Sun Java™ System

Communications Services 6 Schema Migration Guide

2005Q1

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

Part No: 819-0112-10

Contents

List of Figures

List of Tables

Preface

This guide describes how to migrate Sun Java™ System LDAP Directory data from LDAP Schema 1 to LDAP Schema 2 for Sun Java™ System Communications Services, specifically Sun Java™ System Messaging Server and Sun Java™ System Calendar Server.

Topics covered in this chapter include:

Who Should Use This Book

You should read this manual if you currently have installed Messaging Server 5.x or Calendar Server 5.x, using LDAP Schema 1, and you want to take advantage of services provided by Sun Java™ System Access Manager (formerly called Identity Server).

To integrate Messaging Server and Calendar Server with Access Manager, you must migrate your LDAP directory data from Schema 1 to Schema 2.

The audience for this manual consists of:

- System architects who want to understand migration issues and design a schema migration strategy for your installation.
- Site Administrators who want to know how to migrate directory data from Schema 1 to Schema 2.

Before You Read This Book

This book assumes that you have a general understanding of the following:

- Lightweight Directory Access Protocol (LDAP)
- Sun Java™ System Directory Server
- Messaging Server
- Calendar Server
- Access Manager (formerly called Identity Server)
- Sun Java™ System Console
- Delegated Administrator console and utility (`commadmin`) for Messaging Server and Calendar Server, for use with Schema 2. (In the Messaging Server 6 2004Q2 release, the Delegated Administrator utility was called User Management Utility.)

How This Book Is Organized

This book contains the following chapters and appendix:

Table 1 How This Book Is Organized

Chapter	Description
Chapter 1, “Schema Migration Overview”	Explains the reasons for migrating to Schema 2 and provides an overview of the migration steps.
Chapter 2, “Migration Scenarios”	Describes sample scenarios that offer migration paths for various user deployments and priorities.

Table 1 How This Book Is Organized *(Continued)*

Chapter	Description
Chapter 3, “Using the Migration Utility”	Defines the syntax and options of the schema migration utility.
Chapter 4, “Upgrading and Configuring the Servers”	Describes how to upgrade and configure the Messaging Server and Calendar Server to use LDAP Schema 2.
“Glossary”	

Conventions Used in This Book

The tables in this section describe the conventions used in this book.

Typographic Conventions

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

Table 2 Typographic Conventions

Typeface	Meaning	Examples
AaBbCc123 (Monospace)	Any text that appears on the computer screen or text that you should type. Can be API and language elements, HTML tags, web site URLs, command names, file names, directory path names, onscreen computer output, sample code.	Edit your.login file. Use ls -a to list all files. % You have mail.
AaBbCc123 (Monospace bold)	Text you should type when it appears within a code example or other onscreen computer output.	% **su** Password:
AaBbCc123 (Italic)	A placeholder in a command or path name that you should replace with a real name or value (for example, a variable). Also can be a book title, new term, or word to be emphasized.	The file is located in the *msg_svr_base*/bin directory. Read Chapter 6 in the *User’s Guide*. These are called *class* options. Do *not* save the file.

Symbols

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

Table 3 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 4 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`
cal_svr_base	Represents the base installation directory for Calendar Server. The default value of the *cal_svr_base* installation is as follows: Solaris™ systems: `/opt/SUNWics5` Linux systems: `/opt/sun/calendar`

Command Line Prompts

Command line prompts (for example, % for a C-Shell, or $ for a Korn or Bourne shell) are not displayed in the examples. Depending on which operating system you are using, you will see a variety of different command line prompts. However, you should enter the command as it appears in the document unless specifically noted otherwise.

Related Documentation

The http://docs.sun.com℠ 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/MessagingServer_05q1

The following documents are available:

- *Sun Java™ System Messaging Server Release Notes*
- *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 Messaging Server Messenger Express Customization Guide*

  If you are using LDAP Schema 1, use the Provisioning Guide found in the iPlanet Messaging Server 5.2 documents.

  If you are using LDAP Schema 2, use information found in the Sun Java Enterprise System documentation.

The Messaging Server product suite contains other products such as Sun Java™ System Console, 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/CalendarServer_05q1

The following documents are available:

- *Sun Java™ System Calendar Server Release Notes*
- *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/MessagingServer_05q1

or

http://docs.sun.com/coll/CalendarServer_05q1

The following documents are available:

- *Sun Java™ System Communications Services Delegated Administrator Administration 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*

Where to Find This Manual Online

You can find the *Sun Java™ System Communications Services Schema Migration Guide* online in HTML and PDF formats.

To find this manual or other Messaging Server documentation, use the URL:

http://docs.sun.com/coll/MessagingServer_05q1

Or, for this manual and other Calendar Server documentation, use the URL:

http://docs.sun.com/coll/CalendarServer_05q1

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.

Related Third-Party Web Site References

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.

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 6 2005Q1 Schema Migration Guide*, and the part number is 819-0112-10.

Chapter 1

Schema Migration Overview

This chapter describes the reasons for migrating your LDAP directory data from the Sun Java™ System LDAP Schema 1 (Schema 1) to the Sun Java™ System LDAP Schema 2 (Schema 2). It includes the following topics:

This chapter summarizes the migration process. It briefly explains the differences between Schema 1 and Schema 2, the target state of the migration, and the basic steps for reaching the target state.

Migration Prerequisites

Before you begin the migration, your installation should be configured with the following products and versions:

- LDAP directory in Schema 1
- Sun Java™ System Directory Server 5.2 or later
- At least one of these Communications Services servers:
  - Sun Java™ System (formerly Sun ONE) Messaging Server 5.x or later
  - Sun Java™ System (formerly Sun ONE) Calendar Server 5.x or later

It is assumed that all of the installed Messaging and Calendar servers are initially configured to use Schema 1.

Installing Access Manager and Delegated Administrator

During the migration process, you will install Sun Java™ System Access Manager 6.1 or later. (In earlier releases, Access Manager was called Identity Server.)

If you have already installed Access Manager 6.1 or later, you do not need to reinstall it during the migration procedures described in this guide.

The Sun Java™ Enterprise System installer automatically installs the Communications Services Delegated Administrator console and utility (`commadmin`) when you install Access Manager.

The Delegated Administrator console and utility (`commadmin`) are the Messaging Server and Calendar Server tools used to provision the LDAP directory after it has been migrated to Schema 2. (In the Messaging Server 6 2004Q2 release, the Delegated Administrator utility was called User Management Utility.)

Installing the Schema Migration Utility

When you install Access Manager 6.2 or later, the Java Enterprise System installer automatically installs the Schema Migration Utility, `commdirmig`. (Access Manager 6.2 or later is provided with the Java Enterprise System product suite.)

You also can migrate the directory successfully if you install Access Manager 6.1. However, Access Manager 6.1 does not provide the `commdirmig` utility. To obtain `commdirmig`, you will have to apply the following patch:

116585 (Solaris SPARC)

116586 (Solaris x86)

Reasons for Migrating to Schema 2

Migrating your LDAP directory data from Schema 1 to Schema 2 provides Messaging and Calendar servers the following benefits:

- Integration with Sun Java™ System Access Manager, which provides single sign-on (SSO)
- Use of the Delegated Administrator console and utility (`commadmin`) for provisioning the LDAP directory
- Use of a single integrated Directory Information Tree (DIT) for all Sun Java™ Enterprise System products

Access Manager uses Schema 2.

Messaging Server 6 and Calendar Server 6 can use either Schema 1 or Schema 2.

Messaging and Calendar servers cannot obtain authentication services from Access Manager until they migrate to Schema 2.

Definitions of Schema 1 and Schema 2

Messaging Server 6 and Calendar Server 6 have the following schema choices:

- Schema 1
- Schema 2, native mode
- Schema 2, compatibility mode

Schema 1

Messaging Server 5.x and Calendar Server 5.x installations use Schema 1.

The Directory Information Tree (DIT) organizes LDAP entries in a tree structure with nodes representing domains, subdomains, users, groups, and resources.

Schema 1 generally uses a two-tree structure:

- The Domain Component (DC) Tree contains domain nodes decorated with all the pertinent domain attributes.
- The Organization (OSI) Tree contains organization nodes that have the user, group, and resource entries underneath them.

Messaging and Calendar servers look up entries by accessing domain information in the DC Tree and using that information to find the appropriate entries in the Organization Tree.

Schema 2, Native Mode

Schema 2, native mode, introduces a one-tree structure. A single Organization Tree contains all the LDAP entries:

- Domain information held in domain nodes. (In Schema 2, the words domain and organization are used interchangeably.)
- User, group, and resource entries found underneath their respective domain nodes.

Messaging and Calendar servers look up entries by accessing domain information in the Organization Tree and using that information to find the appropriate user entries.

Schema 2, Compatibility Mode

If you are running applications (such as provisioning scripts or tools) developed at your site that rely on Schema 1, and it is not a trivial task to convert the applications to use Schema 2, you can choose to migrate to Schema 2, compatibility mode, as a first step before you migrate to Schema 2, native mode.

Schema 2, compatibility mode, retains the two-tree structure of Schema 1.

The Messaging and Calendar servers, and your own user-developed applications, continue to access the LDAP directory exactly as they did in Schema 1:

- They use the DC Tree to access the user and group nodes in the Organization Tree.
- They use an RFC 2247-compliant search algorithm to look up user entries.

From the perspective of the Messaging and Calendar servers and user-developed applications, Schema 1 is still in place.

At the same time, Schema 2, compatibility mode, enables you to use the Delegated Administrator console and utility (`commadmin`) and Access Manager features such as single sign-on (SSO). During the migration to Schema 2, compatibility mode, Access Manager object classes, attributes, and ACIs are added to the appropriate nodes in the Organization Tree.

Compatibility Mode and Server Configuration

Schema 2, compatibility mode refers to the state of the directory, not to the configuration of the Messaging and Calendar servers.

The Messaging and Calendar servers can only be configured to use Schema 1 or Schema 2.

When the directory is migrated to Schema 2, compatibility mode, the Messaging and Calendar servers should continue to be configured to use Schema 1.

Configure the servers to use Schema 2 only after the directory is migrated to Schema 2, native mode.

Table 1-1 shows the relationship of server configuration to the schema level of the directory.

Table 1-1 Server Configuration and Schema Level

Schema Level of the Directory	Messaging and Calendar Servers Must Be Configured for:	Messaging and Calendar Servers Can Use Access Manager Features
Schema 1	Schema 1	No
Schema 2, compatibility mode	Schema 1	Yes
Schema 2, native mode	Schema 2	Yes

NOTE In this guide, Schema 2 is assumed to be native mode unless the guide refers explicitly to compatibility mode.

What the Schema Migration Utility Does

The Schema Migration Utility, `commdirmig`, migrates LDAP directory data to Schema 2. It performs the following tasks:

- Converts the two-tree DIT structure to a one-tree structure.
- Adds Access Manager object classes, attributes, and ACIs to the domain and user entries. These attributes enable Access Manager to perform single sign-on (SSO) authentication against the LDAP entries.

During the migration to Schema 2, the `commdirmig` utility preserves the DC Tree. This feature allows existing 5.x servers to continue to use the LDAP directory even after it has been migrated to Schema 2.

Target State of the Migration

When the migration is completed, your installation should have the following product configuration:

- LDAP Schema 2, native mode
- At least one of the communications servers:
  - Messaging Server 6
  - Calendar Server 6

All of the installed servers must be configured to use Schema 2, native mode.

Overview of Migration Steps

Chapter 2, "Migration Scenarios," discusses how to choose a migration path and provides detailed migration procedures for each of the migration scenarios. Before you begin the migration, read Chapter 2.

Here is a general overview of the migration process:

1. Upgrade Messaging Server and Calendar Server to version 6.
2. Install Access Manager 6.1 or later and Delegated Administrator (`commadmin`).
3. Back up your LDAP directory data.
4. Migrate the LDAP directory data to Schema 2. Use the `commdirmig` utility to perform the migration of the schema object classes & attributes.
5. Configure Messaging Server and Calendar Server to use Schema 2, native mode.
6. Verify that the following processes are functioning properly:
   - The servers are working with the migrated schema
   - Provisioning can take place successfully

7. Remove the DC Tree (the defunct Schema 1 directory elements). This step is optional.

Suggested Information

Before you begin a schema migration, read “LDAP Directory Information Tree Requirements” in Chapter 3, “Understanding Product Requirements and Considerations,” in the *Sun Java System Communications Services Deployment Planning Guide* (http://docs.sun.com/doc/819-0063). This section describes the different LDAP Directory Information Tree (DIT) structures in Schema 1 and Schema 2.

Chapter 2

Migration Scenarios

The sample scenarios described in this chapter offer a few different paths for stepping through the migration. The chapter also discusses constraints that can affect the migration.

It includes the following topics:

Each scenario emphasizes a priority such as keeping the servers and LDAP directory available (so that, for example, users can continue to send and receive e-mail). The scenarios are not strict procedures. They provide guidelines to assist you in designing your own migration path.

Choosing a Migration Path

As you read the scenarios and plan your migration path, keep in mind the following questions:

- Is your system deployed on a single server or distributed across multiple servers?
- Is it critical to minimize downtime?

- Do you need to limit the time it takes to perform the migration?
- Is it important to minimize the complexity of the migration process?
- Are you running applications developed at your site that rely on LDAP Schema 1? (Have you created your own tools that provision directly against the LDAP directory and use Schema 1?) How complex a task would it be to convert your applications to use Schema 2?

These questions can help you to decide which scenario to use as a model for your own migration path. For example:

- If you have a multiple-server deployment and your highest priority is to minimize downtime, your migration path might resemble Scenario D, "Multiple Servers - Migrate Incrementally to Native Mode."
- If you have created your own provisioning tools that rely on Schema 1 and you have a multiple-server deployment, your migration path might resemble Scenario E, "Multiple Servers - Migrate Incrementally to Compatibility Mode, Then to Native Mode."

However, no single scenario is likely to correspond exactly to your situation. The scenarios are general examples. They do not attempt to replicate an actual user installation.

Read the assumptions and characteristics at the start of each scenario. Read all the steps in the scenarios that most closely resemble your situation. Then refine your specific migration strategy based on those guidelines.

The scenarios are as follows:

- Scenario A: "Single Server - Migrate to Native Mode"
- Scenario B: "Single Server - Migrate to Compatibility Mode, Then to Native Mode"
- Scenario C: "Multiple Servers - Migrate Directly to Native Mode"
- Scenario D: "Multiple Servers - Migrate Incrementally to Native Mode"
- Scenario E: "Multiple Servers - Migrate Incrementally to Compatibility Mode, Then to Native Mode"

NOTE Once you have become familiar with your particular migration issues and designed your migration strategy, it is a good practice to migrate on a test system before you migrate your production LDAP directory and Messaging and Calendar servers.

Potential Restrictions During Migration

Before you choose a migration strategy, you should understand the potential constraints on using the LDAP directory during the migration process.

Depending on the path you follow, old and new components might have to coexist during certain stages of the migration. Your installation temporarily could have a mixed environment, such as one of the following:

- Schema 1; one or more servers upgraded to version 6; remaining servers running version 5.x.
- Schema 2 (native mode or compatibility mode); one or more servers upgraded to version 6; remaining servers running version 5.x.

While your installation is in a mixed state, you might not be able to perform certain tasks such as domain provisioning. The following sections describe these issues in further detail.

Provisioning Tools

The following provisioning tools are available:

- To provision Schema 1:
  - For Messaging Server, use iPlanet Delegated Administrator.

    For Calendar Server, use the command-line utilities provided with Calendar Server, as described in "Calendar Server Command-Line Utilities Reference" in the *Calendar Server Administration Guide* (`http://docs.sun.com/doc/819-0024`).
- To provision Schema 2, native mode or compatibility mode, use the Delegated Administrator console and command-line utility (`commadmin`). (In the Messaging Server 6 2004Q2 release, the Delegated Administrator utility was called User Management Utility.)

Provisioning Rules During Migration

While the directory data is being migrated (while the Schema Migration Utility, `commdirmig`, is running), you *cannot* perform any provisioning tasks of any type.

Provisioning Rules Before and After Schema Migration

Before and after the directory migration, your installation components can be in a mixed state, as described in "Potential Restrictions During Migration" on page 29. Constraints on provisioning depend on the relationships between the server version and configuration and the current schema level.

Table 2-1 shows a matrix of the current directory schema level, the current server version and configuration, the provisioning tool you can use with each combination, and the provisioning constraints.

Table 2-1 Provisioning Constraints in a Mixed Environment

Directory Schema Level	Server 5.x	Server 6 - configured for Schema 1	Server 6 - configured for Schema 2
Schema 1	**1** For Messaging Server, use Delegated Administrator. For Calendar Server, use the Calendar Server command-line utilities. Full provisioning available.	**2** For Messaging Server, use Delegated Administrator. For Calendar Server, use the Calendar Server command-line utilities. Full provisioning available.	**3** Invalid combination for provisioning. *
Schema 2, compatibility mode	**4** Use `commadmin`. Full provisioning available.	**5** Use `commadmin`. Full provisioning available.	**6** Invalid combination for provisioning. *
Schema 2, native mode	**7** Invalid combination for provisioning.	**8** Use `commadmin`. No domain provisioning. No administrative provisioning.	**9** Use `commadmin`. Full provisioning available.

* A Server 6 configured for Schema 2 will not run against a Schema 1 directory or a Schema 2, compatibility mode, directory.

The following characteristics apply to the server-schema configurations shown in Table 2-1. They are numbered 1 - 9 for identification, not to indicate a required sequence of steps:

- Configuration 1 is the beginning state of the migration.
- Configuration 9 is the target state of the migration.
- Configurations 2, 4, 5, and 8: These are interim states that can exist during the migration process (particularly when multiple servers are involved and you migrate one server at a time).
- Configurations 3 and 6: You should never configure a server to use Schema 2 when the directory is Schema 1 or Schema 2, compatibility mode. Only configure a server to use Schema 2 after you migrate to Schema 2, native mode.

- Configuration 7: Do not provision with this configuration. This state can exist temporarily during an incremental migration of multiple servers and directory domains, when some domains have been migrated to Schema 2 and others are still in Schema 1. However, you cannot use 5.x provisioning tools to provision against the Schema 2 domains.
- Configurations 8: This state only works if you do not remove the DC Tree.

Provisioning Rules for Integration with Access Manager

After you migrate the directory to Schema 2 (native mode or compatibility mode), user-developed applications and provisioning tools must use the following rules for provisioning new entries:

- User entries must be underneath the people node in the Organization Tree.
- Group entries must be underneath the group node in the Organization Tree.

Access Manager requires this hierarchy for provisioning user and group entries. Access Manager-based tools will not recognize users and groups provisioned under different nodes than the people node and group node, respectively.

Constraints in Compatibility Mode

In Schema 2, compatibility mode, a version 6 server and a 5.x server would provision using the DC Tree. In compatibility mode, the Messaging and Calendar servers continue to provision the LDAP directory exactly as they did in Schema 1.

`inetDomainStatus`

During the migration from Schema 1 to Schema 2, compatibility mode, the `inetDomainStatus` attribute is copied to the organization / domain node in the Organization Tree.

In compatibility mode, two instances of `inetDomainStatus` exist, one in the DC Tree and one in the Organization Tree.

A 5.x server would reference `inetDomainStatus` in the DC Tree. A version 6 server would reference `inetDomainStatus` in the Organization Tree.

Access Manager-based provisioning tools such as the Delegated Administrator console and command-line utility (`commadmin`) ensure that the two copies of `inetDomainStatus` maintain the same value (active or inactive).

Your own provisioning tools (if you use any) also must ensure that the two copies of `inetDomainStatus` are set to the same value.

Guidelines for Calendar Servers Using Two LDAP Directories

If a Calendar Server has configured separate LDAP directories for authentication and user preferences, you must run the Schema Migration Utility (`commdirmig`) against both directories.

To check if your Calendar Server deployment uses two different directories, examine the values for the following parameters in the Calendar Server configuration file, `ics.conf`:

```
local.authldapbasedn
local.authldaphost
```

and

```
local.ugldapbasedn
local.ugldaphost
```

If the basedn and host values for these parameters are different, Calendar Server is using two different LDAP directories.

Safeguards Built into the Migration

While the Schema Migration Utility (`commdirmig`) is running, Messaging and Calendar servers can stay online and continue to look up user entries in the LDAP directory. (However, no provisioning should take place during the migration.)

In addition, `commdirmig` provides the following safety features that let you control and stage the migration:

- You can migrate one domain (or selected domains) at a time.
- You can perform a dry run of the migration.

  By default, `commdirmig` operates in preview mode (performs a dry run). The `commdirmig` utility writes an LDIF-formatted audit file containing the changes to the directory data that would be made during an actual migration. The LDAP directory itself isn't changed.

  After the utility executes in preview mode, you can examine the LDIF audit file and review the intended changes to the directory data.

  When you are satisfied that the changes are correct, you can use the `ldapmodify` tool to apply the LDIF entries to the LDAP directory. Or you can run `commdirmig` again in online mode, which directly migrates the directory data to Schema 2.

- The `commdirmig` utility produces an undo file, which you can use to roll back the changes made to the LDAP directory.
- If the migration is interrupted, you can run `commdirmig` again. The utility will resume the migration without changing any data that was properly migrated.
- The `commdirmig` utility leaves the DC Tree in place.

  The DC Tree is not used in Schema 2, but it does no harm to leave the deprecated DC Tree in the LDAP directory after the data has been migrated to Schema 2.

  After you have completed the entire migration process, you can choose to remove the DC Tree with an LDAP command-line tool. Before you remove the DC Tree, be sure to verify that the migration was successful.

Single Server - Migrate to Native Mode

This scenario makes the following assumptions:

- Your applications are running on a single-server system.
- The following applications are installed on your system:
  - One installation of Messaging Server, or
  - One installation of Calendar Server, or
  - One installation each of Messaging Server and Calendar Server
- The system does not include user-developed applications that rely on Schema 1.

Characteristics of This Scenario

- Simple and straightforward migration method

Migration Steps

The following steps outline how to migrate a single-server system directly to Schema 2, native mode:

1. Upgrade Messaging Server and Calendar Server from version 5.x to version 6 (if you have not already done so).

   For information about upgrading Messaging Server, see "Upgrading Messaging Server to Version 6" on page 78.

   For information about upgrading Calendar Server, see "Upgrading Calendar Server to Version 6" on page 81.

2. Be sure that the upgraded (version 6) servers are still configured for Schema 1.

   During the server upgrade, you run the Communications Services Directory Server Setup Perl script, `comm_dssetup.pl`. The script asks you to specify the schema version Directory Server will use:

   - Specify Schema 1.

     Set the `comm_dssetup.pl -t` option as follows: `-t 1`

   You only need to run the `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers, although it does no harm to run the script more than once.

   For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

3. Install Access Manager 6.1 or later.

   Follow the Access Manager installation instructions in the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`).

   a. Before you run the Java Enterprise System installation program, gather the information needed to install Access Manager with a provisioned directory. For details, see "Access Manager: Provisioned Directory Information," located in the following section of the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`):

      Part 1: Installation
      Configuration Information
      Access Manager Configuration Information
      Access Manager: Provisioned Directory Information

b. During the installation, you are asked if you want Access Manager to use an existing provisioned directory. Answer yes.

The installation program asks you to specify the following parameters associated with your directory:

Organization Object Marker Class: Object class defined for the organization in the existing provisioned directory. The default value is `SunManagedOrganization`.

Organization Naming Attribute: Naming attribute used to define organizations in the existing provisioned directory. The default value is `o`.

User Marker Object Class: Object class defined for users in the existing provisioned directory. The default value is `inetorgperson`.

User Naming Attribute: Naming attribute used for users in the existing provisioned directory. The default value is `uid`.

c. After you install Access Manager, configure Access Manager to operate with the existing directory. Follow the steps in "Configuring Access Manager with an Existing Directory" in the *Access Manager Migration Guide* (`http://docs.sun.com/doc/817-7645`)

NOTE Do not provision your LDAP directory with Access Manager tools before you have migrated the directory to Schema 2. The Messaging and Calendar servers cannot recognize any new domain information provisioned by Access Manager tools until you perform the migration to Schema 2 and reconfigure the servers for Schema 2.

---

4. Configure the Communications Services Delegated Administrator console and utility (`commadmin`).

Delegated Administrator is installed with Access Manager. After the installation, you must run the Delegated Administrator configuration program, `config-iscli`.

For details, see "Chapter 2: Configuring Delegated Administrator," in the *Communications Services Delegated Administrator Guide* (`http://docs.sun.com/doc/819-0114`).

5. Back up the LDAP directory.

6. Migrate the LDAP directory from Schema 1 to Schema 2, native mode.

   Use the Schema Migration utility, `commdirmig`, to perform the migration.

   Do not provision the directory while `commdirmig` is running.

   For information on running the `commdirmig` utility and on the utility options and syntax, see Chapter 3, “Using the Migration Utility.”

7. Configure Messaging Server and Calendar Server to use Schema 2, native mode.

   For information about reconfiguring Messaging Server, see “Configuring Messaging Server for Schema 2” on page 78.

   For information about reconfiguring Calendar Server, see “Configuring Calendar Server to Use Schema 2” on page 82.

8. Verify that the following processes are functioning properly:

   - The servers are working with the migrated schema
   - Provisioning can take place successfully

9. If you wish, remove the DC Tree (the defunct Schema 1 directory elements).

NOTE Do not remove the DC Tree until you have verified that the migration was completed successfully (as described in the preceding “verify” step).

   You can use an LDAP command-line tool to remove the DC Tree.

   This step is optional. The DC Tree is not used in Schema 2, but it does no harm to leave the deprecated DC Tree in the LDAP directory after Schema 2 is in place.

Single Server - Migrate to Compatibility Mode, Then to Native Mode

This scenario makes the following assumptions:

- Your applications are running on a single-server system.
- The following applications are installed on your system:
  - One instance of Messaging Server, or

  - One instance of Calendar Server, or
  - One instance each of Messaging Server and Calendar Server
- You are running user-developed applications (such as provisioning tools or scripts you have created at your site) that rely on Schema 1 and cannot easily be converted to use Schema 2.

Characteristics of This Scenario

- While the directory is in Schema 2, compatibility mode:
  - User-developed applications can continue to use the LDAP directory exactly as if it were still in Schema 1.
  - Messaging and Calendar servers can continue to use the directory exactly as if it were Schema 1.
  - User-developed provisioning tools that rely on Schema 1 can only work on existing directory data.
- The process is more complex than it is with a direct migration to Schema 2, native mode. The schema migration must be performed twice.

Migration Steps

This scenario outlines how to migrate a single-server system as follows:

- From Schema 1 to Schema 2, compatibility mode
- From Schema 2, compatibility mode, to Schema 2, native mode

Take these steps:

1. Upgrade Messaging Server and Calendar Server from version 5.x to version 6 (if you have not already done so).

   For information about upgrading Messaging Server, see “Upgrading Messaging Server to Version 6” on page 78.

   For information about upgrading Calendar Server, see “Upgrading Calendar Server to Version 6” on page 81.

2. Be sure that the upgraded (version 6) servers are still configured for Schema 1.

   During the server upgrade, you run the Communications Services Directory Server Setup Perl script, `comm_dssetup.pl`. The script asks you to specify the schema version Directory Server will use:

   - Specify Schema 1.

     Set `comm_dssetup.pl -t` option as follows: `-t 1`

   You only need to run the `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers, although it does no harm to run the script more than once.

   For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

3. Install Access Manager 6.1 or later.

   Follow the Access Manager installation instructions in the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`).

   a. Before you run the Java Enterprise System installation program, gather the information needed to install Access Manager with a provisioned directory. For details, see "Access Manager: Provisioned Directory Information," located in the following section of the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`):

      Part 1: Installation
      Configuration Information
      Access Manager Configuration Information
      Access Manager: Provisioned Directory Information

b. During the installation, you are asked if you want Access Manager to use an existing provisioned directory. Answer yes.

The installation program asks you to specify the following parameters associated with your directory:

Organization Object Marker Class: Object class defined for the organization in the existing provisioned directory. The default value is `SunManagedOrganization`.

Organization Naming Attribute: Naming attribute used to define organizations in the existing provisioned directory. The default value is `o`.

User Marker Object Class: Object class defined for users in the existing provisioned directory. The default value is `inetorgperson`.

User Naming Attribute: Naming attribute used for users in the existing provisioned directory. The default value is `uid`.

c. After you install Access Manager, configure Access Manager to operate with the existing directory. Follow the steps in "Configuring Access Manager with an Existing Directory" in the *Access Manager Migration Guide* (`http://docs.sun.com/doc/817-7645`).

NOTE Do not provision your LDAP directory with Access Manager tools before you have migrated the directory to Schema 2. The Messaging and Calendar servers cannot recognize any new domain information provisioned by Access Manager tools until you perform the migration to Schema 2 and reconfigure the servers for Schema 2.

---

4. Configure the Communications Services Delegated Administrator console and utility (`commadmin`).

Delegated Administrator is installed with Access Manager. After the installation, you must run the Delegated Administrator configuration program, `config-iscli`.

For details, see "Chapter 3: Configuring Delegated Administrator," in the *Communications Services Delegated Administrator Guide* (`http://docs.sun.com/doc/819-0114`).

5. Back up the LDAP directory.

6. Migrate the LDAP directory from Schema 1 to Schema 2, compatibility mode.

   Use the Schema Migration utility, `commdirmig`, to perform the migration.

   Do not provision the directory while `commdirmig` is running.

   For information on running `commdirmig` and on the utility options and syntax, see Chapter 3, "Using the Migration Utility."

NOTE You do not have to reconfigure the Messaging and Calendar servers to use Schema 2, compatibility mode.

When the LDAP directory has been migrated to Schema 2, compatibility mode, the servers should continue to be configured to use Schema 1.

7. Configure Access Manager to use Schema 2, compatibility mode.

   a. First, enable Access Manager to use the DC Tree:

      I. Start Access Manager Console as a user with administrator rights.

      II. Click the **Services Configuration** tab.

      III. Select **Administration Services -> Global**.

      IV. Check the box next to **Enable Domain Component Tree**.

      V. Click **Save**.

      For more information about these steps, see the "Domain Component Tree Enabled" section in "Administration Service Attributes," in the *Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

   b. Next, check that the Access Manager configuration properties file contains the correct DC Tree root suffix value:

      I. Open the Access Manager configuration properties file, `AMConfig.properties`. The default location of the file is `/opt/SUNWam/lib`.

      II. The `com.iplanet.am.domaincomponent` property in the `AMConfig.properties` file sets the value of the DC Tree root suffix. If the value is incorrect, edit it and save the file.

III. Restart Access Manager.

For more information, see the "Domain Component Tree Enabled" section in "Administration Service Attributes," in the *Access Manager Administration Guide* (http://docs.sun.com/doc/817-7647).

c. Use the `ldapmodify` tool to add the `inetdomain` object class to all DC Tree nodes. (For example: `dc=com,o=internet`.)

8. Verify that the following processes are functioning properly:
   - The servers are working with the migrated schema
   - Provisioning can take place successfully
9. Upgrade your user-developed applications (in-house provisioning tools or scripts) to use Schema 2, native mode.

   You do not *have* to perform this step (or the remaining steps). The Messaging and Calendar servers can continue to operate with Schema 2, compatibility mode, as long as your user-developed applications rely on the Schema 1 directory structure.

   However, we recommend that you convert your applications to use Schema 2 at some time.

   When you have converted the user-developed applications, proceed with the following steps:
10. Back up the LDAP directory.
11. Migrate the LDAP directory from Schema 2, compatibility mode to Schema 2, native mode.

    Use the Schema Migration utility, `commdirmig`, to perform the migration.

    Do not provision the directory while `commdirmig` is running.

    For information on running `commdirmig` and on the utility options and syntax, see Chapter 3, "Using the Migration Utility."
12. Configure Access Manager to user Schema 2, native mode:
    a. Start Access Manager Console as a user with administrator rights.
    b. Click the **Services Configuration** tab.
    c. Select **Administration Services -> Global**.
    d. Uncheck the box next to **Enable Domain Component Tree**.

e. Click **Save**.

When the **Enable Domain Component Tree** box is not checked, Access Manager ignores the DC Tree root suffix value held in the `com.iplanet.am.domaincomponent` property in the `AMConfig.properties` file.

For more information about these steps, see the "Domain Component Tree Enabled" section in "Administration Service Attributes," in the *Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

13. Configure Messaging Server and Calendar Server to use Schema 2, native mode.

For more information on reconfiguring Messaging Server, see "Configuring Messaging Server for Schema 2" on page 78.

For more information on reconfiguring Calendar Server, see "Configuring Calendar Server to Use Schema 2" on page 82.

14. Verify that the following processes are functioning properly:

- The servers are working with the migrated schema
- Provisioning can take place successfully

15. If you wish, remove the DC Tree (the defunct Schema 1 directory elements).

NOTE Do not remove the DC Tree until you have verified that the migration was completed successfully (as described in the preceding "verify" step).

You can use an LDAP command-line tool to remove the DC Tree.

This step is optional. The DC Tree is not used in Schema 2, but it does no harm to leave the deprecated DC Tree in the LDAP directory after Schema 2 is in place.

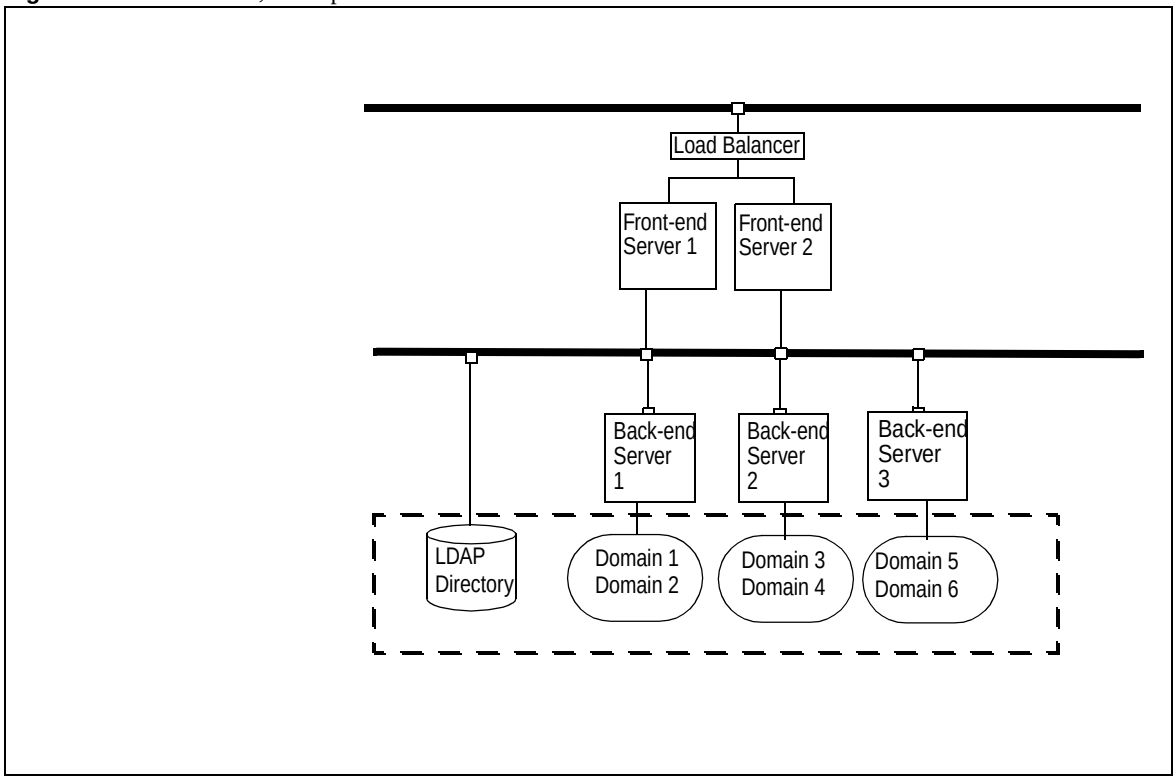
Multiple Servers - Migrate Directly to Native Mode

This direct-migration scenario makes the following assumptions:

- Messaging and Calendar Server are running in a two-tiered, multiple-server environment
- The installation does not include user-developed applications that rely on Schema 1

Figure 2-1 shows a simple example of a distributed environment. Two front-end servers handle incoming and outgoing traffic and three back-end servers look up entries in portions of the LDAP directory. Each back-end server manages two domains in the directory.

Figure 2-1 Two-tier, Multiple-Server Environment



Characteristics of This Scenario

- The entire LDAP directory is migrated in a single step.
- Some downtime is required while you upgrade the servers to version 6.
- The entire system can continue running while you upgrade the servers one at a time.

Migration Steps

The following steps outline how to migrate a two-tiered, multiple-server environment directly to Schema 2, native mode:

1. Upgrade the Messaging Servers and Calendar Servers from version 5.x to version 6 (if you have not already done so).

   In the example shown in Figure 2-1, upgrade the servers as follows:

   a. Upgrade Front-end Server 1 (F1).

   b. Upgrade Front-end Server 2 (F2).

   c. Upgrade Back-end Server 1 (B1).

   d. Upgrade Back-end Server 2 (B2).

   e. Upgrade Back-end Server 2 (B3).

   For information about upgrading Messaging Server, see "Upgrading Messaging Server to Version 6" on page 78.

   For information about upgrading Calendar Server, see "Upgrading Calendar Server to Version 6" on page 81.

2. Be sure that the upgraded (version 6) servers are still configured for Schema 1.

   During the server upgrade, you run the Communications Services Directory Server Setup Perl script, `comm_dssetup.pl`. The script asks you to specify the schema version Directory Server will use:

   - Specify Schema 1.

     Set `comm_dssetup.pl -t` option as follows: `-t 1`

   You only need to run the `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers, although it does no harm to run the script more than once.

   For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

3. Install Access Manager 6.1 or later.

   Follow the Access Manager installation instructions in the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`).

a. Before you run the Java Enterprise System installation program, gather the information needed to install Access Manager with a provisioned directory. For details, see "Access Manager: Provisioned Directory Information," located in the following section of the *Sun Java™ Enterprise System Installation Guide* (http://docs.sun.com/doc/819-0056):

Part 1: Installation
Configuration Information
Access Manager Configuration Information
Access Manager: Provisioned Directory Information

b. During the installation, you are asked if you want Access Manager to use an existing provisioned directory. Answer yes.

The installation program asks you to specify the following parameters associated with your directory:

Organization Object Marker Class: Object class defined for the organization in the existing provisioned directory. The default value is `SunManagedOrganization`.

Organization Naming Attribute: Naming attribute used to define organizations in the existing provisioned directory. The default value is `o`.

User Marker Object Class: Object class defined for users in the existing provisioned directory. The default value is `inetorgperson`.

User Naming Attribute: Naming attribute used for users in the existing provisioned directory. The default value is `uid`.

c. After you install Access Manager, configure Access Manager to operate with the existing directory. Follow the steps in "Configuring Access Manager with an Existing Directory" in the *Access Manager Migration Guide* (http://docs.sun.com/doc/817-7645).

NOTE Do not provision your LDAP directory with Access Manager tools before you have migrated the directory to Schema 2. The Messaging and Calendar servers cannot recognize any new domain information provisioned by Access Manager tools until you perform the migration to Schema 2 and reconfigure the servers for Schema 2.

4. Configure the Communications Services Delegated Administrator console and utility (`commadmin`).

   The Delegated Administrator is installed with Access Manager. After the installation, you must run the Delegated Administrator configuration program, `config-iscli`.

   For details, see "Chapter 3: Configuring Delegated Administrator," in the *Communications Services Delegated Administrator Guide* (`http://docs.sun.com/doc/819-0114`).

5. Back up the LDAP directory.

6. Migrate the LDAP directory from Schema 1 to Schema 2, native mode.

   Use the Schema Migration utility, `commdirmig`, to perform the migration.

   In a direct migration, you run `commdirmig` once to migrate the entire LDAP directory. Do not migrate individual domains.

   Do not provision the directory while `commdirmig` is running.

   For information on running the `commdirmig` utility and on the utility options and syntax, see Chapter 3, "Using the Migration Utility."

7. Configure the Messaging Servers and Calendar Servers to use Schema 2, native mode. In the example shown in Figure 2-1, configure the servers as follows:

   a. Reconfigure Front-end Server 1 (F1).

   b. Reconfigure Front-end Server 2 (F2).

   c. Reconfigure Back-end Server 1 (B1).

   d. Reconfigure Back-end Server 2 (B2).

   e. Reconfigure Back-end Server 2 (B3).

   For information about reconfiguring Messaging Server, see "Configuring Messaging Server for Schema 2" on page 78.

   For information about reconfiguring Calendar Server, see "Configuring Calendar Server to Use Schema 2" on page 82.

8. Verify that the following processes are functioning properly:

   - The servers are working with the migrated schema
   - Provisioning can take place successfully

9. If you wish, remove the DC Tree (the defunct Schema 1 directory elements).

NOTE Do not remove the DC Tree until you have verified that the migration was completed successfully (as described in the preceding “verify” step).

You can use an LDAP command-line tool to remove the DC Tree.

This step is optional. The DC Tree is not used in Schema 2, but it does no harm to leave the deprecated DC Tree in the LDAP directory after Schema 2 is in place.

Multiple Servers - Migrate Incrementally to Native Mode

This incremental-migration scenario makes the following assumptions:

- Messaging and Calendar Server are running in a two-tiered, multiple-server environment.
- The installation does not include user-developed applications (or provisioning tools) that rely on Schema 1.

This scenario uses the sample distributed environment shown in Figure 2-3 on page 51.

Characteristics of This Scenario

- Server downtime is minimized. At any given time, most servers are running and available.
- Most of the LDAP directory is available to the servers and for provisioning.
- You migrate the LDAP directory in stages, selecting individual domains for migration.
- The overall migration time is extended.
- The migration process is somewhat more complex than that of a direct, all-at-once migration.

Deployments Suitable for Incremental Migration

The scenario described in this section uses the sample distributed environment shown in Figure 2-3 on page 51.

In this example, each back-end server manages a unique portion of the LDAP directory, as follows:

- Back-end Server 1 (B1) manages Domain 1 and 2.
- Back-end Server 2 (B2) manages Domain 3 and 4.
- Back-end Server 3 (B3) manages Domain 5 and 6.

This structure lends itself to incremental migration because each server can be upgraded and configured separately, and its corresponding domains can be migrated separately.

In the scenario, the migration proceeds in three stages corresponding to the three server-domain groups listed above.

Rules for Incremental Migration

The following rules apply to incremental migration of servers and LDAP directory domains:

- When you migrate a domain, you also must upgrade and configure every server that manages any part of that domain.
- When you upgrade and configure a server, you also must migrate every domain (or part of a domain) managed by the server.

Cross-Domain Deployment—Not Recommended for Incremental Migration

If all the servers in your installation manage across domain boundaries (if multiple servers share access to each domain), your installation might not be a good candidate for incremental migration.

For example, suppose your installation contains two back-end servers in the following configuration:

- Back-end Server 1 manages Domain 1, 2, and 3.
- Back-end Server 2 manages Domain 2, 3, and 4.

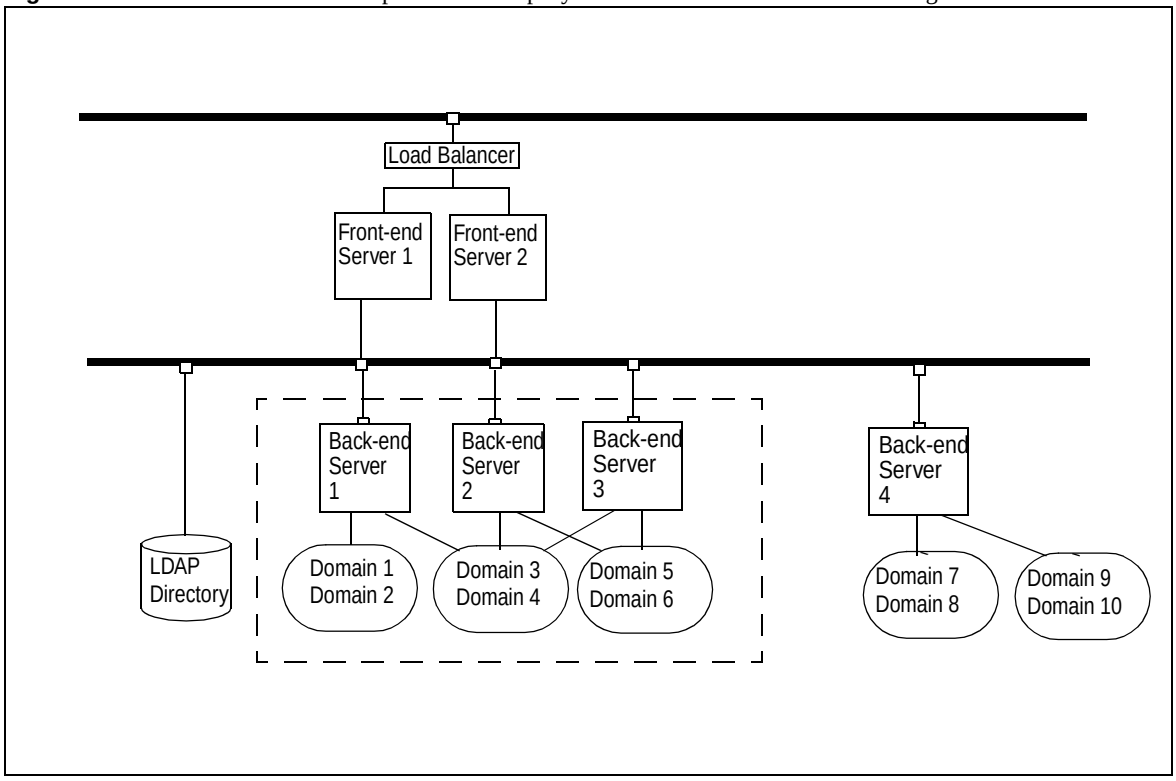
This installation should migrate directly (both servers, the entire LDAP directory), not incrementally.

A Complex Deployment Suitable for Incremental Migration

In a complex deployment with many back-end servers, you might still be able to migrate groups of domains incrementally. Your installation must fit the guidelines described in "Rules for Incremental Migration" on page 48.

Figure 2-2 shows one part of a large, complex server configuration and LDAP directory. It is assumed that the entire deployment includes many additional servers and domains not shown in the figure.

Figure 2-2 A Portion of a Multiple-Server Deployment Suitable for Incremental Migration



In the example shown in Figure 2-2, Back-end servers 1, 2, and 3 manage across domain boundaries, as follows:

- Back-end Server 1 manages Domain 1, 2, and 3.
- Back-end Server 2 manages Domain 3, 4, and 5.
- Back-end Server 3 manages Domain 4, 5, and 6.

No individual server exclusively manages a single domain.

Taken together, however, Back-end servers 1, 2, and 3 manage a unique set of domains that can be migrated incrementally.

In this example, when you run the Schema Migration Utility, you can specify Domains 1, 2, 3, 4, 5, and 6 in the migration to Schema 2. You can then reconfigure Back-end servers 1, 2, and 3 to use Schema 2.

Similarly, you could migrate and configure other groups of domains and servers that form distinct units within the deployment. In the example shown in Figure 2-2, Back-end Server 4 and the domains it manages might be candidates for another stage in an incremental migration.

When to Configure the Front-end Servers

When you migrate directory domains incrementally, the front-end servers should remain configured to use Schema 1 until you have migrated the entire directory to Schema 2.

To look up user entries, the front-end servers might have to read information in any domain in the directory. The servers must be able to use the DC Tree to find user entries in the domains still in Schema 1. Once a front-end server is configured for Schema 2, it cannot recognize domain information held in the DC Tree.

After you migrate all domains to Schema 2 and reconfigure all the back-end servers to use Schema 2, you can reconfigure the front-end servers to use Schema 2.

Domain Provisioning During an Incremental Migration

If you must create a new domain during an incremental migration, create it in Schema 1, by using a 5.x (Schema 1) provisioning tool. Of course, the new domain must be managed by a server still configured to use Schema 1.

This rule assumes that the front-end servers are configured to use Schema 1 until the entire directory has been migrated to Schema 2. A front-end server configured for Schema 1 can look up user entries in an *existing* domain that was migrated to Schema 2; the front-end server uses the DC Tree, which still contains the old routing information to the user entries.

However, if you create a *new* domain with a Schema 2 provisioning tool, no domain information will exist in the DC Tree. The front-end server will be unable to find the new domain information in the Organization Tree and will not find the new user entries.

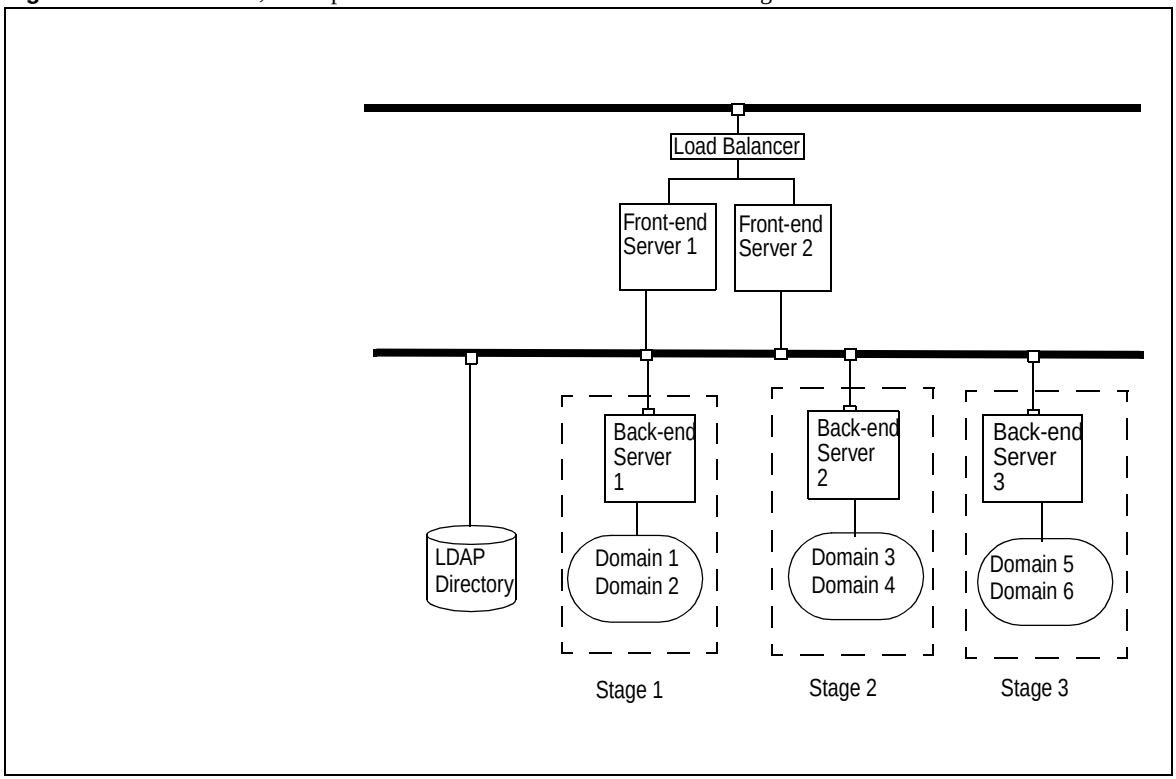
At some point in the migration, the new domain must be migrated to Schema 2 and its managing server(s) reconfigured to use Schema 2.

Migration Steps

The following steps outline how to migrate a two-tiered, multiple-server deployment to Schema 2, native mode in three stages.

Figure 2-3 shows the sample configuration of servers and domains used in this scenario.

Figure 2-3 Two-tier, Multiple-Server Environment: Incremental Migration



The steps for incremental migration are as follows:

1. Upgrade Back-end Server 1 (B1) from version 5.x to version 6 (if you have not already done so).

   For information about upgrading Messaging Server, see "Upgrading Messaging Server to Version 6" on page 78.

   For information about upgrading Calendar Server, see "Upgrading Calendar Server to Version 6" on page 81.

2. Be sure that Server B1 is still configured for Schema 1.

   During the server upgrade, you run the Communications Services Directory Server Setup Perl script, `comm_dssetup.pl`. The script asks you to specify the schema version Directory Server will use:

   - Specify Schema 1.

     Set `comm_dssetup.pl -t` option as follows: `-t 1`

   You only need to run the `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers, although it does no harm to run the script more than once.

   For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

3. Install Access Manager 6.1 or later.

   Follow the Access Manager installation instructions in the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`).

   a. Before you run the Java Enterprise System installation program, gather the information needed to install Access Manager with a provisioned directory. For details, see "Access Manager: Provisioned Directory Information," located in the following section of the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`):

      Part 1: Installation
      Configuration Information
      Access Manager Configuration Information
      Access Manager: Provisioned Directory Information

b. During the installation, you are asked if you want Access Manager to use an existing provisioned directory. Answer yes.

The installation program asks you to specify the following parameters associated with your directory:

Organization Object Marker Class: Object class defined for the organization in the existing provisioned directory. The default value is `SunManagedOrganization`.

Organization Naming Attribute: Naming attribute used to define organizations in the existing provisioned directory. The default value is `o`.

User Marker Object Class: Object class defined for users in the existing provisioned directory. The default value is `inetorgperson`.

User Naming Attribute: Naming attribute used for users in the existing provisioned directory. The default value is `uid`.

c. After you install Access Manager, configure Access Manager to operate with the existing directory. Follow the steps in "Configuring Access Manager with an Existing Directory" in the *Access Manager Migration Guide* (`http://docs.sun.com/doc/817-7645`).

NOTE Do not provision your LDAP directory with Access Manager tools before you have migrated the directory to Schema 2. The Messaging and Calendar servers cannot recognize any new domain information provisioned by Access Manager tools until you perform the migration to Schema 2 and reconfigure the servers for Schema 2.

---

4. Configure the Communications Services Delegated Administrator console and utility (`commadmin`).

The Delegated Administrator is installed with Access Manager. After the installation, you must run the Delegated Administrator configuration program, `config-iscli`.

For details, see "Chapter 3: Configuring Delegated Administrator," in the *Communications Services Delegated Administrator Guide* (`http://docs.sun.com/doc/819-0114`).

5. Back up Domains 1 and 2 in the LDAP directory.

6. Migrate Domains 1 and 2 of the LDAP directory from Schema 1 to Schema 2, native mode. (Server B1 uniquely manages Domains 1 and 2.)

- Use the Schema Migration utility, `commdirmig`, to perform the migration.

- Use the `-d` *Domain* option to migrate Domains 1 and 2.

Do not provision Domains 1 and 2 while `commdirmig` is running. You can provision other domains in the directory.

For information on running the `commdirmig` utility and on the utility options and syntax, see Chapter 3, "Using the Migration Utility."

NOTE Do not remove the DC Tree for Domains 1 and 2 until all domains in the directory have been migrated to Schema 2, native mode, and all dependencies on the DC Tree are removed.

7. Reconfigure Server B1 to use Schema 2, native mode.

   For information about reconfiguring Messaging Server, see "Configuring Messaging Server for Schema 2" on page 78.

   For information about reconfiguring Calendar Server, see "Configuring Calendar Server to Use Schema 2" on page 82.

8. Verify that the following processes are functioning properly:

   - The upgraded server is working with the migrated domains
   - Provisioning can take place successfully

9. Repeat Step 1 on page 52 through Step 8 on page 54 for

   - Server B2
   - Domains 3 and 4 in the LDAP directory

10. Repeat Step 1 on page 52 through Step 8 on page 54 for

    - Server B3
    - Domains 5 and 6 in the LDAP directory

11. Upgrade Front-end Server 1 (F1) and Front-end Server 2 (F2) from version 5.x to version 6 (if you have not already done so).

    For information about upgrading Messaging Server, see "Upgrading Messaging Server to Version 6" on page 78.

    For information about upgrading Calendar Server, see "Upgrading Calendar Server to Version 6" on page 81.

12. Run the `comm_dssetup.pl` script. The script asks you to specify the schema version Directory Server will use:

- Specify Schema 2, native mode. Choose Schema 2 because you have already migrated all domains in the directory to Schema 2.

  Set `comm_dssetup.pl -t` option as follows: `-t 2`

For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

13. Reconfigure Server F1 and Server F2 to use Schema 2, native mode.

    For information about reconfiguring Messaging Server, see "Configuring Messaging Server for Schema 2" on page 78.

    For information about reconfiguring Calendar Server, see "Configuring Calendar Server to Use Schema 2" on page 82.

14. If you wish, remove the DC Tree (the defunct Schema 1 directory elements).

NOTE Do not remove the DC Tree until you have verified that the migration was completed successfully (as described in the preceding "verify" step).

You can use an LDAP command-line tool to remove the DC Tree.

This step is optional. The DC Tree is not used in Schema 2, but it does no harm to leave the deprecated DC Tree in the LDAP directory after Schema 2 is in place.

Multiple Servers - Migrate Incrementally to Compatibility Mode, Then to Native Mode

This incremental-migration scenario makes the following assumptions:

- Messaging and Calendar Server are running in a two-tiered, multiple-server environment.
- You are running user-developed applications (such as provisioning tools or scripts you have created at your site) that rely on Schema 1 and that cannot be converted immediately to use Schema 2

This scenario uses the sample distributed environment shown in Figure 2-3 on page 51.

Characteristics of This Scenario

- Server downtime is minimized. At any given time, most servers are running and available.
- Most of the LDAP directory is available to the servers and for provisioning.
- You migrate the LDAP directory in stages, selecting individual domains for migration.
- The overall migration time is extended.
- While the directory is in Schema 2, compatibility mode:
  - User-developed applications can continue to use the LDAP directory exactly as if it were still in Schema 1.
  - Messaging and Calendar servers can continue to use the directory exactly as if it were Schema 1.
  - User-developed provisioning tools that rely on Schema 1 can only work on existing directory data.
- This migration process is the most complex of the scenarios; it is more complex than a direct migration to Schema 2, native mode, or an incremental migration to native mode. The schema migration must be performed twice.

For a discussion of the conditions best suited for migrating your installation incrementally, see "Deployments Suitable for Incremental Migration" on page 48.

Migration Steps

The following steps outline how to migrate a two-tiered, multiple-server environment to Schema 2, native mode in stages.

1. Upgrade Back-end Server 1 (B1) from version 5.x to version 6 (if you have not already done so). Server B1 is shown in the example in Figure 2-3 on page 51.

For information about upgrading Messaging Server, see "Upgrading Messaging Server to Version 6" on page 78.

For information about upgrading Calendar Server, see "Upgrading Calendar Server to Version 6" on page 81.

2. Be sure that Server B1 is still configured for Schema 1.

   During the server upgrade, you run the Communications Services Directory Server Setup Perl script, `comm_dssetup.pl`. The script asks you to specify the schema version Directory Server will use:

   - Specify Schema 1.

     Set `comm_dssetup.pl -t` option as follows: `-t 1`

   You only need to run the `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers, although it does no harm to run the script more than once.

   For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

3. Install Access Manager 6.1 or later.

   Follow the Access Manager installation instructions in the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`).

   a. Before you run the Java Enterprise System installation program, gather the information needed to install Access Manager with a provisioned directory. For details, see "Access Manager: Provisioned Directory Information," located in the following section of the *Sun Java™ Enterprise System Installation Guide* (`http://docs.sun.com/doc/819-0056`):

      Part 1: Installation
      Configuration Information
      Access Manager Configuration Information
      Access Manager: Provisioned Directory Information

b. During the installation, you are asked if you want Access Manager to use an existing provisioned directory. Answer yes.

The installation program asks you to specify the following parameters associated with your directory:

Organization Object Marker Class: Object class defined for the organization in the existing provisioned directory. The default value is `SunManagedOrganization`.

Organization Naming Attribute: Naming attribute used to define organizations in the existing provisioned directory. The default value is `o`.

User Marker Object Class: Object class defined for users in the existing provisioned directory. The default value is `inetorgperson`.

User Naming Attribute: Naming attribute used for users in the existing provisioned directory. The default value is `uid`.

c. After you install Access Manager, configure Access Manager to operate with the existing directory. Follow the steps in "Configuring Access Manager with an Existing Directory" in the *Access Manager Migration Guide* (`http://docs.sun.com/doc/817-7645`).

NOTE Do not provision your LDAP directory with Access Manager tools before you have migrated the directory to Schema 2. The Messaging and Calendar servers cannot recognize any new domain information provisioned by Access Manager tools until you perform the migration to Schema 2 and reconfigure the servers for Schema 2.

---

4. Configure the Communications Services Delegated Administrator console and utility (`commadmin`).

The Delegated Administrator is installed with Access Manager. After the installation, you must run the Delegated Administrator configuration program, `config-iscli`.

For details, see "Chapter 2: Configuring Delegated Administrator," in the *Communications Services Delegated Administrator Guide* (`http://docs.sun.com/doc/819-0114`).

5. Back up Domains 1 and 2 in the LDAP directory.

6. Migrate Domains 1 and 2 of the LDAP directory from Schema 1 to Schema 2, compatibility mode. (Server B1 uniquely manages Domains 1 and 2.)

- Use the Schema Migration utility, `commdirmig`, to perform the migration.

- Use the `-d` *Domain* option to migrate Domains 1 and 2.

Do not provision Domains 1 and 2 while `commdirmig` is running. You can provision other domains in the directory.

For information on running the `commdirmig` utility and on the utility options and syntax, see Chapter 3, "Using the Migration Utility."

NOTE You do not have to reconfigure the Messaging and Calendar servers to use Schema 2, compatibility mode.

When the LDAP directory has been migrated to Schema 2, compatibility mode, the servers should continue to be configured to use Schema 1.

7. Configure Access Manager to use Schema 2, compatibility mode.

   a. First, enable Access Manager to use the DC Tree:

      I. Start Access Manager Console as a user with administrator rights.

      II. Click the **Services Configuration** tab.

      III. Select **Administration Services -> Global**.

      IV. Check the box next to **Enable Domain Component Tree**.

      V. Click **Save**.

      For more information about these steps, see the "Domain Component Tree Enabled" section in "Administration Service Attributes," in the *Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

   b. Next, check that the Access Manager configuration properties file contains the correct DC Tree root suffix value:

      I. Open the Access Manager configuration properties file, `AMConfig.properties`. The default location of the file is `/opt/SUNWam/lib`.

      II. The `com.iplanet.am.domaincomponent` property in the `AMConfig.properties` file sets the value of the DC Tree root suffix. If the value is incorrect, edit it and save the file.

      III. Restart Access Manager.

      For more information, see the "Domain Component Tree Enabled" section in "Administration Service Attributes," in the *Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

c. Use the `ldapmodify` tool to add the `inetdomain` object class to all DC Tree nodes. (For example: `dc=com,o=internet`.)

8. Verify that the following processes are functioning properly:

- The upgraded server is working with the migrated domains
- Provisioning can take place successfully

9. Repeat Step 1 on page 56 through Step 8 on page 60 for

- Server B2
- Domains 3 and 4 in the LDAP directory

10. Repeat Step 1 on page 56 through Step 8 on page 60 for

- Server B3
- Domains 5 and 6 in the LDAP directory

11. Upgrade Front-end Server 1 (F1) and Front-end Server 2 (F2) from version 5.x to version 6 (if you have not already done so).

For information about upgrading Messaging Server, see "Upgrading Messaging Server to Version 6" on page 78.

For information about upgrading Calendar Server, see "Upgrading Calendar Server to Version 6" on page 81.

12. Run the `comm_dssetup.pl` script. The script asks you to specify the schema version Directory Server will use:

- Specify Schema 2, compatibility mode. (You do this because you have already migrated all domains in the directory to Schema 2, compatibility mode.)

  Set `comm_dssetup.pl -t` option as follows: `-t 1.5`

For information about running `comm_dssetup.pl`, see "Running the Directory Server Setup Script" on page 78.

13. Upgrade your user-developed applications (in-house provisioning tools or scripts) to use Schema 2, native mode.

    You do not *have* to perform this step (or the remaining steps). The Messaging and Calendar servers can continue to operate with Schema 2, compatibility mode, as long as your user-developed applications rely on the Schema 1 directory structure.

    However, we recommend that you convert your applications to use Schema 2 at some time.

    When you have converted the user-developed applications, proceed with the following steps:

14. Back up Domains 1 and 2 in the LDAP directory.

15. Migrate Domains 1 and 2 from Schema 2, compatibility mode, to Schema 2, native mode.

    - Use the Schema Migration utility, `commdirmig`, to perform the migration.
    - Use the `-d` *Domain* option to migrate Domains 1 and 2.

    Do not provision Domains 1 and 2 while `commdirmig` is running. You can provision other domains in the directory.

    For information on running `commdirmig` and on the utility options and syntax, see Chapter 3, “Using the Migration Utility.”

NOTE Do not remove the DC Tree for Domains 1 and 2 until all domains in the directory have been migrated to Schema 2, native mode, and all dependencies on the DC Tree are removed.

16. Configure Access Manager to user Schema 2, native mode:

    a. Start Access Manager Console as a user with administrator rights.

    b. Click the **Services Configuration** tab.

    c. Select **Administration Services -> Global**.

    d. Uncheck the box next to **Enable Domain Component Tree**.

e. Click **Save**.

When the **Enable Domain Component Tree** box is not checked, Access Manager ignores the DC Tree root suffix value held in the `com.iplanet.am.domaincomponent` property in the `AMConfig.properties` file.

For more information about these steps, see the "Domain Component Tree Enabled" section in "Administration Service Attributes," in the *Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

NOTE Once you enable Access Manager to use Schema 2, native mode, you can only provision in the domains that have been migrated to Schema 2, native mode. Do not provision new entries in the domains that are still in Schema 2, compatibility mode.

17. Reconfigure Server B1 to use Schema 2, native mode.

    For information about reconfiguring Messaging Server, see "Configuring Messaging Server for Schema 2" on page 78.

    For information about reconfiguring Calendar Server, see "Configuring Calendar Server to Use Schema 2" on page 82.

18. Verify that the following processes are functioning properly:

    - The reconfigured server is working with the migrated domains
    - Provisioning can take place successfully

19. Repeat Step 14 on page 61 through Step 18 on page 62 for

    - Server B2
    - Domains 3 and 4 in the LDAP directory

20. Repeat Step 14 on page 61 through Step 18 on page 62 for

    - Server B3
    - Domains 5 and 6 in the LDAP directory

21. Reconfigure Server F1 and Server F2 to use Schema 2, native mode.

    For information about reconfiguring Messaging Server, see "Configuring Messaging Server for Schema 2" on page 78.

    For information about reconfiguring Calendar Server, see "Configuring Calendar Server to Use Schema 2" on page 82.

22. If you wish, remove the DC Tree (the defunct Schema 1 directory elements).

NOTE Do not remove the DC Tree until you have verified that the migration was completed successfully (as described in the preceding “verify” step).

You can use an LDAP command-line tool to remove the DC Tree.

This step is optional. The DC Tree is not used in Schema 2, but it does no harm to leave the deprecated DC Tree in the LDAP directory after Schema 2 is in place.

Chapter 3

Using the Migration Utility

This chapter describes the Schema Migration utility, `commdirmig`. It includes the following topics:

The `commdirmig` utility migrates an LDAP directory from Schema 1 to Schema 2. The utility adds object classes and attributes to existing LDAP entries; it updates the current LDAP directory. To complete the migration, you do not have to create a new LDAP directory and copy data into it from the old directory.

commdirmig Syntax

The `commdirmig` utility has the following syntax:

```
commdirmig -t {1|2|3}
           -D AuthenticationID          -w AuthenticationPasswordFile
           -X DirectoryServerHost       -p DirectoryServerPort
           -b OSIRoot                   -r DCRoot
           [-o online]                   [-a AuditLDIFFile]
           [-d Domain [, Domain]... [, Domain] | "*"]
           [-f DomainFile]
           [-S mail, cal]               [-H MailHost]
           [-i InputFile]               [-l LogFile]
           [-v]                         [-c]
           [-m LogMaxSize]               [-k]
           [-u UndoFile ]
           [-h Option ]  [-? Option]  [-V]
```

Table 3-1 lists the `commdirmig` mandatory options and summarizes the information in the following sections.

Table 3-1 `commdirmig` Mandatory Options

commdirmig Mandatory Option	Description
`-t 1|2|3`	`1` — specifies a migration from Schema 1 to Schema 2, native mode. `2` — specifies a migration from Schema 1 to Schema 2, compatibility mode. `3` — specifies a migration from Schema 2, compatibility mode to Schema 2, native mode.
`-D` *AuthenticationID*	Specifies the login ID of the user authorized to run and modify the Directory Server.
`-w` *AuthenticationPasswordFile*	Specifies a text file containing the password for the Directory Server login ID. You can choose to set the password file to be readable only by superuser (root).
`-X` *DirectoryServerHost*	Specifies the host name of the Directory Server that manages the LDAP directory you are migrating.
`-p` *DirectoryServerPort*	Specifies the port number for accessing the Directory Server.

Table 3-1 `commdirmig` Mandatory Options

commdirmig Mandatory Option	Description
`-b` *OSIRoot*	Specifies the root suffix of the OSI (Organization) Tree in the LDAP directory.
`-r` *DCRoot*	Specifies the root suffix of the DC Tree in the LDAP directory.

Table 3-2 lists the `commdirmig` non-mandatory options and summarizes the information in the following sections.

Table 3-2 `commdirmig` Non-Mandatory Options

commdirmig Non-Mandatory Option	Description
`[-o ]`	Directs `commdirmig` to migrate the LDAP directory online (immediately).
`[-a` *AuditLDIFFile*`]`	Directs `commdirmig` to write the migration audit to an LDIF-formatted file you specify. The directory entries are not changed. By default, `commdirmig` writes the migration audit to a file. It does not migrate online. The default *AuditLDIFFile* is `commdirmig.audit.ldif`.
`[-d` *Domain* `[,`*Domain*`]...[,`*Domain*`]|"*"]`	*Domain*`[,`*Domain*`]...[,`*Domain*`]` – specifies inidividual domain names. You can specify a single domain or a comma-separated list of domains. `"*"` – specifies all domains in the LDAP directory. You must enclose the asterisk in quotes or use the Escape character before the asterisk. The default is to migrate all domains in the LDAP directory.
`[-f` *DomainFile*`]`	*DomainFile* – specifies an ASCII text file that contains a blank-line separated list of domain names. `commdirmig` migrates the domains named in the file. Optionally, you can specify a preferred mail host associated with a specified domain. This option is used as the mail host when mail service is added to users and groups in the domain. For details about formatting the *DomainFile*, see *"Formatting the Domain File" on page 71*.
`[-S mail, cal]`	`mail` – adds new Messaging services to the directory. `cal` – adds new Calendar services to the directory. The default is to migrate only the services `commdirmig` finds in the current directory.

Table 3-2 `commdirmig` Non-Mandatory Options *(Continued)*

commdirmig Non-Mandatory Option	Description
`[-H` *MailHost*`]`	Specifies the mail host to be used to add mail services to users and groups. When you use `-S mail` to add mail services, `-H` *MailHost* is required.
`[-i` *InputFile*`]`	Directs `commdirmig` to migrate the directory by using the options and arguments listed in a user-created file, *InputFile*.
`[-l` *LogFile*`]`	Specifies the file to which `commdirmig` writes log information. The default is `commdirmig.log`.
`[-v ]`	Specifies verbose (maximum) log details. The default level is standard.
`[-c ]`	Directs `commdirmig` to continue running when an error occurs. The default is to exit when an error occurs.
`[-m` *LogMaxSize*`]`	Specifies the maximum size of the log file. Size can be configured in kilobytes (K) or megabytes (M). For example: `500 K` or `2 M`.
`[-k ]`	Checks for erroneous domain provisioning in the existing LDAP directory and reports the erroneous information to the log file.
`[-u` *UndoFile*`]`	Directs `commdirmig` to create an undo log that can be applied to undo the migration. The log entries are saved in LDIF format in the user-specified file, *UndoFile*. The default is to create an undo log. The default file is `commdirmig.undo.ldif`.
`[-h` *Option*`]`	Displays help information about the specified option.
`[-?` *Option*`]`	Displays help information about the specified option.
`[-V ]`	Displays the current version of the `commdirmig` utility.

commdirmig Mandatory Options

Migration Type

`commdirmig` can migrate the LDAP directory directly to Schema 2, native mode, or through the intermediate stage—Schema 2, compatibility mode.

Use the `-t` option to specify the current schema version and mode (before the migration begins) and the version and mode to which `commdirmig` will migrate the schema. The `-t` option takes one of the following arguments:

- `-t 1` specifies a migration from Schema 1 to Schema 2, native mode.
- `-t 2` specifies a migration from Schema 1 to Schema 2, compatibility mode.
- `-t 3` specifies a migration from Schema 2, compatibility mode to Schema 2, native mode.

`-t` is a required option.

Directory Server Access

During the migration, `commdirmig` updates Directory Server schema and configuration data for Schema 2 (compatibility or native mode).

Use the following options to specify the information `commdirmig` needs to gain access to the Directory Server:

- `-D` *AuthenticationID* specifies the login ID of the user authorized to run and modify the Directory Server.
- `-w` *AuthenticationPasswordFile* specifies an ASCII text file containing the password for the Directory Server login ID. For security, you can, for example, set the password file to be readable only by superuser (root).
- `-X` *DirectoryServerHost* specifies the host name of the Directory Server that manages the LDAP directory you are migrating.
- `-p` *DirectoryServerPort* specifies the port number for accessing the Directory Server.
- `-b` *OSIRoot* specifies the root suffix of the OSI (Organization) Tree in the LDAP directory.
- `-r` *DCRoot* specifies the root suffix of the DC Tree in the LDAP directory.

`-D`, `-w`, `-X`, `-p`, `-b`, and `-r` are required options.

When you run `commdirmig` for the first time, the `-X`, `-p`, `-b`, and `-r` options are saved in a configuration file, `commdirmig-userprefs.properties`. When you run `commdirmig` again, it uses the option values stored in the configuration file. For details, see “commdirmig Configuration File” on page 76.

commdirmig Non-Mandatory Options

Migration Online or in Preview Mode

You can choose whether to migrate the LDAP directory data directly (online) or run the utility in preview mode (write an audit of the migration to an LDIF-formatted file).

Use one of the following options to specify whether to use online or preview mode:

- `-o` directs `commdirmig` to update the LDAP directory immediately. When you choose `-o`, `commdirmig` migrates the directory data.
- `-a` *AuditLDIFFile* directs `commdirmig` to write the migration audit to the LDIF-formatted file you specify. The directory entries are not changed. Choose this option to perform a dry run of the migration.

  If you want to run the utility in preview mode, do not specify the `-o` option.

By default, `commdirmig` runs in preview mode (writes the migration audit to the LDIF file). It does not migrate the directory data online.

The default *AuditLDIFFile* is named `commdirmig.audit.ldif`.

Examples

```
commdirmig -o
```

```
commdirmig -a /home/user/migration.audit.ldif
```

Domains Being Migrated

`commdirmig` can migrate a single domain, a list of domains, or all the domains in the LDAP directory. By default, `commdirmig` migrates all domains in the LDAP directory.

Use one of the following options to specify the domains to be migrated:

- `-d` *Domain [, Domain]... [, Domain]* specifies individual domain names. You can specify a single domain or a comma-separated list of domains.
- `-d` “*” specifies all domains in the LDAP directory. You must enclose the asterisk in quotes or use the Escape character before the asterisk.

- `-f` *DomainFile* specifies an ASCII text file that contains a blank-line separated list of domain names. The `commdirmig` utility migrates the domains named in the file.

  In a *DomainFile*, you also can specify a preferred mail host associated with a specified domain. This option is used as the mail host when mail service is added to users and groups in the domain.

  Formatting the Domain File

  For each domain to be specified in the *DomainFile*, type the option letter `d`, then a space, then the domain name.

  To specify an associated mail host, start a new line and type the option letter `H`, then a space, then the mail host name.

  Separate each specified domain with a blank line.

  Do not type a dash (`-`) before the option letters.

  In the following example, a *DomainFile* named `domainnames.txt` specifies three domains to be migrated and their associated mail hosts to be used for new mail services:

  ```
  d Domain1
  H host1.siroe.com

  d Domain2
  H host2.sesta.com

  d Domain3
  H host3.siroe.com
  ```

Examples

```
commdirmig -d sesta.com, siroe.com, varrius.org

commdirmig -d *

commdirmig -f /home/user/domainnames.txt
```

Services to Add

By default, `commdirmig` migrates only the services it finds in the current directory. It does not add new services.

The `-S` option specifies whether to add new mail services, Calendar services, or both mail and Calendar services to the migrated directory.

Use the following arguments to add mail and Calendar services:

- `-S mail` adds new mail services to the directory.
- `-H` *MailHost* specifies the mail host to be used to add mail services to users and groups.

  When you use `-S mail` to add mail services, `-H` *MailHost* is required.
- `-S cal` adds new Calendar services to the directory.

Examples

```
commdirmig -S mail -H host1.siroe.com
```

```
commdirmig -S mail, cal -H host1.siroe.com
```

Input File

`-i` *InputFile* directs `commdirmig` to read a user-created text file, *InputFile*, which contains a list of `commdirmig` options and arguments. `commdirmig` uses the information in the file to migrate the directory.

The command-line version of an option overrides the *InputFile* version of the same option. That is, if you enter an option in the command line and the same option exists in the *InputFile*, `commdirmig` uses the command-line option and ignores the option in the *InputFile*.

Formatting the Input File

The *InputFile* is a new-line separated ASCII text file. For each option to be specified in the *InputFile*, type the option letter, then a space, then the option arguments. Do not type a dash (-) before the option letters.

In the following example, an *InputFile* named `commdirmig.input.txt` specifies the Directory Server login ID and a file containing the password of the Directory Server user, the Directory Server host name and port number, and the OSI root and DC root:

```
D "cn=Directory Manager"
w /opt/SUNWcomm/passwd
X ldaphost
p 389
b "o=isp"
r "o=internet"
```

Uses of the Input File

If you use this option, you do not have to type all the options in the command line when you run the utility. Also, you can edit and reuse the *InputFile*, which makes it easier to run the utility multiple times. For example, you can do the following:

- Run the utility once to migrate a test directory and later to migrate the production directory.
- Migrate several domains, one at a time.

  Before you reuse the file, alter the `-d` or `-f` option to point to the domains or the directory you intend to migrate.
- Migrate to Schema 2, compatibility mode, and later to Schema 2, native mode. Before you perform the second migration, alter the `-t` option to specify the correct target Schema version and mode.

Example

```
commdirmig -i /home/user/commdirmig.input.txt
```

Logging

Use the following options to specify logging:

- `-l` *LogFile* specifes the file to which `commdirmig` writes log information. The default *LogFile* is `commdirmig.log`.
- `-v` specifes verbose (maximum) log details. The default level is standard.
- `-c` directs `commdirmig` to continue running when an error occurs. The default is to exit when an error occurs.
- `-m` *LogMazSize* specifies the maximum size of the log file. You can configure the size in kilobytes (K) or megabytes (M). Following are two examples:

  ```
  500 K
  2 M
  ```

  When you run `commdirmig` for the first time, the `-m` option is saved in a configuration file, `commdirmig-userprefs.properties`. When you run `commdirmig` again, it uses the option values stored in the configuration file. For details, see “commdirmig Configuration File” on page 76.
- `-k` checks for erroneous domain provisioning in the existing LDAP directory and reports the erroneous information to the log file.

Undo Migration

The following option allows you to undo (roll back) the changes made to the LDAP directory if an error occurs during the migration process:

- `-u` *UndoFile* directs `commdirmig` to create a log in LDIF format that can be applied to undo the migration. The log entries are saved in the *UndoFile* you specify.

If an error occurs during the migration, you can use the `ldapmodify` tool with the Undo log to roll back all the changes made by `commdirmig`. This step returns the LDAP directory to the state it was in before the migration began.

By default, `commdirmig` creates an Undo file.

By default, the *UndoFile* is named `commdirmig.undo.ldif`.

Help

Use the following options to get help information and version:

- `-h` *Option* displays help information about the specified option.
- `-?` *Option* displays help information about the specified option.
- `-V` displays the current version of the `commdirmig` utility.

Steps for Running commdirmig

You can run `commdirmig` while the Messaging and Calendar servers are online. The servers can continue to look up user entries in the LDAP directory while `commdirmig` migrates the directory data to Schema 2.

Before you run `commdirmig`, complete following tasks:

- If you intend to use a file that lists domain names (by specifying the `-f` option), create the domain-name file.
- If you intend to use an input file containing the `commdirmig` options (by specifying the `-i` option), create the input file.
- Create a file to contain the Directory Server login password. The password file must be specified as an argument with the `-w` option.

To run commdirmig, follow these steps:

1. Log in as or become superuser (root).

   By default, the commdirmig utility is located in the /opt/SUNWcomm/bin directory.

2. Run commdirmig. For the syntax, see commdirmig Syntax.

   Command-line examples are shown below.

3. After commdirmig is finished, view the commdirmig.log file to check the migration status. If errors occur during the migration or if schema entries cannot be migrated, commdirmig writes them to commdirmig.log.

   By default, the log file is located in the following directory:

   /var/opt/SUNWcomm/logs/commdirmig.log

Example 1

The following example migrates all domains in the LDAP directory from Schema 1 to Schema 2, native mode:

```
commdirmig -D "cn=Directory Manager" -w /opt/SUNWcomm/passwd -t 1 -X
ldaphost -p 389 -b "o=isp" -r "o=internet" -o -d “*”
```

Example 2

The following example does not migrate the actual directory data. It creates an LDIF audit file showing the modification requests for migrating domains siroe.com and sesta.com from Schema 1 to Schema 2, native mode:

```
commdirmig -D "cn=Directory Manager" -w /opt/SUNWcomm/passwd -t 1 -X
ldaphost -p 389 -b "o=isp" -r "o=internet" -d siroe.com -d sesta.com
```

If this example were run with the -o option, the actual directory data would be migrated.

Example 3

The following example migrates the domain varrius.com from Schema 1 to Schema 2, native mode, and adds Calendar service to all the users in the domain:

```
commdirmig -D "cn=Directory Manager" -w /opt/SUNWcomm/passwd -t 1 -X
ldaphost -p 389 -b "o=isp" -r "o=internet" -d varrius.com -S cal -o
```

commdirmig Configuration File

When you run `commdirmig` for the first time, it saves the following options in a configuration file named `commdirmig-userprefs.properties`:

`-X` *DirectoryServerHost*
`-p` *DirectoryServerPort*
`-b` *OSIRoot*
`-r` *DCRoot*
`-m` *LogMaxSize*

When you run `commdirmig` again, it uses the option values stored in the configuration file.

The `commdirmig-userprefs.properties` file is created in the following directory:

/opt/SUNWcomm/lib

How commdirmig Chooses Which Option Value to Use

The command-line version of an option overrides the *InputFile* version of the same option; the *InputFile* version overrides the configuration-file version.

That is, for a given option, `commdirmig` uses the value entered in the command line and ignores any other value for that option stored in the *InputFile* or configuration file.

If an option is not in the command line and the `-i` *InputFile* option is entered, `commdirmig` uses the value stored in the *InputFile* (if it is present), ignoring the configuration file.

Chapter 4

Upgrading and Configuring the Servers

This chapter describes how to configure the Messaging Server and Calendar Server to use LDAP Schema 2. It includes the following topics:

Guidelines for Server Configuration

The following rules and guidelines apply to server configuration:

- You must upgrade a Messaging or Calendar Server to version 6 before you can configure it to use Schema 2.
- We recommend that you upgrade the Messaging and Calendar servers before you migrate to Schema 2.
- When you upgrade a server to version 6, you can configure it to use Schema 1 (until the directory data has been migrated).
- After you migrate the directory data to Schema 2, you can reconfigure the server to use Schema 2.
- If you migrate the directory data to Schema 2, compatibility mode, configure the servers to use Schema 1.

  After you migrate the directory data from Schema 2, compatibility mode to Schema 2, native mode, you must reconfigure the servers to use Schema 2.

Configuring Messaging Server

The following procedures outline how to upgrade Messaging Server to version 6 and configure it to use Schema 2.

Upgrading Messaging Server to Version 6

To upgrade Messaging Server 5.x to Messaging Server 6, follow the instructions in "Upgrading to Sun Java System Messaging Server," in the *Messaging Server Administration Guide* (http://docs.sun.com/doc/819-0105).

Running the Directory Server Setup Script

During the upgrade process, you run the Directory Server Setup Perl script (`comm_dssetup.pl`) to configure Directory Server 5.x for Messaging Server 6 and Calendar Server 6.

The `comm_dssetup.pl` script asks you to specify which schema version Directory Server is to use by setting the `comm_dssetup.pl -t` option, as follows:

- `-t 1` — Schema 1
- `-t 1.5` — Schema 2, compatibility mode
- `-t 2` — Schema 2, native mode.

Since you are upgrading your Messaging and Calendar servers before you migrate to Schema 2, you should specify Schema 1 at this stage. If you specify Schema 1 when you run `comm_dssetup.pl`, the upgraded servers will continue to use the existing schema without interruption.

If you also have installed Calendar Server 6 and have already run `comm_dssetup.pl`, you might not need to run the script again.

NOTE You only need to run `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers. However, if you are not sure what to do, it will not hurt your system to run it again. In fact, the script checks to see if the current version has already been installed and will notify you.

Configuring Messaging Server for Schema 2

To configure Messaging Server to use Schema 2, native mode, perform these tasks:

1. Edit the `LDAP_SCHEMALEVEL` option in the `option.dat` file to support Schema 2.

2. Change the `service.dcroot` configuration parameter to point to the root of the Organization Tree (by using the `configutil` command).

These tasks are described in the sections that follow.

Step 1: Edit the Schema-Level Option in the Option File

Set the `LDAP_SCHEMALEVEL` option value to 2.

You can set the following values for the `LDAP_SCHEMALEVEL` option in the `option.dat` file:

- `LDAP_SCHEMALEVEL=1` enables Messaging Server to support Schema 1.
- `LDAP_SCHEMALEVEL=2` enables Messaging Server to support Schema 2, native mode.

For details about editing and using the `option.dat` file, see "Editing the Option File" on page 80 and "Other Options in the Option File" on page 80.

Step 2: Change the DC Root Configuration Parameter

Update the following configuration parameter with the `configutil` command:

`service.dcroot`

This parameter tells Messaging Server where to begin doing lookups in the LDAP directory.

For Schema 1, the value of this parameter is the root of DC Tree in the directory. The default value is `o=Internet`.

To configure Messaging Server to support Schema 2, change the value of `service.dcroot` to the root of the Organization Tree in the directory.

For information about using the `configutil` utility, see "Chapter 1: Messaging Server Command-line Utilities" in the *Messaging Server Administration Reference*.

Schema 2, Compatibility Mode

If you are migrating to Schema 2, compatibility mode, Messaging Server should continue to be configured to use Schema 1:

- Set the value of the `LDAP_SCHEMALEVEL` option to 1.
- Set the value of the `service.dcroot` configuration parameter to the root of the DC Tree.

In Schema 2, compatibility mode, the Messaging and Calendar servers continue to use the schema exactly as they did in Schema 1. The servers use the DC Tree to access the correct nodes in the Organization Tree. They use an RFC 2247-compliant search algorithm to look up user entries. From the Messaging and Calendar servers' perspective, Schema 1 is still in place.

At the same time, Schema 2, compatibility mode enables you to use Access Manager features such as the `commadmin` utility or single sign-on (SSO). During the migration to Schema 2, compatibility mode, Access Manager object classes, attributes, and ACIs are added to the appropriate nodes in the Organization Tree.

Editing the Option File

Each line in the `option.dat` file contains the setting for one option. An option setting has the form:

option=value

The `option.dat` file is the file specified with the `IMTA_OPTION_FILE` option in the IMTA tailor file (*msg_svr_base*`/config/imta_tailor`). By default, it is located in *msg_svr_base*`/config/option.dat`

For more information about the `option.dat` file, see "Chapter 4: MTA Configuration," in the *Messaging Server Administration Reference*.

Other Options in the Option File

Other LDAP Schema 2 options in the `option.dat` file let you customize Messaging Server's interaction with the LDAP directory.

For example, `LDAP_DOMAIN_FILTER_SCHEMA2` lets you set the LDAP search filter used for Schema, 2 domain lookups. (The default value for this option is `objectclass=sunManagedOrganization`.)

However, to configure Messaging Server to use Schema 2, you only have to set the `LDAP_SCHEMALEVEL` option. When you migrate to Schema 2, the Schema Migration Utility (`commdirmig`) automatically migrates all the current domain object classes and domain attributes from the DC Tree to the Organization Tree.

Your `option.dat` file also might contain options that customize Schema 1 values. After you migrate to Schema 2, these options become irrelevant and are not used. They do no harm. You do not have to delete Schema 1 options from the `option.dat` file.

For more information about the options available in the `option.dat` file, see "Chapter 4: MTA Configuration," in the *Messaging Server Administration Reference*.

Configuring Calendar Server

The following procedures outline how to upgrade Calendar Server to version 6, migrate Calendar Server data to version 6, and configure Calendar Server to use Schema 2.

Upgrading Calendar Server to Version 6

To upgrade Calendar Server 5.x to Calendar Server 6, follow the instructions in "Database Migration Utilities," in the *Calendar Server Administration Guide* (http://docs.sun.com/doc/819-0024).

After the upgrade / installation, you must configure Calendar Server and migrate Calendar Server data. For details, see "Post-Installation Configuration" and "Database Migration Utilities" in the *Calendar Server Administration Guide* (http://docs.sun.com/doc/819-0024).

Running the Directory Server Setup Script

During the upgrade process, you run the Directory Server Setup Perl script (`comm_dssetup.pl`) to configure Directory Server 5.x for Calendar Server 6 and Messaging Server 6.

The `comm_dssetup.pl` script asks you to specify which schema version Directory Server is to use by setting the `comm_dssetup.pl -t` option, as follows:

- `-t 1` — Schema 1
- `-t 1.5` — Schema 2, compatibility mode
- `-t 2` — Schema 2, native mode.

Since you are upgrading your Messaging and Calendar servers before you migrate to Schema 2, you should specify Schema 1 at this stage. If you specify Schema 1 when you run `comm_dssetup.pl`, the upgraded servers will continue to use the existing schema without interruption.

If you have just installed Messaging Server 6 and have already run `comm_dssetup.pl`, you do not need to run the script again.

NOTE You only need to run `comm_dssetup.pl` once for each Directory Server used by the Messaging and Calendar servers. However, if you are not sure what to do, it will not hurt your system to run it again. In fact, the script checks to see if the current version has already been installed and will notify you.

For more information about running the comm_dssetup.pl script, see "Post-Installation Instructions," in the *Calendar Server Administration Guide* (http://docs.sun.com/doc/819-0024).

Configuring Calendar Server to Use Schema 2

To configure Calendar Server to use Schema 2, you must set configuration parameters in the Calendar Server configuration file, ics.conf.

You also must set additional configuration parameters to support hosted (virtual) domains. For details, see "Configuring Calendar Server for Hosted Domain Support" on page 83.

(The Calendar Server configuration program, csconfigurator.sh, does not configure Calendar Server to use Schema 2 or to support hosted domains.)

To configure Calendar Server to use Schema 2, edit the following parameters in the ics.conf file:

- local.schemaversion

  local.schemaversion="1" specifies Schema 1. If the server is using Schema 1, you also must specify the service.dcroot parameter.

  local.schemaversion="2" specifies Schema 2. If the server is using Schema 2, you also must specify the service.schema2root parameter.

- service.dcroot

  Specifies the root suffix of the DC Tree in the LDAP directory.

  For example: "o=internet"

  service.dcroot is active when the server is using Schema 1. If the server is using Schema 2, service.dcroot is ignored.

- service.schema2root

  Specifies the root suffix in the Organization (OSI) Tree in the LDAP directory, underneath which all domains are found.

  For example: "o=sesta.com"

  service.schema2root is active when the server is using Schema 2. If the server is using Schema 1, service.schema2root is ignored.

Configuring Calendar Server for Compatibility Mode

If you are migrating to Schema 2, compatibility mode, set the `local.schemaversion` value to 1.

In Schema 2, compatibility mode, the Messaging and Calendar servers continue to use the schema exactly as they did in Schema 1. The servers use the DC Tree to access the correct nodes in the Organization Tree. They use an RFC 2247-compliant search algorithm to look up user entries. From the Messaging and Calendar servers' perspective, Schema 1 is still in place.

At the same time, Schema 2, compatibility mode enables you to use Access Manager features such as the `commadmin` utility or single sign-on (SSO). During the migration to Schema 2, compatibility mode, Access Manager object classes, attributes, and ACIs are added to the appropriate nodes in the Organization Tree.

Configuring Calendar Server for Hosted Domain Support

To support Schema 2, Calendar Server also must be configured to support hosted (virtual) domains. This section briefly summarizes the procedures for supporting hosted domains. For more information, see "Administering Hosted Domains" in the *Calendar Server Administration Guide* (`http://docs.sun.com/doc/819-0024`).

To migrate a site to use hosted domains, you must perform the following tasks:

- Run the `csvdmig` utility. For details, see "Database Migration Utilities" in the *Calendar Server Administration Guide* (`http://docs.sun.com/doc/819-0024`).
- Set additional configuration parameters in the `ics.conf` file.

Table 4-1 on page 83 describes the parameters in the `ics.conf` file used for hosted domain support. If any of the following parameters are not in the `ics.conf` file, add the parameter and its associated value to the file and then restart Calendar Server for the values to take effect.

For more information about editing the `ics.conf` file, see "Calendar Server Configuration Parameters," in the *Calendar Server Administration Guide* (`http://docs.sun.com/doc/819-0024`).

Table 4-1 Configuration Parameters for Hosted Domain Support

Parameter	Description
service.virtualdomain.support	Enables ("y") or disables ("n") support for hosted (virtual) domain mode. Default is "n".

Table 4-1 Configuration Parameters for Hosted Domain Support *(Continued)*

Parameter	Description
local.schemaversion	Specifies the version of the LDAP schema: • "1" = Schema 1. See also service.dcroot. • "2" = Schema 2. See also service.schema2root. Default is "1".
service.dcroot	Specifies the root suffix of the DC tree in the LDAP directory, if local.schemaversion = "1". For example: "o=internet". In hosted (virtual) domain mode, Calendar Server uses the service.dcroot parameter and not the local.ugldapbasedn and local.authldapbasedn parameters. Conversely, in non-hosted (virtual) domain mode, Calendar Server uses the local.ugldapbasedn and local.authldapbasedn parameters and not the service.dcroot parameter.
service.schema2root	Specifies the root suffix underneath which all domains are found, if local.schemaversion = "2". For example: "o=sesta.com".
service.defaultdomain	Specifies the default domain for this instance of Calendar Server. Used when a domain name is not supplied during a login. For example: "sesta.com".
service.loginseparator	Specifies a string of separators used for the *login-separator* when Calendar Server parses "userid[*login-separator*]domain". Calendar Server tries each separator in turn. Default is "@+".
service.siteadmin.userid	Specifies the user ID of the domain administrator. For example: DomainAdmin@sesta.com.
service.virtualdomain.scope = "select"	Controls cross domain searching: • "primary" = Search only within the domain where the user is logged in. • "select" = Search in any domain that allows the search. Default is "select".
local.domain.language	Specifies the language for the domain. Default is "en" (English).

Provisioning Rules for Hosted Domains

After you configure Calendar Server to support hosted domains (and after you migrate the directory data to Schema 2), user-developed applications and provisioning tools must use the following rules for provisioning new entries:

- User entries must be underneath the people node in the Organization Tree.
- Group entries must be underneath the group node in the Organization Tree.

Access Manager requires this hierarchy for provisioning user and group entries. Access Manager-based tools will not recognize users and groups provisioned under different nodes than the people node and group node, respectively.

Editing the Configuration File

Calendar Server configuration parameters are stored in the following file:

cal_svr_base`/etc/opt/SUNWics5/config/ics.conf`

The `ics.conf` file is an ASCII text file, with each line defining a parameter and its associated value(s). The parameters are initialized during Calendar Server installation. After installation, a user with administrator rights on the system where Calendar Server is running can edit the `ics.conf` file. You can edit the file by using a text editor such as `vi` on Solaris Systems.

For more information about editing configuration parameters in the `ics.conf` file, see “Calendar Server Configuration Parameters,” in the *Calendar Server Administration Guide* (`http://docs.sun.com/doc/819-0024`).

Glossary

Refer to the *Java Enterprise System Glossary* (http://docs.sun.com/doc/816-6873) for a complete list of terms that are used in this documentation set.

Index

SYMBOLS

A

B

C

D

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X