Comparison of Sun Java System LDAP Schema Modes for Communications Suite Products

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

Part No: 820–0639

070322@17039

Contents

◆ ◆ ◆ CHAPTER 1

Comparison of Sun Java System LDAP Schema Modes for Communications Suite Products

This article compares the Sun Java™ System LDAP schema modes used by the Sun Java Communications Suite products. It includes an overview and history of both modes, an example of domain and user LDAP entries for both schema modes, and a discussion on how to decide which mode is appropriate for you.

Article Contents

This article contains the following topics:

Before You Read This Article

This article uses the following assumptions:

- You are familiar with both LDAP databases and schema basics.
- You already have an earlier version of Sun Java System Calendar Server or Sun Java System Messaging Server software installed.
- You need to determine which of the Schema versions to use when you upgrade to the 6.3 versions of Calendar Server and Messaging Server software.

This article should supply you with enough information to understand the differences between the Schema versions and help you determine which version is best suited to your needs.

A Quick Summary of this Article's Recommendations

- You should use the same schema version for all Communications Suite products sharing the same LDAP directory.
- If you require Sun Java System Access Manager to share the same LDAP user directory with Communications Suite products, use one of the Schema version 2 modes.
- You should not use Schema version 1 mode unless you satisfy *all* of the following criteria:
  - You have an earlier version of one of the Communications Suite products already installed using Schema version 1.
  - And, you don't want to use Access Manager.
  - And, you don't want to migrate your LDAP database to either mode of Schema version 2.
- If Sun Java Communications Suite Delegated Administrator does not have the features you require, but iPlanet™ Delegated Administrator does, use Schema version 1 mode.
- If you are installing Communications Suite products for the first time, choose the Schema version 2 mode that integrates most easily with your current DIT structure. You can choose between Schema version 2 native mode or compatibility mode. The two modes are defined in "Schema Version 2 Background Information" on page 9

Overview of LDAP Schema Versions 1 and 2 Modes

This sections discusses the following topics:

What is an LDAP Schema?

Generically, an LDAP schema refers to a specific collection of LDAP object classes and attributes. The Sun Java Communications Suite provides schema definition files that are used to update the Sun Java System Directory Server with a definition of schema that are allowed for the following products: Messaging Server, Sun Java System Calendar Server and Sun Java System Instant Messaging. However, the names Schema version 1 and Schema version 2 imply more than just their unique collections of object classes and attributes. Each schema mode implies a logical layout of the application's domains in Directory Information Trees (DITs) . The structure of these DITs differs radically between the two schema modes. Each structure implies

something about how the LDAP information is accessed. This article discusses the history of the two modes, the differences in the logical structures associated with them, and the schema attribute differences.

A History of Two Schema Versions

There are two collections of object classes and attributes for Communications Suite products; that is, there are two schema versions you can choose to run in, called Schema version 1 and Schema version 2. Because of product changes over time, the collection of object classes and attributes used by Communications Suite products has been split between an older legacy version and the newer version.

Originally, the legacy schema collection was not named. To differentiate between the two schema collections, when the second collection was introduced, the terms Schema version 1 and Schema version 2 were created. The schema split occurred at the iPlanet to Sun™ ONE branding change. Both schema versions are allowed in the current products, but at configuration time, you must choose which schema version mode your system will use.

Note – Schema version 2 has two modes: native mode and compatibility mode. These modes are described in "Schema Version 2 Background Information" on page 9.

This article gives a comparison of the two schema versions, including the following topics:

- Object Classes and Attributes — Each schema version has a specific list of object classes and attributes it works with. Some of the object classes and attributes are the same in both versions, but there are also object classes and attributes that are unique to each schema version. To avoid confusion, use the same schema version for all of the Communications Suite products in your deployment that share the same LDAP database.
- Administrative Tools — The administration tools used to administer domains, users and groups are different for each schema version.

A discussion of the various consequences of choosing one schema version over the other is found in "To Migrate to Schema Version 2 or Not to Migrate" on page 20.

Schema Version 1 Mode Background Information

The chief characteristic of Schema version 1 mode is its association with the use of two DITs, a Domain Component tree (DC tree) and an Organization tree. A DIT is a logical view of the relationship between domain, user and group LDAP entries, and implies how the information can be located.

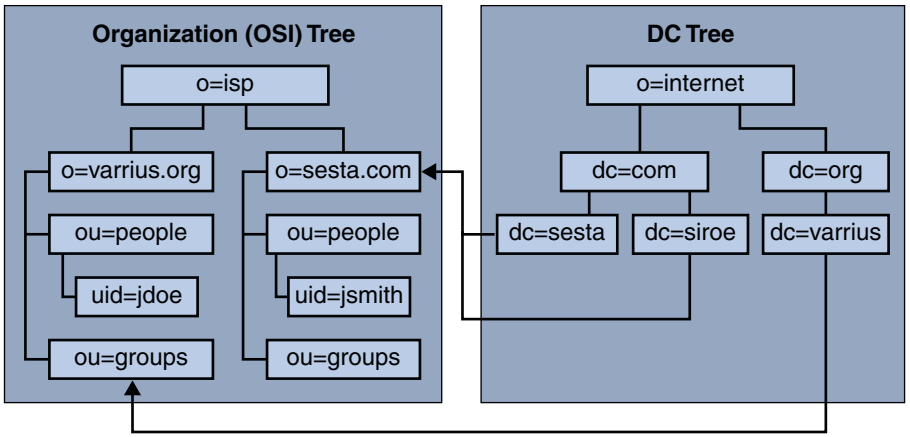

FIGURE 1–1 Schema Version 1 Two DIT Layout

For Schema version 1 mode, the domain information is carried exclusively on the DC tree. The user and group information is all carried in the Organization tree. The domain nodes on the Organization tree are just place holders and don't carry functional attributes

The server software finds the distinguished name (DN) of the Organization tree domain by reading the value of the `inetDomainBaseDN` attribute in the DC tree domain node. The system uses this DN to search the LDAP for the Organization tree domain node, under which the domain's users and groups reside.

Domain nodes that function as aliases can be created in two different ways, with or without their own routing and access information. The alias domains that contain no routing and access information of their own reference another DC tree domain node, and use that node's routing and access control information. The alias domains, more properly called index nodes, containing their own routing and access control information, reference an Organization tree domain node. For more information about Schema version 1 aliases, see "How Alias Domains Are Handled In Schema Version 1 Mode" on page 12.

The two tree layout illustrated in Figure 1–1, shows how the LDAP entries are logically structured. In the figure, arrows from the DC tree show how the nodes in the DC tree point to the domain nodes in the Organization tree. Furthermore, it shows an alias domain node in the DC tree, `siroe`. This node carries its own routing and access control information, while still pointing to the canonical domain, `sesta.com` If it did not contain its own routing and access control information, it would point to the DC tree domain where the routing and access control information it's using resides, `sesta`.

In the earlier versions of Calendar Server and Messaging Server, each product provided its own provisioning and administration utilities based on Schema version 1 mode. In addition, Messaging Server offered the iPlanet Delegated Administrator GUI for provisioning and administration in the Schema version 1 environment, as well as an Administration Server GUI that was separately installable.

Schema Version 2 Background Information

With the release of Sun ONE Calendar Server, a new schema was introduced to provide compatibility with the Sun ONE Access Manager product, which was the new authentication and identity management product introduced in the Sun ONE branded software family. This new schema was called Schema version 2 to distinguish it from the heretofore unnamed Schema version 1. It has two modes that can be selected at configuration time: native mode and compatibility mode.

Schema version 2 native mode — This mode is associated with a single DIT LDAP layout containing an Organization tree, but no DC tree. For an example of this kind of layout, see Figure 1–2. In this mode, all domain nodes and their attributes are found in the Organization tree. Schema version 2 native mode is the default LDAP layout for new installations of Communications Suite products.

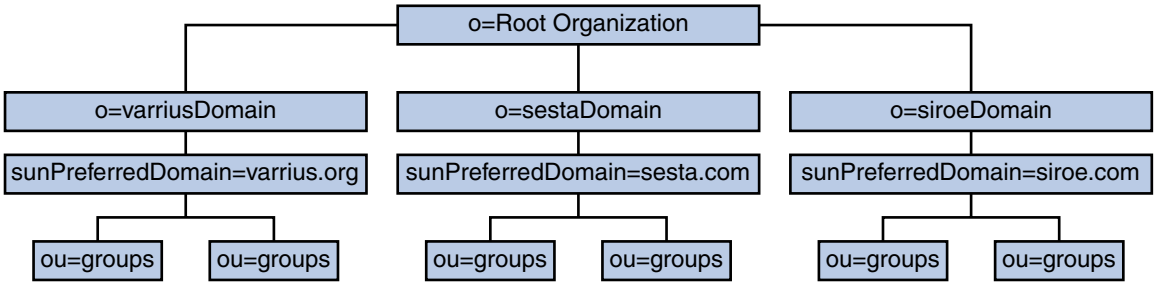

FIGURE 1–2 Schema Version 2 Native Mode One DIT Layout

Access Manager does not recognize hierarchical domain structures; therefore all domain nodes for this mode must be located only under the root node. No nesting of organizations is allowed in this schema layout. Another limitation of Schema version 2 native mode with Access Manager is the inability to define index nodes (alias domains) that carry alternate routing and access control information. In Schema version 2 native mode, the only kind of aliasing allowed is the simple kind which are just other names for the canonical domain. That is, all aliases must use the same routing and access control information as the actual domain.

Schema version 2 compatibility mode — This mode is the exception to this one tree structure. It uses the same two DIT layout as in Schema version 1 mode, with an Organization tree and a DC tree. However, unlike Schema version 1 mode, in Schema version 2 compatibility mode, the Organization tree domain nodes do carry some domain information. That is, they are decorated with an `icsStatus` attribute.

Tip – Compatibility mode is called Schema version 1.5 in the postinstallation scripts.

A new command-line utility, `commadmin`, was introduced for administration of Schema version 2 LDAP entries. This utility allowed an administrator to provision and manage domains, users and groups in Schema version 2 mode from a command line. The utility used the Access

Manager SDK to create LDAP records compatible with Access Manager. Later the software product line was rebranded as Java Enterprise System. In Java Enterprise System 2005Q1, the Sun Java System Communications Services Delegated Administrator Console was introduced. It is a graphical user interface (GUI) with functionality similar to the command-line utility.

Originally the Delegated Administrator Console only supported administration of Messaging Server users. It now supports administration of both Calendar Server and Messaging Server domains, users and groups. However, there is some disparity between the functionality of the two tools. For a list of the differences, see "Functional Differences Between the Delegated Administrator Console and Utility" on page 23.

Tip – If Access Manager is not required, Schema version 2 native mode can be used to provision an Organization tree containing hierarchical (nested) organizations and index node aliases as in Schema version 1 mode.

For customers with Schema version 1 mode installations who wish to migrate to one of the Schema version 2 modes, there is a Schema Migration Utility. For more information on how to migrate your LDAP from Schema version 1 mode to one of the Schema version 2 modes, see *Sun Java Communications Suite 5 Schema Migration Guide*.

The next section contains more detailed information about the three schema modes just described: Schema version 1, Schema version 2 native mode, and Schema version 2 compatibility mode.

Differences Between the Three Schema Modes

This section contains more information about the three schema types described earlier: Schema version 1, Schema version 2 native mode and Schema version 2 compatibility mode. This section contains the following topics:

For more detailed information about domain structures for Schema version 1 mode and Schema version 2 mode, see the "inetCanonicalDomainName" in *Sun Java Communications Suite 5 Schema Reference*.

How Domain Searches Work

Schema version 1 mode	The DC tree domain entry is found using an LDAP lookup. Messaging Server lookup code builds the DN needed for the lookup using the domain

	specified to the right of the separator (@) in the email address. For Calendar Server the DN is created from the domain name in the fully qualified unique identifier, *uid*. Once retrieved, the entry is processed as described in "How Alias Domains Are Handled In Schema Version 1 Mode" on page 12.
	Tip – For Messaging Server, if the original search did not find a match in the DC tree, the `DOMAIN_UPLEVEL` option can be used to search a domain from one level higher in the tree. You must set this option to a value of either `1` or `3` to enable uplevel searches. The default is for this feature to be turned off. For more information on this option, see the *Sun Java System Messaging Server 6.3 Administration Guide*.
Schema version 2 native mode	This mode implements the Access Manager model, with all domain nodes residing directly below the root node. Messaging Server and Calendar Server retrieve the correct LDAP domain entry using a search template. The system compares each node with the search criteria until it finds the correct domain. All domains are treated as if they were at the same level. There is no hierarchical structure for retrieval. once retrieved, the entry is processed as described in "How Alias Domains are Handled in Schema Version 2 Native Mode" on page 12.
Schema Version 2 compatibility mode	Search queries are constructed using templates as with native mode, but the LDAP entry retrieved is in the DC tree. Once retrieved, the domain LDAP entry is processed as if it were Schema version 1 mode. For more information, see "How Alias Domains are Handled in Schema Version 2 Compatibility Mode" on page 13.

Note – While earlier Calendar Server versions supported multiple domains, it was optional. In a non-domain environment, all user and group records are located directly under the root, with no domain node present. However, starting with Calendar Server 6.3, the system default is for multiple domains. That is, the system assumes at least one domain below the root for all schema modes.

How Alias Domains Are Handled In Schema Version 1 Mode

When the system finds the DC tree domain node with the appropriate name, it checks to see if it's an alias, index node, or the canonical domain. The canonical DC tree domain has the same name as the Organization tree containing the user and group records. This is the official name of the domain. For Messaging Server, this canonical domain name determines the name of the domain in the message store hierarchy where users' inboxes are located. The system retrieves the DN for the corresponding Organization tree domain from the `inetDomainBaseDN` attribute found in the DC tree canonical domain.

If the DC tree domain does not have the same name as the corresponding Organization tree domain, it is not the canonical domain. It is an alias, or an index node, and must carry either the `inetCanonicalDomainName` attribute or the `aliasedObjectName` attribute.

When a DC tree domain node carries the `aliasedObjectName` attribute, it is an alias that contains no routing or access control information. The attribute value is used to find the DC tree canonical domain node where the routing and access control information for this alias resides.

When a DC tree domain node carries the `inetCanonicalDomainName` attribute, it is an index node. This type of alias contains its own routing and access control information, which can be different than the information carried on the DC tree canonical domain. The system uses the value of the `inetCanonicalDomainName` attribute to find the name of the Organization tree domain node, under which user and group records for this index node alias reside.

If neither the `aliasedObjectName` attribute, nor the `inetCanonicalDomainName` attribute is present in the DC tree domain, then the system assumes it is the canonical domain and uses the value of the `inetDomainBaseDN` attribute to find the Organization tree domain.

How Alias Domains are Handled in Schema Version 2 Native Mode

In Schema version 2 native mode, as implemented for use with Access Manager, no hierarchy is allowed. That is, all domain nodes (base nodes) must reside directly below the root node. Index nodes are not allowed. This means a loss of functionality from Schema version 1 mode since index nodes containing alternate routing and access control information can't be created. However, aliases with the same routing information as the base node can be created by adding

one `associatedDomain` attribute for each alias domain name to the Organization node domain entry. Note that the `inetCanonicalDomainName` attribute is not used.

In Schema version 2 native mode without Access Manager, both base and index nodes can be created in the Organization tree using a hierarchical structure. Index nodes can contain different routing and access control information, similar to index nodes found in the DC tree for Schema version 1 mode. Index nodes are decorated with the `inetCanonicalDomainName` attribute, as in Schema version 1 mode. However, the alias domains found in Schema version 1 mode don't exist in Schema 2 native mode. They have been replaced by the use of the `associatedDomain` attribute decorating the canonical domain.

How Alias Domains are Handled in Schema Version 2 Compatibility Mode

In Schema version 2 compatibility mode, the domain structure is the same as in Schema version 1 mode. Aliasing works the same way as described for Schema version 1 mode. The only difference is that the Organization tree domain nodes each carry an `icsStatus` attribute.

Comparing Domain LDAP Entries for Schema Version 1 and Schema Version 2 Native Mode

This section contains example domain LDAP entries for Schema version 1 and for Schema version 2 native mode. The Schema version 2 native mode entry reflects Delegated Administrator's services orientation, including many `sunRegisteredServiceName` attributes. The main difference between the two schema versions for domains and users are the object classes and attributes required by the administration tools used by each. These are called out in the examples that follow.

For more information on schema object classes and attributes for each administration tool, see *Sun Java Communications Suite 5 Schema Reference*.

EXAMPLE 1–1 Schema Version 1 DC Tree Top Level Entries

This is the domain entry for the top level domain that does not carry the routing information.

```
dn: dc=com, o=internet
objectClass: domain
objectClass: top
dc: com

dn: dc=sesta, dc=com, o=internet
objectClass: domain
objectClass: top
```

EXAMPLE 1–1 Schema Version 1 DC Tree Top Level Entries *(Continued)*

```
dc: sesta
```

EXAMPLE 1–2 Schema Version 1 DC Tree Domain Entry

This is the domain entry for the canonical domain. That is, the Organization tree domain has the same name as this DC tree domain.

Notice the iPlanet Delegated Administrator object class `nsManagedDomain`.

```
dn: dc=red, dc=sesta, dc=com, o=internet
objectClass: top
objectClass: domain
objectClass: inetDomain
objectClass: icsCalendarDomain
objectClass: nsManagedDomain
dc: red
description: DC node for red.sesta.com hosted domain
inetDomainBaseDN: o=red.sesta.com,o=mailQA
inetDomainStatus: active
icsStatus: active
icsExtendedDomainPrefs: domainaccess=@@d^a^lsfrwd^g;anonymous^a^r^g;@^a^s^g
icsExtendedDomainPrefs: calmasterUid=calmaster
icsDomainNames: red.sesta.com
```

EXAMPLE 1–3 Schema Version 1 Organization Tree Domain Entry

This is the domain entry in the Organization tree for the `red.sesta.com` canonical domain.

Notice the iPlanet Delegated Administrator object class `nsManagedDomain`.

```
dn: o=red.sesta.com,o=isp
objectClass: top
objectClass: organization
objectClass: nsManagedDomain
o: red.sesta.com
nsNumUsers: 50
```

EXAMPLE 1–4 Schema Version 2 Domain Entry

Notice the inclusion of the Delegated Administrator class `sunDelegatedOrganization`. Also notice the following Access Manager object classes: `sunNamespace`, and `sunManagedOrganization`. The attributes listed starting with “sun” all come from these object classes.

EXAMPLE 1–4 Schema Version 2 Domain Entry *(Continued)*

```
dn: o=red.sesta.com, o=sestaMail
objectClass: inetdomainauthinfo
objectClass: sunismanagedorganization
objectClass: top
objectClass: sunnamespace
objectClass: sundelegatedorganization
objectClass: sunmanagedorganization
objectClass: maildomain
objectClass: icscalendardomain
objectClass: organization
o: red.sesta.com
sunNameSpaceUniqueAttrs: uid
sunPreferredDomain: red.sesta.com
inetDomainStatus: active
sunOrgType: full
preferredMailHost: spartan.red.sesta.com
mailDomainStatus: active
icsStatus: Active
icsExtendedDomainPrefs: domainaccess=@@d^a^lsfrwd^g;anonymous^a^r^g;@^a^s^g
icsExtendedDomainPrefs: calmasterUid=calmaster
icsDomainNames: red.sesta.com
sunRegisteredServiceName: DomainMailService
sunRegisteredServiceName: GroupMailService
sunRegisteredServiceName: UserMailService
sunRegisteredServiceName: iPlanetAMAuthService
sunRegisteredServiceName: UserCalendarService
sunRegisteredServiceName: iPlanetAMAuthLDAPService
sunRegisteredServiceName: DomainCalendarService
sunNumUsers: 64
```

Comparing User LDAP Entries for Schema Version 1 and Schema Version 2 Modes

User LDAP entries for Schema version 1 mode and Schema version 2 modes reflect the products that use them. They carry different object classes and attributes depending on which other products and administration tools access them. For example, for Schema version 2 modes with Access Manager, many Access Manager attributes starting with “iplanet-am-” are added to user entries. For Schema version 1 mode, the iPlanet Delegated Administrator object class `nsManagedPerson` and its attributes are added to user entries.

This section contains examples of user LDAP entries for both schemas for Messaging Server and Calendar Server.

- "Examples of User LDAP Entries for Messaging Server" on page 16
- "Examples of User LDAP Entries for Calendar" on page 18

For more information on schema object classes and attributes used by the administration tools, see *Sun Java Communications Suite 5 Schema Reference*

Examples of User LDAP Entries for Messaging Server

This section contains examples of user LDAP entries for Schema version 1 and Schema version 2 modes. The Schema version 1 mode entry is larger and more complete. The Schema version 2 mode entry illustrates a minimal user entry.

EXAMPLE 1–5 Schema Version 1 Mode User LDAP Entry for Messaging Server

Notice the iPlanet Delegated Administrator object class `nsManagedPerson`.

```
uid=mj123456789,ou=People,o=red.sesta.com, o=SestaMail
sunUCDefaultEmailHandler=uc
givenName=Mike
objectClass=top
objectClass=person
objectClass=organizationalPerson
objectClass=inetOrgPerson
objectClass=inetUser
objectClass=inetSubscriber
objectClass=ipUser
objectClass=userPresenceProfile
objectClass=inetMailUser
objectClass=inetLocalMailRecipient
objectClass=nsManagedPerson
objectClass=sunUCPreferences
sunUCTheme=uwc
nsdaCapability=mailListCreate
sunUCTimeZone=America/Los_Angeles
mailQuota=-1
uid=mj123456789
mail=michael.jonese@sesta.COM
cn=Mike Jones
initials=MJ
inetUserStatus=active
mailHost=mail1.red.sesta.com
sn=Jones
mailMsgQuota=-1
pabURI=ldap://mail1.red.sesta.com:389/    \\
    ou=mjones,ou=People,o=red.sesta.com,o=SestaMail,o=pab
mailAutoReplyTimeout=168
```

EXAMPLE 1–5 Schema Version 1 Mode User LDAP Entry for Messaging Server *(Continued)*

```
mailDeliveryOption=mailbox
mailDeliveryOption=autoreply
sunUCDateFormat=M/D/Y
sunUCDateDelimiter=/
sunUCTimeFormat=12
vacationEndDate=20050219182103Z
vacationStartDate=20050217182103Z
mailAutoReplySubject=Auto-reply - I am out of the office
mailAutoReplyTextInternal=This is an automatic reply.
mailAutoReplyText=This is an automatic reply.
mailAlternateAddress=Mike.Jones@red.sesta.com
mailAlternateAddress=mjones@mail1.red.sesta.com
mailUserStatus=active
userPassword= password
```

EXAMPLE 1–6 Schema Version 2 Modes User LDAP Entry for Messaging Server

Notice the Access Manager object classes `iplanet-am-managed-person`, `iplanet-am-user-service`, and `iplanetpreferences`. Likewise, the attributes from these object classes are `iplanet-am-modifiable-by`, and `preferredLanguage`.

Sometimes an object class in included but none of its attributes are currently used. This can be done to simplify the addition of further attributes later, without having to add the object class, but its not mandatory.

```
dn: uid=jdoe,ou=People,o=sesta.com,o=sestMail
objectClass: top
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: inetadmin
objectClass: organizationalperson
objectClass: person
objectClass: userpresenceprofile
objectClass: inetuser
objectClass: inetlocalmailrecipient
objectClass: iplanetpreferences
objectClass: ipuser
objectClass: inetorgperson
objectClass: inetsubscriber
objectClass: inetmailuser
sn: jdoe
mailDeliveryOption: mailbox
cn: John Doe
uid: jdoe
```

EXAMPLE 1–6 Schema Version 2 Modes User LDAP Entry for Messaging Server *(Continued)*

```
iplanet-am-modifiable-by: cn=Top-level Admin Role,o=mailQA
mail: jdoe@sesta.com
givenName: John
mailHost: toystory2.red.sesta.com
mailUserStatus: active
inetUserStatus: Active
userPassword: password
preferredLanguage: en
```

Examples of User LDAP Entries for Calendar

This section contains examples of user LDAP entries for Schema version 1 and Schema version 2 modes. The Schema version 1 mode entry is larger and more complete. The Schema version 2 modes entry illustrates a minimal user entry. This illustrates that user entries can be very complex or very minimal, depending on your needs.

For more information on schema object classes and attributes, see *Sun Java Communications Suite 5 Schema Reference*.

EXAMPLE 1–7 Schema Version 1 Mode User Entry for Calendar Server

```
cn=Michael Jones,ou=people,dc=sesta,dc=com
objectClass=icsCalendarUser
objectClass=emailPerson
objectClass=inetOrgPerson
objectClass=inetadmin
objectClass=inetuser
objectClass=mailRecipient
objectClass=organizationalPerson
objectClass=person
objectClass=sunOrganizationalPerson
objectClass=top
objectClass=sunUCPreferences
objectClass=inetLocalMailRecipient
objectClass=inetMailUser
objectClass=ipUser
cn=Michael Jones
mail=Michael.Jones@sesta.com
mailAlternateAddress=mjones@sesta.com
mailAlternateAddress=mikej@sesta.COM
preferredrfc822recipient=Michael.Jones@sesta.com
rfc822recipient=Michael.Jones@Sun.com
rfc822recipient=Michael.Jones@west.sesta.com
```

EXAMPLE 1–7 Schema Version 1 Mode User Entry for Calendar Server *(Continued)*

```
sn=Jones
uid=mj123456789
inetUserStatus=active
sunwmailserverdomain=west
userPassword={crypt}e/UnVTLVBX71s
nswmExtendedUserPrefs=UWCMailPreferencesInitialized=true
nswmExtendedUserPrefs=mepabmigration=1
icsCalendar=mj123456789@sesta.com
icsTimezone=America/Los_Angeles
icsFirstDay=1
icsFreeBusy=mj123456789@sesta.com
icsExtendedUserPrefs=sunCalInitialized=true
icsExtendedUserPrefs=ceColorSet=pref_group_3
icsExtendedUserPrefs=ceToolText=1
icsExtendedUserPrefs=ceToolImage=1
icsExtendedUserPrefs=ceFontFace=PrimaSans BT,Verdana,sans-serif
icsExtendedUserPrefs=ceExcludeSatSun=0
icsExtendedUserPrefs=ceGroupInviteAll=1
icsExtendedUserPrefs=ceAllCalendarTZIDs=1
icsExtendedUserPrefs=ceShowCompletedTasks=false
icsExtendedUserPrefs=ceDefaultCategory=Business
icsExtendedUserPrefs=ceDayHead=9
icsExtendedUserPrefs=ceDayTail=16
icsExtendedUserPrefs=ceInterval=PT0H30M
icsExtendedUserPrefs=ceWeekEndDays=1,7
icsExtendedUserPrefs=ceIncludeWeekendInViews=true
icsExtendedUserPrefs=ceSingleCalendarTZID=0
icsExtendedUserPrefs=ceNotifyEnable=1
icsExtendedUserPrefs=ceDefaultAlarmEmail=Michael.Jones@sesta.com
icsExtendedUserPrefs=ceNotifyEmail=Michael.Jones@sesta.com
icsExtendedUserPrefs=ceDefaultView=weekview
icsDWPHost=cal1
icsCalendarOwned=mj123456789@sesta.com:meetings
icsCalendarOwned=mj123456789@sesta.com:Birthdays$Birthdays
icsCalendarOwned=mj123456789@sesta.com:Test$Test Calendar
icsSubscribed=pgreen@sesta.com$pgreen
icsSubscribed=russs@sesta.com$Russ Smith
```

EXAMPLE 1–8 Schema Version 2 Modes User LDAP Entry for Calendar Server

```
dn: uid=jdoe,ou=People,o=sesta.com,o=mailqa
objectClass: iplanetpreferences
objectClass: iplanet-am-user-service
objectClass: iplanet-am-managed-person
objectClass: top
```

EXAMPLE 1–8 Schema Version 2 Modes User LDAP Entry for Calendar Server *(Continued)*

```
objectClass: icscalendaruser
objectClass: organizationalperson
objectClass: inetadmin
objectClass: ipuser
objectClass: inetorgperson
objectClass: person
objectClass: inetuser
sn: user2
cn: test user2
icsStatus: Active
icsCalendar: jdoe@sesta.com
icsFirstDay: 2
uid: jdoe@sesta.com
iplanet-am-modifiable-by: cn=Top-level Admin Role,o=mailQA
icsTimezone: America/Denver
mail: jdoe@sesta.com
givenName: John
inetUserStatus: Active
userPassword: {SSHA}jlwkaCB8YO/DfaqNWVMZ1bF3DDgvfGJorXu5VA==
```

To Migrate to Schema Version 2 or Not to Migrate

While the examples given earlier in this document don't show a single user record with both calendar and messaging services, you might want both software applications to share the domain, user and group LDAP entries. If you do want both applications to share the same LDAP, they must both use the same schema mode.

This section discusses the things you need to consider about two products sharing the same LDAP entries, in order to help you decide whether its necessary to migrate your Schema version 1 LDAP to one of the Schema version 2 modes.

This section contains the following topics:

Facts About Schema Version 1 and Schema Version 2 Modes

If you have an earlier version of one of the Communications Suite products installed in Schema version 1 mode, and want to install a second product, you might be tempted to avoid migrating your Schema version 1 mode LDAP to a Schema version 2 mode. If so, consider the following facts:

- For Schema version 1 mode, there is not one unified tool to use for user, group, resource and domain administration.

  For Calendar Server, only command-line utilities are available, no GUI.

  For Messaging Server, there are three separate tools used, a command-line utility, a GUI (iPlanet Delegated Administrator) and the Administration Server Console. None of these tools support Calendar Server. In Communications Suite 5, the latter two are deprecated and are no longer included in the distribution.
- While it is possible to run both products in Schema version 1 mode, it places a lot of burden on the system administrators to keep it all straight and avoid deleting something the other product needs.

  Schema version 1 based Calendar Server administration utilities allow entries to be fully deleted (purged) from LDAP without regard to another product's dependence on the entries. Thus, the administrator must be responsible for the integrity of the LDAP for both products. The administrator of a deployment of two products using Schema version 1 might find it difficult to avoid inadvertent purges or unwanted changes to a user's LDAP record. For the same reason, you should not attempt to have both a Schema version 1 mode product and a Schema version 2 mode product share the same LDAP.
- Keeping your older Calendar Server deployment in Schema version 1 non-domain mode is no longer possible. Calendar Server 6.3 software automatically converts Schema version 1 non-domain configurations to multiple domain mode by creating a single default domain under the root at configuration time and assuming all non-fully qualified `uid`'s imply the default domain. For Calendar Server 6.3, you can't avoid multiple domain mode.
- Access Manager won't work with a Schema version 1 LDAP entries.
- To Use Schema version 2 in either mode and its administration tool, Delegated Administrator, you must have Access Manager installed in legacy mode.
- For Schema version 2 modes, there is one unified tool, Delegated Administrator Console (GUI) and its command-line utility equivalent, `commadmin`. You can administer both Calendar Server and Messaging Server domains, users and groups with these tools. Using a Delegated Administrator interface for both services, prevents an administrator from inadvertently deleting another service's LDAP entries.
- If you plan to use Access Manager, you must choose one of the Schema version 2 modes for both Messaging Server and Calendar Server deployments.

Administration Tools for LDAP Entries in Both Schema Versions

This section lists the various tools used to administer LDAP in Schema version 1 mode.

- For Schema version 1 mode, the following tools apply:
  - iPlanet Delegated Administrator (Messaging only) — This software is deprecated and no longer bundled in the distribution.
  - Administration Server Console (Messaging only) — This software is deprecated and no longer bundled in the distribution.
  - Messaging Server command-line utility
  - Calendar Server command-line utilities (many)

    For information about these command-line utilities, see *Sun Java System Calendar Server 6.3 Administration Guide*.

  For Schema version 2 mode. the following tools apply:

  - Delegated Administrator Utility (Command-line)
  - Delegated Administrator Console (GUI)

Conclusions

Based on the facts presented in this article, here are some possible scenarios and conclusions:

Our deployment is using the Access Manager software installed in legacy mode.

Choose Schema version 2 native mode for both Calendar Server and Messaging Server products at configuration time.

If you have an existing two DIT LDAP structure with a DC tree, and you don't want to migrate to a single DIT structure, you can choose Schema version 2 compatibility mode.

We have Access Manager installed in Realm mode and want to add Communications Suite products.

You must have Access Manager installed in legacy mode in order to use Delegated Administrator.

Our deployment isn't using the Access Manager product. We don't have an existing product installed and there are no previous LDAP entries.

Install Access Manager in legacy mode to enable Delegated Administrator. Choose Schema version 2 native mode for both Calendar Server and Messaging Server products at configuration time. Delegated Administrator creates Access Manager-ready LDAP records, but you are not required to implement any other Access Manager features.

We have a two DIT LDAP structure, and we are willing to change to a single DIT LDAP structure.

Choose Schema version 2 native mode. Migrate your existing LDAP database to Schema version 2 mode. Use Delegated Administrator interfaces to administer domains, users and groups.

We have a two DIT LDAP structure, and we don't wish to change to a single DIT LDAP structure.

Choose Schema version 2 compatibility mode for both calendar and messaging applications.

We have a Schema version 1 two DIT LDAP structure, and don't wish to migrate it to Schema version 2 mode.

You can choose to keep all Communications Suite products in Schema version 1 mode, but administration of two products in Schema version 1 mode will be difficult and involve many different interfaces, some of which are deprecated.

For further information on migrating your old Schema version 1 mode system to Schema version 2 mode, see *Sun Java Communications Suite 5 Schema Migration Guide*.

Functional Differences Between the Delegated Administrator Console and Utility

The Delegated Administrator Console and the Delegated Administrator Utility (commadmin) have some differences in functionality. This section covers those differences and includes the following topics:

- "Functions in Utility but not in Console" on page 23
- "Functions in Console but not in Utility" on page 24

Functions in Utility but not in Console

The following functions can be done in the Utility, but not in the Console:

- The purge command, `commadmin domain purge`, permanently removes a user, group, or calendar resource from the LDAP directory. The console can only mark the LDAP entries for deletion, but the purge utility actually deletes them.

  This restriction is purposefully set up to protect the LDAP from an administrator inadvertently permanently removing entries.

- The debug command, `commadmin debug log`, creates a debug log; it cannot be done in the console.

Functions in Console but not in Utility

The following functions can be done in the Console but not in the Utility:

- Create and manage service packages.

  With the utility, you can use the `-S mail,cal` option to add mail and calendar services to a resource, but this does not let you assign a set of service attributes with specific values, as you can do with service packages.
- Manage Service Provider Administrators (SPAs) and provider organizations.

  To create a Service Provider Administrator and provider organization, you must use `LDIF` files and directly write to LDAP using LDAP tools. Also, the Top Level Administrator (TLA) does not have administrative control over provider organizations; they appear as regular organizations to the TLA. And a TLA cannot create an SPA. Once they are created, you can modify and delete them in the Console.
- Create and manage shared organizations and full organizations subordinate to a provider organization.

For more information on the Delegated Administrator Console and Utility, see *Sun Java System Delegated Administrator 6.4 Administration Guide*.