldif file) in your directory when you run the Delegated Administrator configuration program, `config-commda`. (When you run the configuration program, select **Load sample organizations** in the **Service Package and Organization Samples** panel.) The configuration program adds the `da.sample.data.ldif` file to the LDAP directory tree.

This ldif file is meant to be used as an example, not as a template for creating your own provider organizations. To create a new provider organization, see "Information Needed to Create a Provider Organization, Subordinate Organization, and SPA" on page 149.

Organizations Provided by the Sample Data

Figure A–1shows a logical view of the organizational structure provided by the sample ldif file. (Figure A–1 adds a shared organization, HIJ, that does not exist in the file.)

The sample ldif file contains the following organizations under the root-suffix nodes:

- VIS provider organization. The following organizations are managed by the SPA for the VIS provider organization:
  - SESTA, a full organization. The SESTA organization has its own domain, `sesta.com`.
  - DEF, a shared organization. The DEF organization uses the shared domain, `siroe.com`.
- ESG provider organization. No subordinate organizations are defined for this provider organization.

The ldif file defines the following administrator roles for these organizations:

- An SPA for the VIS provider organization (`user2@abc.com`)
- An SPA for the ESG provider organization (`user2_def`)
- An OA for the SESTA organization (`user1@abc.com`)
- An OA for the DEF organization (`user1_def`)

Logical Hierarchy and the Directory Information Tree

In a three-tiered directory hierarchy, a Directory Information Tree (DIT) does not look exactly like the logical view shown in Figure A–1. Organizations are implemented in the DIT in a somewhat different hierarchy.

For example, in a DIT, full domains must reside directly under the root suffix. Therefore, domain nodes are added under the root suffix to store LDAP information for shared domains (used by shared organizations) and for full organizations (which have their own domains).

Sample Organization Data: Directory Information Tree View

Figure A–3 shows a Directory Information Tree (DIT) view of the sample organization data.

The example shown in Figure A–3, like the logical view shown in Figure A–1, contains the following organizations:

- VIS and ESG (provider organizations)
- DEF, a shared organization subordinate to the VIS provider organization

- SESTA, a full organization subordinate to the VIS provider organization

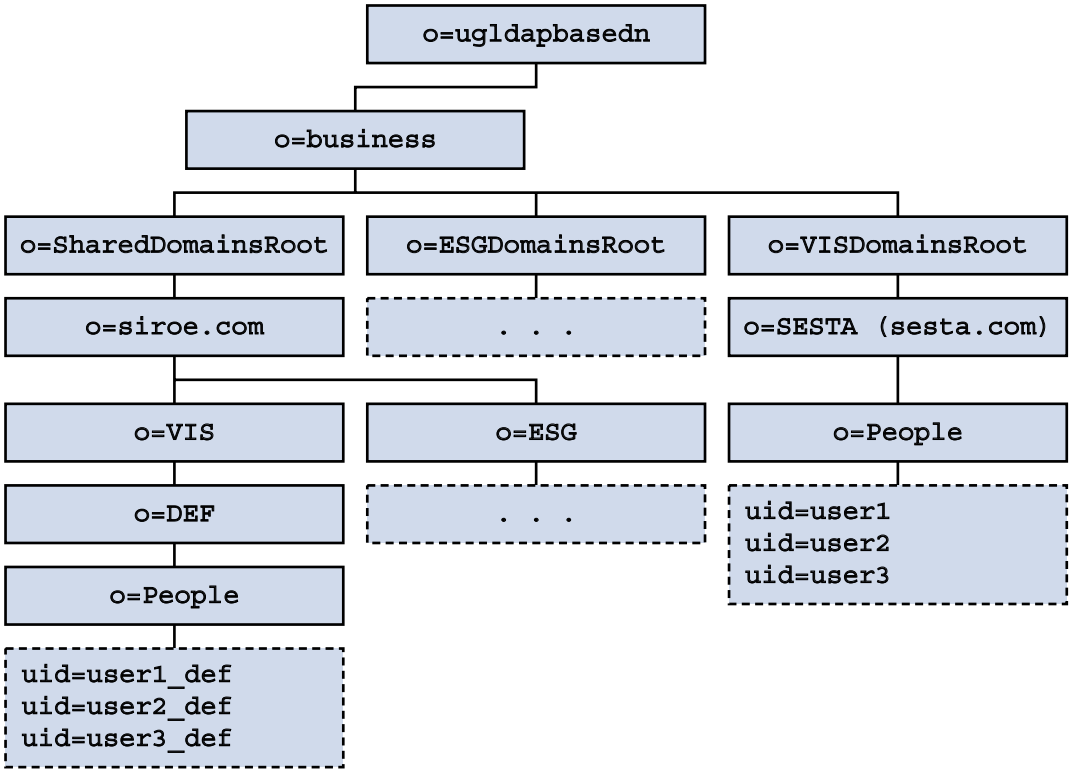

FIGURE A–3 Sample Organization Data: Directory Information Tree View

Nodes in the Sample Directory Information Tree

The nodes in the sample organization file (`da.sample.data.ldif`) are as follows:

- *ugldapbasedn* - This parameter represents the root suffix.
- `o=business` - A node that contains all businesses in the directory.
- `o=SharedDomainsRoot` - A node needed to contain the domains used by shared organizations.

  In this Directory Information Tree, shared organizations subordinate to different service provider organizations can use the same shared domain. This can be done because both the provider organizations have nodes under the `SharedDomainsRoot` node.
- `o=ESGDomainsRoot` and `o=VISDomainsRoot` - These nodes contain any full organizations that are subordinate to the ESG and VIS provider organizations.

Each provider organization that manages full organizations must have a node at this level (under the root suffix).

Multiple full organizations, each with its own domain, can exist under `ESGDomainsRoot` or `VISDomainsRoot`.

- `o=siroe.com` - The shared domain. It is used by the shared organization, DEF.
- `o=VIS` and `o=ESG` - These provider organization nodes contain any shared organizations subordinate to the VIS and ESG provider organizations.

  For example, the shared organization, DEF, is subordinate to the VIS provider organization.
- `o=SESTA` - The full organization. It has its own domain, `sesta.com`.
- `o=DEF` - The shared organization. It uses the domain `siroe.com`.
- `ou=people` - The standard LDAP organization unit required for containing users.

User DNs in the Sample Directory Information Tree

Some user DNs in the sample organization file shown in Figure A–3 are as follows:

- For the user named `user1_def`, who belongs to the DEF organization:

  `dn: uid=user1_def,ou=People,o=DEF,o=VIS,o=siroe.com,`
  `o=SharedDomainsRoot,o=Business,`*`ugldapbasedn`*
- For the user named `user1`, who belongs to the SESTA organization:

  `dn: uid=user1,ou=People,o=SESTA,o=VISDomainsRoot,`
  `o=Business,`*`ugldapbasedn`*

APPENDIX **B**

Attribute Values and Calendar Time Zones

Attribute Values

The attributes listed in Table B–1 can be used with the `-P` option for the following commands: "commadmin domain create" on page 103 and "commadmin domain modify" on page 107. The attributes are either bit oriented attributes or multivalued attributes.

TABLE B–1 Attributes for `-P` Option

Attribute	Value	Description
`createLowerCase`	yes/no	Specifies whether or not a lowercase calendar is to be created for a new user. Also, when looking up calendar, whether to lookup lowercase calendars or not.
`filterPrivateEvents`	yes/no	Specifies whether or not to filter the private or confidential events when querying the server
`fbIncludeDefCal`	yes/no	Specifies whether or not user's default calendar is included in user's `freebusy-calendar-list`.
`subIncludeDefCal`	yes/no	Specifies whether or not the user's default calendar is to be included in user's `subscribed-calendar-list` or not
`resourceDefaultAcl`	yes/no	Specifies whether to use the default ACL for resource calendars.
`calmasterCred`	string	Credentials of user specified as the Calendar Server administrator.

TABLE B–1 Attributes for `-P` Option *(Continued)*

Attribute	Value	Description
`calmasterUid`	string	`service.admin.calmaster.userid`
`calmasterAccessOverride`	yes/no	Specifies whether or not the Calendar Server administrator can override access control.
`setPublicRead`	yes/no	Sets the default user calendars to public read or private write. If `no` is selected, sets user calendars to private read or private write.
`uiBaseUrl`	string	BaseServerAddress, for example, `"https://proxyserver/"`
`uiConfigFile`	string	Configuration file for the user interface.
`uiProxyUrl`	string	Proxy Server Address to append in the HTML user interfaces' JavaScript file. For example, `https://web_portal.iplanet.com/`
`domainAccess`	string	Access control string for domain. Used in cross domain searching.
`uiAllowAnyone`	yes/no	Specifies whether or not to allow the HTML user interface to show and use the "`Everybody`" ACL.
`allowProxyLogin`	yes/no	Specify whether to allow proxy login

The attributes listed in Table B–2 can be used with the `-R` option for the following commands: "commadmin domain create" on page 103 and "commadmin domain modify" on page 107. The attributes have a bit-oriented value.

For information about WCAP and the WCAP `set-userprefs` command, see the *Sun Java System Calendar Server Programmer's Manual*.

TABLE B–2 Attributes for `-R` Option

Attribute	Value	Description
`allowUserDoubleBook`	bit 8	Allows this calendar to be scheduled more than once for the same time slot.
`allowResourceDoubleBook`	bit 9	allows this resource calendar to be scheduled more than once for the same time slot.

TABLE B–2 Attributes for `-R` Option *(Continued)*

Attribute	Value	Description
`allowModifyUserPreferences`	bit 4	Allows Calendar Server administrator `get/set userprefs` should be obtained from WCAP for users.
`allowModifyPassword`	bit 5	Allows users to change their password via this server.
`allowCalendarCreation`	bit 0	Allows calendars to be created.
`allowCalendarDeletion`	bit 1	Allows calendars to be deleted.
`allowPublicWritableCalendars`	bit 2	Allows users to own publicly writable calendars.
`allowSetCn`	bit 10	Allows `set-userprefs.wcap` to modify the `cn` user preference.
`allowSetGivenName`	bit 11	Allows `set_userprefs.wcap` to modify the `givenname` user preference.
`allowSetGivenMail`	bit 12	Allows `set_userprefs.wcap` to modify the `mail` user preference.
`allowSetPrefLang`	bit 13	Allows `set_userprefs.wcap` to modify the `preferredlanguage` user preference.
`allowSetSn`	bit 14	Allows `set-userprefs.wcap` to modify the `sn` user preference.

Calendar Time Zone Strings

The following time zone strings can be used with the `-T` time zone option for the "commadmin domain create" on page 103, "commadmin domain modify" on page 107, "commadmin resource create" on page 122, "commadmin resource modify" on page 126, "commadmin user create" on page 129, and "commadmin user modify" on page 134 commands:

You also can add a new time zone and set it as the default time zone. For details, see "Adding a New Calendar Time Zone" on page 92.

- Africa/Cairo
- Africa/Casablanca
- Africa/Johannesburg
- Africa/Lagos
- Africa/Tripoli

- Africa/Windhoek
- America/Adak
- America/Anchorage
- America/Buenos_Aires
- America/Caracas
- America/Chicago
- America/Costa_Rica
- America/Cuiaba
- America/Denver
- America/Godthab
- America/Grand_Turk
- America/Halifax
- America/Havana
- America/Indianapolis
- America/Los_Angeles
- America/Miquelon
- America/New_York
- America/Phoenix
- America/Port-au-Prince
- America/Santiago
- America/Sao_Paulo
- America/St_Johns
- Asia/Alma-Ata
- Asia/Amman
- Asia/Anadyr
- Asia/Aqtau
- Asia/Aqtobe
- Asia/Baku
- Asia/Bangkok
- Asia/Beirut
- Asia/Bishkek
- Asia/Calcutta
- Asia/Dacca
- Asia/Irkutsk
- Asia/Jerusalem
- Asia/Kabul
- Asia/Kamchatka
- Asia/Karachi
- Asia/Katmandu
- Asia/Krasnoyarsk
- Asia/Magadan
- Asia/Novosibirsk
- Asia/Rangoon
- Asia/Riyadh
- Asia/Shanghai
- Asia/Tokyo
- Asia/Ulan_Bator
- Asia/Vladivostok

- Asia/Yakutsk
- Asia/Yekaterinburg
- Asia/Yerevan
- Atlantic/Azores
- Atlantic/Cape_Verde
- Atlantic/South_Georgia
- Atlantic/Stanley
- Australia/Adelaide
- Australia/Brisbane
- Australia/Darwin
- Australia/Hobart
- Australia/Lord_Howe
- Australia/Sydney
- Europe/Bucharest
- Europe/Istanbul
- Europe/London
- Europe/Minsk
- Europe/Moscow
- Europe/Paris
- Europe/Riga
- Europe/Samara
- Europe/Simferopol
- Europe/Warsaw
- Pacific/Apia
- Pacific/Auckland
- Pacific/Chatham
- Pacific/Easter
- Pacific/Fiji
- Pacific/Gambier
- Pacific/Guadalcanal
- Pacific/Honolulu
- Pacific/Kiritimati
- Pacific/Marquesas
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pitcairn
- Pacific/Rarotonga
- Pacific/Tongatapu

APPENDIX C

Debugging Delegated Administrator

You can obtain log information for Delegated Administrator by examining log files generated by the Delegated Administrator components, by the Web container to which Delegated Administrator has been deployed, and by Directory Server and Access Manager.

This appendix includes the following topics:

Debugging the Command-Line Utilities

To debug the Delegated Administrator utility (`commadmin`), you can print debug messages in the client by using the `-v` option with the `commadmin` command.

Delegated Administrator Console Log

The Delegated Administrator console creates a runtime log file:

- Default log file name: `da.log`
- Default location: `/opt/SUNWcomm/log`

You can specify your own log file by editing a log properties file:

- Log properties file name: `logger.properties`
- Default location:

```
/var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
comm/da/resources
```

You can change the following properties in the logger.properties file:

- `da.logging.enable=yes` or `no`

  where `yes` enables logging and `no` disables logging.

  By default, logging is disabled. To turn on logging, you must set this value to `yes`.
- `da.log.file=`*full pathname*

  specifies the directory and file to which logging statements are written. This property changes `da.log` to a file name and location you specify.

Delegated Administrator Server Log

You can create a Delegated Administrator server log that contains debug statements generated by the Delegated Administrator servlets installed on the Web container.

To do so, you enable a Debug servlet to log debug messages from the Delegated Administrator servlet execution. You can turn on the Debug servlet through your browser by going to the following url path:

`http://`*machine name*`:`*port*`/commcli/debug?op=set&state=all&package=all&filename=`*full path*

where

- *machine name* is the name of the machine where Delegated Administrator server is running.
- *full path* is the full directory path and name of the log to which messages will be written.

For example:

```
http://abc.red.iplanet.com:8008/commcli/debug?op= \
set&state=all&package=all&filename=/tmp/debug.log
```

The preceding url would log Debug servlet messages to the following path and file:

`/tmp/debug.log`

Whenever you restart the Web container, you must turn on the Debug servlet.

Web Container Server Logs

You can debug Delegated Administrator further by examining the server logs generated by your Web container.

Web Server

Web Server maintains access and error logs, located in the following path:

/web_server_base`/https-`*machine name*`/logs`

where

- *web_server_base* is the path where Web Server software is installed.
- *machine name* is the name of the machine where Web Server is running.

Application Server 7.*x*

Application Server 7.*x* maintains access and error logs, located in the following path:

/application_server7_base`/domains/domain1/server1/logs`

where

- *application_server7_base* is the path where Application Server 7.*x* software is installed.

Application Server 8.*x*

Application Server 8.*x* maintains access and error logs, located in the following paths.

Server log:

/application_server8_base`/domains/domain1/logs`

Access log:

/application_server8_base`/domains/domain1/logs/access/server_access_log`

where

- *application_server8_base* is the path where Application Server 8.*x* software is installed.

Directory Server and Access Manager Logs

You can debug Delegated Administrator further by examining the logs generated by Directory Server and Access Manager.

Directory Server

Directory Server maintains access and error logs, located in the following path:

`/var/opt/mps/serverroot/slapd-`*hostname*`/logs`

where

- *hostname*is the name of the machine where Directory Server is running.

Access Manager

Access Manager maintains log files in the following paths:

`/var/opt/SUNWam/debug`

The preceding path contains the `amProfile` and `amAuth` logs.

`/var/opt/SUNWam/logs`

The preceding path contains the `amAdmin.access` and `amAdmin.error` logs.

APPENDIX **D**

Delegated Administrator Performance Tuning

The following topics describe how you can tune Delegated Administrator and related software to improve Delegated Administrator performance:

In addition to following the guidelines described in this appendix, you can improve Directory Server performance by consolidating and reducing the number of default ACIs in the directory. For information, see Appendix E.

Speed Up Display of Users, Groups, and Organizations

If an organization contains many users, the Delegated Administrator console may take time to display the User list page. If you try to create or edit a user while the page is still loading the existing users, an error occurs. Do not click any buttons or links until the page is ready.

Similarly, it can take time to open the Organization page or Group page if your directory contains many organizations or groups.

If these pages take too long to load, you can set wild-card search properties to a sufficiently low value to allow the pages to load quickly.

The properties are

jdapi-wildusersearchmaxresults	Search property for users.
jdapi-groupsmaxsearchresults	Search property for groups.

jdapi-wildorgsearchmaxresults Search property for organizations.

The wild-card search property limits are as follows:

`-1`	Return all results. (Display all users, groups, or organizations.) `-1` is the default value.
`0`	Do not search. (Display no users, groups, or organizations.)
n `(>0)`	Return *n* (the specified number of results).

▼ To display the User page more quickly

Steps

1. **Open the `resource.properties` file.**

   The `resource.properties` file is located in the following directory:

   da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. **Set the value of `jdapi-wildusersearchmaxresults` to a low value. For example:**

   ```
   jdapi-wildusersearchmaxresults=50
   ```

   Alternatively, you can set the value to `0` to display no users. In the Delegated Administrator console, use the **Search** drop-down list to search for specified users.

▼ To display the Group page more quickly

Steps

1. **Open the `resource.properties` file.**

   The `resource.properties` file is located in the following directory:

   da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. **Set the value of `jdapi-groupsmaxsearchresults` to a low value. For example:**

   ```
   jdapi-groupsmaxsearchresults=50
   ```

   Alternatively, you can set the value to `0` to display no groups. In the Delegated Administrator console, use the **Search** drop-down list to search for specified groups.

▼ To display the Organization page more quickly

Steps

1. **Open the `resource.properties` file.**

   The `resource.properties` file is located in the following directory:

   da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. **Set the value of `jdapi-wildorgsearchmaxresults` to a low value. For example:**

   ```
   jdapi-wildusersearchmaxresults=10
   ```

   Alternatively, you can set the value to `0` to display no organizations. In the Delegated Administrator console, use the **Search** drop-down list to search for specified organizations.

Increase JVM Heap Size

To improve the performance of common Delegated Administrator functions such as displaying pages and performing searches, you can increase the Java Virtual Machine (JVM) heap size used by the Web container to which Delegated Administrator is deployed. When the Web container's JVM heap size is too small, performance can be affected.

The JVM heap size is set by the following JVM option:

`-Xmx<`*n*`>m`

where <*n*> is the heap size in megabytes.

Typically, <*n*> is set to `256m`.

The following tasks outline how to set a higher JVM heap size for Web Server and Application Server.

▼ To increase the Web Server JVM heap size

Steps

1. **Log in to the Web Server Administration Server.**
2. **Under the Java tab, select JVM Options.**
3. **Edit the `-Xmx256m` option.**
   This option sets the JVM heap size.
4. **Set the `-Xmx256m` option to a higher value, such as `Xmx1024m`.**
5. **Save the new setting.**

More Information

Web Server Documentation

See the *Sun Java System Web Server Administration Guide* and *Web Server Performance Tuning, Sizing, and Scaling Guide* for more information about using the Web Server Administration Server and setting JVM options.

▼ To increase the Application Server JVM heap size

Steps

1. **Log in to the Application Server Administration Server.**
2. **Navigate to the JVM options.**
3. **Edit the `-Xmx256m` option.**
   This option sets the JVM heap size.
4. **Set the `-Xmx256m` option to a higher value, such as `Xmx1024m`.**
5. **Save the new setting.**

More Information

Application Server Documentation

For more information about using the Application Server Administration Server and setting JVM options, go to the *Sun Java System Application Server Documentation Center* and select "JVM Advanced Settings." Alternatively, see "Tuning the Java Runtime System" in the *Sun Java System Application Server Enterprise Edition 8.1 2005Q4 Performance Tuning Guide*

Raise Directory Server Indexing Threshold

To improve performance of Delegated Administrator functions such as searching and displaying users, you can increase the threshold for indexes used by Directory Server to search the directory.

When Directory Server searches a large number of LDAP objects, if the threshold is set to a low value, the index might run out of space before the search is completed. The remainder of the search is performed without indexing, which slows down the search operation.

Caution – Perform this operation only if you are an experienced Directory Server administrator.

To set the index threshold to a higher value, change the value of the `nssldap-allidsthreshold` option in the `dse.ldif` file

This option might be set to a value such as the following:

```
nssldap-allidsthreshold: 4000
```

Set `nssldap-allidsthreshold` to a higher value. For example:

```
nssldap-allidsthreshold: 200000
```

For more information about the All IDs Threshold, see "Managing Indexes" in "Indexing Directory Data" in the *Sun Java System Directory Server Administration Guide*. For a definition of the `nssldap-allidsthreshold` option, see "Database Configuration Attributes" in "Server Configuration Reference" in the *Sun Java System Directory Server Administration Reference*.

APPENDIX **E**

Consolidating ACIs for Directory Server Performance

This appendix describes the following topics:

Introduction

When you install Access Manager with Messaging Server and use an LDAP Schema 2 directory, a large number of Access Control Instructions (ACIs) initially are installed in the directory. Many default ACIs are not needed or used by Messaging Server.

The need to check these ACIs at runtime can affect the performance of Directory Server, which can, in turn, affect the performance of Messaging Server look-ups and other directory operations.

You can improve the performance of the Directory Server by consolidating and reducing the number of default ACIs in the directory. Consolidating the ACIs also makes them easier to manage.

The approach to reducing ACIs is as follows:

- Combine, optimize, and simplify redundant ACIs
- Modify ACIs to use a simpler, more efficient syntax
- Consolidate ACIs with other ACIs (at the root suffix)
- Eliminate unused ACIs
- For directories with many organizations, allows organization ACIs to be removed on individual organization nodes.

This appendix first describes how to use an ldif file (`replacment.acis.ldif`) to consolidate ACIs at the root suffix and remove unused ACIs from the directory. For details, see "Consolidating and Removing ACIs" on page 182, below.

Next, the appendix analyzes each ACI and recommends a method for handling it: removing it, revising it to make it more efficient, or rewriting it.

Note the following constraints in these recommendations:

- There is no end-user access for the Directory console
- There is no end-user access to the Access Manager console.

Given these constraints, you must determine for yourself (according to the requirements of your installation) whether you can use the ldif file to consolidate and remove ACIs, or whether you need to retain certain ACIs as they now exist in the directory.

For more information, see "Analysis of the Existing ACIs" on page 187, later in this appendix.

Next, this appendix describes the ACIs that are consolidated by the `replacement.acis.ldif` file. It lists the existing ACIs before they are consolidated and the modified ACIs after they are consolidated. For more information, see "Analysis of How ACIs Are Consolidated" on page 203, later in this appendix.

Finally, the appendix lists the ACIs discarded by the `replacement.acis.ldif`. For more information, see "List of Unused ACIs to be Discarded" on page 210, later in this appendix.

Consolidating and Removing ACIs

The ldif file listed in this section, `replacement.acis.ldif`, installs consolidated ACIs at the root suffix and deletes unused ACIs from the directory. This ldif file is provided by Delegated Administrator, located in the following directory:

da_base`/lib/config-templates`

When you apply the `replacement.acis.ldif` file to the directory (with `ldapmodify`), the `ldapmodify` command removes all instances of the `aci` attribute at the root suffix and replaces these ACIs with the ACIs in the `replacement.acis.ldif` file.

Thus, this procedure will initially remove *all* ACIs from the root suffix and then replace them with the set of ACIs listed below. If the directory contains ACIs generated by another application such as Portal Server, you should save those ACIs to a file and reapply them to the directory after you apply the `replacement.acis.ldif` file.

For instructions in using this ldif file to clean up your ACIs, see "Steps for Replacing ACIs" on page 185.

replacement.acis.ldif File

```
dn: $rootSuffix
changetype: modify
replace: aci
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator";
   allow (all)
   userdn="ldap:///uid=admin,ou=Administrators,ou=TopologyManagement,
o=NetscapeRoot";)
aci: (target="ldap:///$rootSuffix")
  (targetfilter=(!(objectclass=sunServiceComponent)))
  (targetattr != "userPassword||passwordHistory
   ||passwordExpirationTime||passwordExpWarned||passwordRetryCount
  ||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
  (version 3.0; acl "anonymous access rights";
   allow (read,search,compare)
   userdn = "ldap:///anyone"; )
aci: (targetattr != "nsroledn||aci||nsLookThroughLimit||nsSizeLimit
  ||nsTimeLimit||nsIdleTimeout||passwordPolicySubentry||passwordExpiration
    Time
  ||passwordExpWarned||passwordRetryCount||retryCountResetTime
  ||accountUnlockTime||passwordHistory||passwordAllowChangeTime||uid||mem
    berOf
  ||objectclass||inetuserstatus||ou||owner||mail||mailuserstatus
  ||memberOfManagedGroup||mailQuota||mailMsgQuota||mailhost
  ||mailAllowedServiceAccess||inetCOS||mailSMTPSubmitChannel")
  (version 3.0; acl "Allow self entry modification";
  allow (write)
  userdn ="ldap:///self";)
aci: (targetattr != " aci || nsLookThroughLimit || nsSizeLimit
  || nsTimeLimit|| nsIdleTimeout")
  (version 3.0; acl "Allow self entry read search";
  allow(write)
  userdn ="ldap:///self";)
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Proxy user rights";
  allow (proxy)
  userdn = "ldap:///cn=puser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS special dsame user rights for all under the root
   suffix";
  allow (all)
  userdn = "ldap:///cn=dsameuser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
```

```
  (version 3.0; acl "S1IS special ldap auth user rights";
  allow (read,search)
  userdn = "ldap:///cn=amldapuser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Top-level admin rights";
  allow (all)
  roledn = "ldap:///cn=Top-level Admin Role,
  $rootSuffix"; )
aci: (targetattr="*")
  (version 3.0; acl "Messaging Server End User Administrator Read Only
   Access";
  allow (read,search)
  groupdn="ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr="objectclass || mailalternateaddress || Mailautoreplymode
   || mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
   || mailforwardingaddress || mailAutoReplyTimeout
   || mailautoreplytextinternal
   || mailautoreplytext || vacationEndDate || vacationStartDate
   || mailautoreplysubject || maxPabEntries || mailMessageStore
   || mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
   || sunUCTimeFormat || mailuserstatus || maildomainstatus")
  (version 3.0; acl "Messaging Server End User Administrator All Access";
  allow (all)
  groupdn = "ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr = "*")
  (version 3.0;acl "Allow Read-Only Access";
  allow (read,search,compare)
  groupdn = "ldap:///cn=Read-Only,ou=Groups,
  $rootSuffix";)
aci: (target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Organization Admin Role access deny";
  deny (write,add,delete,compare,proxy)
  roledn = "ldap:///cn=Organization Admin Role,($dn),
  $rootSuffix";)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "Organization Admin Role access allow read";
  allow(read,search)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix" ;)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
  (entrydn=($dn),$rootSuffix))))
  ( targetattr = "*")
  (version 3.0; acl "S1IS Organization Admin Role access allow";
  allow (all)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix";)
```

Steps for Replacing ACIs

Before You Begin

Before you begin this procedure, we recommend that you examine the existing ACIs in your directory. You should determine whether you might need to keep any ACIs that would be deleted by the procedure.

This procedure will initially remove *all* ACIs from the root suffix and then replace them with the set of ACIs listed below. If the directory contains ACIs generated by applications other than Messaging Server, you should save those ACIs to a file and reapply them to the directory after you apply the `replacement.acis.ldif` file.

To help you analyze existing ACIs generated by Access Manager and Messaging Server, see the following sections later in this appendix:

- "Analysis of the Existing ACIs" on page 187
- "Analysis of How ACIs Are Consolidated" on page 203
- "List of Unused ACIs to be Discarded" on page 210

Replacing ACIs

The following procedure describes how to consolidate ACIS in the root suffix and remove unused ACIs.

▼ To replace ACIs

Steps

1. **Save your existing ACIs currently on the root suffix.**

   You can use the `ldapsearch` command, as in the following example:

   ```
   ldapsearch -D "cn=Directory Manager" -w <password> -s base -b
   <$rootSuffix> aci=* aci ><filename>
   ```

   where

   `<password>` is the password of the Directory Server administrator.

   `<$rootSuffix>` is your root suffix, such as `o=usergroup`.

   `<filename>` is the name of the file into which the saved ACIs will be written.

2. **Copy and rename the `replacement.acis.ldif` file.**

   When you install Delegated Administrator, the `replacement.acis.ldif` file is installed in the following directory:

da_base/lib/config-templates

3. **Edit the `$rootSuffix` entries in your copy of the `replacement.acis.ldif` file.**

   Change the root suffix parameter, $rootSuffix, to your root suffix (such as `o=usergroup`). The $rootSuffix parameter appears multiple times in the ldif file; each instance must be replaced.

4. **Use the LDAP directory tool `ldapmodify` to replace the ACIs.**

   For example, you could run the following command:

   ```
   ldapmodify -D <directory manager> -w <password> -f
   <replacement.acis.finished.ldif>
   ```

   where

   `<directory manager>` is the name of the Directory Server administrator.

   `<password>` is the password of the Directory Service administrator.

   `<replacement.acis.finished.ldif>` is the name of the edited ldif file that consolidates and removes ACIs in the directory.

Eliminating Dynamic Organization ACIs

When you use the Delegated Administrator console to create an organization, a group of ACIs is created on the organization node.

The replacement ACIs installed in the preceding procedure eliminate the need for these per-organization ACIs. You can prevent the creation of the per-organization ACIs by using the Access Manager console.

▼ To eliminate dynamic organization ACIs

Steps

1. **Log in to the AM console as `amadmin`.**

   The AM console is located at the following url:

   `http://<`*machine name*`>:<`*port*`>/amconsole`

   where

   <*machine name*> is machine where Access Manager is running

   <*port*> is the port

2. **Select the Service Configuration tab.**

   By default, the Administration configuration page is displayed.

3. **In the right side of the console, scroll down to Dynamic Administrative Role ACIs.**
4. **Select and delete all ACIs in the text box for Dynamic Administrative Role ACIs.**
5. **Save the edited settings.**

Analysis of the Existing ACIs

The listing in this section shows the ACIs installed in the directory when you install Access Manager and Messaging Server. It also describes the function of each ACI and recommends whether an ACI can be retained, consolidated, or discarded.

The ACIs are divided into the following categories:

Root Suffix

```
dn: $rootSuffix
#
# consolidate
#
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry
|| passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy state
attributes";
```

```
allow (write)
userdn ="ldap:///self";)
```

Action: Consolidate.

There is no requirement for self access to this suffix. This ACI is duplicated; it can be incorporated into the self ACIs on the root suffix.

```
#
# retain
#
aci:
(targetattr = "*")
(version 3.0; acl "Configuration Administrator";
allow (all)
userdn = "ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement,o=NetscapeRoot";)
```

Action: Retain.

This is the "admin" user who would authenticate via Pass-Through Authentication to the `slapd-config` instance. If all configuration is to be performed as Directory Manager, using comm and line utilities, this ACI is not required. On the chance that someone needs to authenticate to the console as this user, this ACI can be kept here. Similar ACIs can be removed.

```
#
# discard
#
aci:
(targetattr ="*")
(version 3.0;acl "Configuration Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot");)
```

Action: Discard on all DB back-ends.

This is the "Configuration Administrators" group that would have privileges if the console were being used to delegate server-administration privileges.

```
#
# discard
```

```
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)
```

Action: Discard on all DB back-ends.

This is the general “Directory Administrators” group privilege definition.

```
#
# discard
#
aci:
(targetattr = “*”)
(version 3.0; acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server,
cn=Server Group, cn=whater.red.iplanet.com, ou=red.iplanet.com,
o=NetscapeRoot”;)
```

Action: Discard on all DB back-ends.

This is a Console/Administration server-related group privilege definition.

Access Manager

```
# retain
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Proxy user rights”;
allow (proxy)
userdn = “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”; )
```

Action: Retain.

This ACI grants access to a system user for Access Manager.

```
#
# retain
```

```
#
aci:
 (target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix";
allow (all)
userdn = "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix"; )
```

Action: Retain.

This ACI grants access to a system user for Access Manager.

```
#
# retain
#
aci:
(target="ldap:///$rootSuffix")(targetattr="*")|
(version 3.0;acl "S1IS special ldap auth user rights";
allow (read,search)
userdn = "ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix"; )
```

Action: Retain.

This ACI grants access to a system user for Access Manager.

```
#
# discard
#
aci:
(target="ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix")
(targetattr = "*")
(version 3.0;
acl "S1IS special ldap auth user modify right";
deny (write)
roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI prevents the Top-Level Administrator (TLA) from modifying the `amldapuser` account.

```
#
# retain
```

```
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all)
roledn = "ldap:///cn=Top-level Admin Role,$rootSuffix"; )
```

Action: Retain.

This ACI grants access to the Top-Level Administrator role.

```
#
# discard
#
aci:
(targetattr="iplanet-am-saml-user || iplanet-am-saml-password")
(targetfilter="(objectclass=iplanet-am-saml-service)")
(version 3.0; acl "S1IS Right to modify saml user and password";
deny (all)
(roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix")
AND (userdn != "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix")
AND (userdn != "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"); )
```

Action: Discard.

This ACI protects SAML-related attributes.

Top-level Help Desk Admin Role

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

Action: Discard.

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

Action: Discard.

Top-level Policy Admin Role

```
#
# discard
#
aci:
target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Top-level Policy Admin role.

```
#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access Auth Service
deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Top-level Policy Admin role.

```
#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Top-level Policy Admin role.

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter="(objectclass=sunismanagedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Top-level Policy Admin role.

AM Self

```
#
# consolidate
#
aci:
(targetattr = "*")
(version 3.0;
acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)
```

Action: Consolidate into a single self-write ACI. The explicit deny is not required, since end users do not have permission to delete any entry, including themselves.

This is one of several ACIs that set self-privileges. The explicit deny prevents any entry from deleting itself.

```
#
# consolidate
#
aci:
(targetattr = "objectclass || inetuserstatus
|| iplanet-am-user-login-status
|| iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || iplanet-am-user-account-life
|| iplanet-am-session-max-session-time || iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)
```

Action: Consolidate into a single self-write ACI.

This is one of several ACIs that set self-write privileges.

```
#
# consolidate
#
aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
|| nsLookThroughLimit || nsSizeLimit || nsTimeLimit || nsIdleTimeout
|| memberOf || iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except for nsroledn,
aci, and resource limit attributes";
allow (write)
userdn ="ldap:///self";)
```

Action: Consolidate into a single self-write ACI.

This is one of several ACIs that set privileges.

```
#
# consolidate
#
aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; acl "S1IS Allow self entry read search except for nsroledn,
aci, resource limit and web agent policy attributes";
allow (read,search)
userdn ="ldap:///self";)
```

Action: Consolidate into a single self-write ACI.

This is one of several ACIs that set self-write privileges.

AM Anonymous

```
#
# consolidate
#
aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*")
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

Action: Consolidate into a single anonymous ACI.

This is one of several ACIs that grant anonymous privileges.

```
#
# consolidate
#
aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

Action: Consolidate into a single anonymous ACI.

This is one of several ACIs that grant anonymous privileges.

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

Action: Discard.

This ACI prevents any user (other than the `rootdn`) from deleting the default organization.

```
#
# discard
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

Action: Discard.

This ACI prevents any user (other than the `rootdn`) from deleting the Top-level Administrator role.

AM Deny Write Access

```
#
# discard
#
aci: (targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn ="ldap:///cn=Deny Write Access,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Deny Write Access Role.

AM Container Admin Role

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Container Admin Role.

```
#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Container Admin Role.

```
#
# discard
#
aci:
 (target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
```

```
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Group and People Container Admin Role.

Organization Help Desk

```
#
# discard
#
aci: (extra verses dreambig)
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Organization Help Desk Admin Role.

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
```

```
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

Action: Discard.

This ACI pertains to the Organization Help Desk Admin Role.

AM Organization Admin Role

```
#
# consolidate
#
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn ="ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

Action: Consolidate.

```
#
# consolidate
#
aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)
```

Action: Consolidate.

This ACI pertains to the Organization Admin Role.

```
#
# consolidate
#
aci: (missing)
```

```
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

Action: Consolidate.

This ACI pertains to the Organization Admin Role.

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

Action: Consolidate.

This ACI pertains to the Organization Admin Role.

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox ||
postalCode
|| registeredaddress || street || l || st || telephonenumber
||maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

Action: Consolidate.

This ACI pertains to the Organization Admin Role.

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

Action: Consolidate.

AM Miscellaneous

```
#
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

Action: Discard.

Discarding this ACI disables the associated privileges to the attribute `iplanet-am-modifiable-by`.

Messaging Server

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
```

```
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

Action: Consolidate.

This ACI grants permission to the Messaging End User Administrators Group.

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode
||mailprogramdeliveryinfo||nswmextendeduserprefs||preferredlanguage
||maildeliveryoption||mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext
||vacationEndDate||vacationStartDate||mailautoreplysubject||pabURI
||maxPabEntries||mailMessageStore||mailSieveRuleSource||sunUCDateFormat
||sunUCDateDeLimiter||sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

Action: Consolidate.

This ACI grants permission to the Messaging End User Administrators Group.

```
#
# consolidate
#
aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota||inetSubscriberAccountId||dataSource||mailhost
||mailAllowedServiceAcces||pabURI||inetCOS||mailSMTPSubmitChannel
||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization
Admin Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

Action: Consolidate.

This is one of several ACIs that set self privileges.

Analysis of How ACIs Are Consolidated

The listing in this section shows the ACIs that have been consolidated in the replacement ldif file, `replacement.acis.ldif`, which you can use to consolidate ACIs in the directory. For instructions in how to replace ACIs, see "Steps for Replacing ACIs" on page 185.

The ACIs are divided into pairs. For each category, first the original ACIs and then the consolidated ACIs are listed:

Original Anonymous Access Rights

```
aci:
(targetattr != "userPassword || passwordHistory || passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordAllowChangeTime ")
(version 3.0; acl "Anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

```
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
version 3.0; acl "S1IS Top-level admin delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

```
aci:
(target="ldap:///$rootSuffix")
```

```
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*")
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)


aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

Consolidated Anonymous Access Rights

```
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr != "userPassword||passwordHistory
||passwordExpirationTime||passwordExpWarned||passwordRetryCount
||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
(version 3.0; acl "anonymous access rights";
allow (read,search,compare)
userdn = "ldap:///anyone"; )
```

Analysis: This ACI, which is on the root, allows the same access as the original collection of anonymous ACIs. It does this by listing a set of excluded attributes. This replacement ACI improves performance by eliminating the (*) in the target.

Original Self Acis

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy
state attributes";
allow (write)
```

```
userdn ="ldap:///self";)


aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)


aci:
(targetattr = "objectclass || inetuserstatus ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list
|| iplanet-am-user-account-life || iplanet-am-session-max-session-time
|| iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-levelAdmin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)


aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
|| LookThroughLimit
|| nsSizeLimit || nsTimeLimit || nsIdleTimeout || memberOf ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
planet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except
for nsroledn, aci, and resource limit attributes";
allow (write)
userdn ="ldap:///self";)


aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; acl "S1IS Allow self entry read search except for
nsroledn, aci, resource limit and web agent policy attributes";
allow (read,search)
userdn ="ldap:///self";)


aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentaddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota
```

```
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

Consolidated Self Acis

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
asswordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime ||
id || memberOf
|| objectclass || inetuserstatus || ou || owner || mail || mailuserstatus
|| memberOfManagedGroup ||mailQuota || mailMsgQuota || mailhost
|| mailAllowedServiceAccess || inetCOS || mailSMTPSubmitChannel")
(version 3.0; acl "Allow self entry modification";
allow (write)
userdn ="ldap:///self";)
```

```
aci:
(targetattr != " aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit|| nsIdleTimeout")
(version 3.0; acl "Allow self entry read search";
allow(read,search)
userdn ="ldap:///self";)
```

Analysis: Missing all the `iplanet-am-*` attributes. Since `deny` is the default if an ACI is not present, all `deny` ACIs are removed. The ones that allow `write` are consolidated into a single ACI.

Original Messaging Server ACIs

```
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix";)
```

```
aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode||
mailprogramdeliveryinfo
||nswmextendeduserprefs||preferredlanguage||maildeliveryoption||
mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext||
vacationEndDate
||vacationStartDate||mailautoreplysubject||pabURI||maxPabEntries||
mailMessageStore
||mailSieveRuleSource||sunUCDateFormat||sunUCDateDeLimiter||
sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix";)


aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress||
mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota||
mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

Consolidated Messaging Server ACIs

The self ACI is handled in the self ACIs.

```
aci:
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator
Read Only Access";
allow (read,search)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix"; )


aci:
(targetattr="objectclass || mailalternateaddress || Mailautoreplymode
|| mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
|| mailforwardingaddress || mailAutoReplyTimeout
|| mailautoreplytextinternal
```

```
|| mailautoreplytext || vacationEndDate || vacationStartDate
|| mailautoreplysubject || maxPabEntries || mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
|| sunUCTimeFormat || mailuserstatus || maildomainstatus")
(version 3.0; acl "Messaging Server End User Administrator All Access";
allow (all)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix";)
```

Analysis: Same as the original ACIs.

Original Organization Admin ACIs

```
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn ="ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)


aci: (missing)
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox
|| postalCode
|| registeredaddress || street || l || st || telephonenumber
|| maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

```
aci: (duplicate of per organization aci)
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///cn=Organization Admin
Role,($dn),dc=red,dc=iplanet,dc=com")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=red,dc=iplanet,dc=com))))
(targetattr = "nsroledn")
(targattrfilters="add=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,
o=SharedDomainsRoot,o=Business,$rootSuffix),
del=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,$rootSuffix)")
(version 3.0;
acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,o=Business,
$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,[$dn],dc=red,dc=iplanet,dc=com";)
```

Consolidated Organization Admin ACIs

```
aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
```

```
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read";
allow(read,search)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix" ;)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(entrydn=($dn),$rootSuffix))))
( targetattr = "*")
(version 3.0; acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

List of Unused ACIs to be Discarded

The listing in this section shows the unused default ACIs that are discarded from the directory when you apply the `replacement.acis.ldif` file to the directory.

The ACIs to be discarded are divided into the following categories:

Suffix

```
# discard
#
aci:
(targetattr ="*")
(version 3.0;acl "Configuration Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups,
```

```
ou=TopologyManagement, o=NetscapeRoot”);)


#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)


#
# discard
#
aci:
(targetattr = “*”)
(version 3.0;
acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server, cn=Server
Group, cn=whater.red.iplanet.com, ou=red.iplanet.com, o=NetscapeRoot”;)


#
# discard - prevents TLA from modifying the amldapuser account.
#
aci:
(target=”ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix”)
(targetattr = “*”)
(version 3.0;
acl “S1IS special ldap auth user modify right”;
deny (write)
roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”;)


#
# discard - protects SAML related attributes
#
aci:
(targetattr=”iplanet-am-saml-user || iplanet-am-saml-password”)
(targetfilter=”(objectclass=iplanet-am-saml-service)”)
(version 3.0; acl “S1IS Right to modify saml user and password”;
deny (all)
(roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”)
AND (userdn != “ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix”)
AND (userdn != “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”); )
```

Top-level Help Desk Admin Role

```
#
# discard
 #
```

```
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

Top-level Policy Admin Role

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access
Auth Service deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
```

```
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter="(objectclass=sunismanagedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Access Manager Anonymous

```
#
# discard - prevents anyone other than rootdn from deleting
# default organization.
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


#
# discard - prevents any user other than rootdn from deleting the
# TLA admin role.
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

Access Manager Deny Write Access

```
#
# discard
#
aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn ="ldap:///cn=Deny Write Access,$rootSuffix";)
```

Access Manager Container Admin Role

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix";)
```

Organization Help Desk

```
#
# discard
#
aci: (extra verses dreambig)
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
```

```
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

Access Manager Miscellaneous

```
#
# discard - Removal disables the associated privileges to the attribute
# iplanetam-modifiable-by
#
aci:
(target="ldap:///$rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

Index

D

F