



Sun Java™ System

Communications Services 6 Delegated Administrator 代理

2005Q1

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

☎ 件號碼 : 819-1104

Copyright © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版權所有。

Sun Microsystems, Inc. 對本文件所述產品所採用的技術擁有相關智慧產權。特別是 (但不僅限於)，這些智慧產權可能包括一項或多項在 <http://www.sun.com/patents> 上列出的美國專利，以及一項或多項美國和其他國家 / 地區的其他專利或待批專利。

本產品包含 SUN MICROSYSTEMS, INC. 的機密資訊和商業秘密。未經 SUN MICROSYSTEMS, INC. 事先明確的書面許可，禁止使用、公開或複製本產品。

美國政府權利 - 商業軟體。政府使用者均應遵守 Sun Microsystems, Inc. 的標準授權合約和 FAR 及其增補文件中的適當規定。

本發行物可能包含由協力廠商開發的材料。

產品的某些部份可能源自 Berkeley BSD 系統，並經加州大學授權。UNIX 是在美國和其他國家 / 地區的註冊商標，由 X/Open Company, Ltd 獨家授權。

Sun、Sun Microsystems、Sun 標誌、Java、Solaris、JDK、Java Naming and Directory Interface、JavaMail、JavaHelp、J2SE、iPlanet、Duke 標誌、Java Coffee Cup 標誌、Solaris 標誌、SunTone Certified 標誌和 Sun ONE 標誌是 Sun Microsystems, Inc. 在美國和其他國家 / 地區的商標或註冊商標。

所有 SPARC 商標均在授權下使用，它們是 SPARC International, Inc. 在美國和其他國家 / 地區的商標或註冊商標。帶有 SPARC 商標的產品均基於 Sun Microsystems, Inc. 開發的架構。

Legato 和 Legato 標誌是 Legato Systems, Inc. 的註冊商標，Legato NetWorker 是 Legato Systems, Inc. 的商標或註冊商標。Netscape Communications Corp 標誌是 Netscape Communications Corporation 的商標或註冊商標。

OPEN LOOK 和 Sun(TM) 圖形化使用者介面由 Sun Microsystems, Inc. 為其使用者和被授權者開發。Sun 感謝 Xerox 在研究和設計電腦業中視覺化或圖形化使用者介面這個觀念上所作的領先努力。Sun 保有 Xerox 對 Xerox 圖形化使用者介面非獨佔性的授權，這項授權也涵蓋獲得 Sun 授權使用 OPEN LOOK GUI 並符合 SUN 的書面授權合約的廠商。

本產品包含由卡內基美隆大學之 Computing Services 開發的軟體 (<http://www.cmu.edu/computing/>)。

本服務手冊所涵蓋的產品和包含的資訊受到美國出口控制法規的控制，並可能受到其他國家 / 地區進出口法規的管轄。嚴禁核子武器、飛彈、生化武器或海上核動力裝備等最終用途或最終使用者直接或間接使用本產品。嚴禁向受到美國禁運的國家 / 地區或美國出口除外清單 (包括但不僅限於被拒人清單和特別指定的國家 / 地區清單) 上標識的實體出口或再出口本產品。

本文件以「現狀」提供，所有明示或暗示的條件、陳述與保證，包括對於適銷性或非侵權行為的任何暗示性保證在內，均恕不負責，除非此免責聲明在法律上被認為無效。

目錄

前言	7
本書適冊對象	7
閱讀本書之前	8
本書架構	8
本書採冊的慣例	9
印刷排版慣例	9
符號	10
預設路徑和檔案名稱	10
指令行提示符號	11
相關物件	11
Messaging Server 物件	11
Calendar Server 物件	12
Communications Services 物件	12
存取 Sun 線上資源	13
聯絡 Sun 技術支援	13
協力廠商物件	13
Sun 歡迎您提出寶貴意見	13
第 1 章 Delegated Administrator 簡介	15
簡介	15
Delegated Administrator 公用程式	16
Delegated Administrator 主控台	16
Delegated Administrator 和LDAP 目錄	17
佈建使用者的分析藍本	17
單層次階層	17
雙層次階層	18
三層次階層	19
管理員角色和目錄階層	21
支援單層次階層的目錄結構	21
單層次階層：根代碼之下的預設社團組織	21

單層次階層：根基礎上的預見社會組織	22
支援雙層次階層的目錄結構	23
頂層管理員角色	23
社會組織管理員角色	24
若原為 iplanet Delegated Administrator 的使用者	25
服務套裝軟體	25
服務等級定義	26
檢查延伸式服務套裝軟體的限制	27
服務等級範本	27
預見服務等級範本	28
服務等級範本的範例	28
建立您自己的服務套裝軟體	29
指定至 LDAP 使用者項目的服務套裝軟體範例	30
服務等級定義和套裝軟體的位置	30
服務等級範本範例中的郵件服務層級	31
Platinum	31
Gold	31
Silver	31
Bronze	31
Ruby	32
Emerald	32
Diamond	32
Topaz	32
第 2 章 安裝和配置控制	33
取得您的 Delegated Administrator 配置資訊	33
Delegated Administrator 元件	33
Web 伺服器	34
配置資訊	34
執行 Java Enterprise System 安裝程式	37
執行 Directory Server 設定程序檔	39
在目錄中合併計算 ACI	39
配置 Delegated Administrator	39
配置 Messaging Server 和 Calendar Server	40
第 3 章 配置 Delegated Administrator	41
選擇要配置的元件	41
執行配置程式	43
啟動配置	43
配置 Delegated Administrator 公用程式	45
配置 Delegated Administrator 主控台	46
Web Server 配置	47

Application Server 7.x 配置	48
Application Server 8.x 配置	50
配置 Delegated Administrator 伺服器	51
完成配置	54
重新啟動 Web 伺服器	55
由 config-command 程式所建立的配置和記錄檔	55
配置檔	55
記錄檔	56
執行無訊息安裝	56
執行 Delegated Administrator 主控台和公用程式	57
啟動主控台	57
執行指令行公用程式	57
配置後作業	58
在預設網域中新增郵件和行事曆服務	58
建立服務套裝軟體	58
預先定義服務等級範本	58
建立您自己的服務套裝軟體	59
新增 Schema 2 相容性模式的 ACI	61
第 4 章 配置 Delegated Administrator	65
使服務整體的預設值配置喜好的郵件主機	65
為 Delegated Administrator 新增外掛程式	66
啟用作外掛程式	67
外掛程式格式	68
兩個外掛程式的其他平面檔案	68
自訂使用者登入	69
如何設定使用者登入值	69
新增使用者登入值	69
第 5 章 指令行公用程式	71
執行模式	72
指令檔格式	73
指令描述	74
必要的 commadmin 選項	74
commadmin admin add	74
commadmin admin remove	76
commadmin admin search	77
commadmin domain create	78
commadmin domain delete	81
commadmin domain modify	83
commadmin domain purge	85
commadmin domain search	87

commadmin group create	89
commadmin group delete	91
commadmin group modify	93
commadmin group search	96
commadmin resource create	98
建立資源	100
commadmin resource delete	101
commadmin resource modify	102
commadmin resource search	104
commadmin user create	106
commadmin user delete	108
commadmin user modify	110
commadmin user search	114
附錄 A 服務提供者管理員及服務提供者社區組織	117
服務提供者管理員	117
服務提供者管理員角色	119
指定 SPA 角色給一個使用者	120
此發行版本的注意事項	121
服務提供者管理員所管理的社區組織	121
提供者社區組織	121
完整社區組織	122
共隸社區組織	122
建立提供者社區組織及服務提供者管理員	122
範本所建立的項目	123
範本中「裝訂」自訂服務提供者範本的節點	124
建立提供者社區組織、下層社區組織及 SPA 所需的資訊	125
定義提供者及下層社區組織之參數	125
定義 SPA 的參數	129
建立提供者社區組織及服務提供者管理員的步驟	130
自訂服務提供者範本	131
da.provider.skeleton.idif 檔案 (相關的區段)	132
範例服務提供者社區組織資料	136
範例資料所提供的社區組織	136
邏輯階層結構和目錄資訊樹	137
範例社區組織資料：目錄資訊樹檢視	137
.....	139
附錄 B 屬性值和行事曆字串	141
屬性值	141
行事曆時區字串	143

附錄 C 除錯 Delegated Administrator	147
除錯指令行公用程式	147
Delegated Administrator 主控台記錄	147
Delegated Administrator 伺服器記錄	148
Web 伺服器伺服器記錄	149
Web Server	149
Application Server 7.x	149
Application Server 8.x	149
Directory Server 和 Access Manager 記錄	150
Directory Server	150
Access Manager	150
附錄 D ACI 合併計算	151
簡介	151
合併計算和移除 ACI	152
replacement.acis.ldif 檔	153
替代 ACI 之步驟	155
在您開始之前	155
替代 ACI	155
消除動態社群組織 ACI	156
分析現有的 ACI	157
根底碼	158
Access Manager	160
頂層服務台管理員角色	163
頂層策略管理員角色	164
AM 自身	165
匿名 AM	167
AM 拒絕登入存取	169
AM 伺服器管理員角色	170
社群組織服務台	171
AM 社群組織管理員角色	172
AM 其他	175
Messaging Server	176
分析如何合併計算 ACI	178
原始匿名存取權限	178
合併計算的匿名存取權限	179
原始自身 ACI	179
合併計算自身 ACI	181
原始 Messaging Server ACI	182
合併計算 Messaging Server ACI	183
原始社群組織管理員 ACI	184
合併計算社群組織管理員 ACI	186
捨棄之未使用的 ACI 清單	187

屍碼	187
頂層服務台管理員角色	188
頂層策略管理員角色	189
Access Manager 匿名	190
Access Manager 拒絕登入存取	191
Access Manager 容器管理員角色	191
社團組織服務台	192
Access Manager 其他	193
字彙表	195
索引	197

本指南解釋如何配置和管理 Sun™ Java System Communications Services Delegated Administrator。本指南也描述了 Delegated Administrator 指令，並提供語法和範例。

Delegated Administrator 是由一個主控台 (圖形化使用者介面) 和一組佈建 Sun Java System Messaging Server 和 Sun Java System Calendar Server (使用 Sun Java System Access Manager) 使用者、群組、網域以及資源的指令行工具。

本章囊括之主題如下：

- [本書適用對象](#)
- [閱讀本書之前](#)
- [本書架構](#)
- [本書採用的慣例](#)
- [相關文件](#)
- [存取 Sun 線上資源](#)
- [聯絡 Sun 技術支援](#)
- [協力廠商文件](#)
- [Sun 歡迎您提出寶貴意見](#)

本書適用對象

如果您負責在站點上管理、配置和部署 Delegated Administrator，則應閱讀本指南。

閱讀本書之前

本指南假定您負責管理此軟體並且大致瞭解以下內容：

- 網際網路和全球資訊網
- Messaging Server 協定
- Sun Java System Administration Server
- Sun Java System Directory Server 和 LDAP
- Sun Java System Console
- 以下平台上的系統管理和網路：
 - 用於 SPARC 和 x86 的 Solaris 8
 - 用於 SPARC 和 x86 的 Solaris 9
 - 用於 SPARC 和 x86 的 Solaris 10
 - HP-UX 11.x
 - Windows 2000
- 一般部署架構

本書架構

下列表格摘要本指南的內容。

表 1 本書架構

章	描述
第 1 章「 Delegated Administrator 簡介 」	描述目錄社團組織、管理員角色和 Delegated Administrator 所提供的服務等級套裝軟體。
第 2 章「 安裝和配置規劃 」	描述安裝和配置 Sun Java System Communications Services Delegated Administrator 所需的步驟。
第 3 章「 配置 Delegated Administrator 」	描述和逐步引導 Delegated Administrator 的配置程式。
第 4 章「 自訂 Delegated Administrator 」	描述如何自訂 Delegated Administrator。例如，變更主控台的外視感覺。
第 5 章「 指令行公用程式 」	描述 commadmin 公用程式，並提供語法和範例。

表 1 本書架構 (續)

章	描述
附錄 A 「服務提供者管理員及服務提供者社團組織」	描述服務提供者管理員角色和服務提供者管理員所管理的企業社團組織。
附錄 B 「屬性值和行事曆時區」	列出用於特定指令行選項的屬性值和時區值。
附錄 C 「除錯 Delegated Administrator」	列出用來除錯 Delegated Administrator 所能夠檢查的記錄檔。
附錄 D 「ACI 合併計算」	描述如何合併計算 ACI 和從目錄移除未使用的 ACI。

本書採用的慣例

本節中的表格描述本指南採用的慣例。

印刷排版慣例

下列表格描述本指南中所使用的印刷排版慣例。

表 2 印刷排版慣例

字體	意義	範例
AaBbCc123 (固定間距)	所有在電腦螢幕上顯示的文字，或是您應該輸入的文字。可以是 API 和語言元素、HTML 標籤、網站 URL、指令名稱、檔案名稱、目錄路徑名稱、電腦螢幕輸出、範例代碼。	編輯您的 .login 檔案。 使用 <code>ls -a</code> 以列出所有檔案。 <code>% You have mail.</code>
AaBbCc123 (粗體固定間距)	出現在程式碼範例或其他電腦螢幕輸出中時，表示您應該鍵入的文字。	<code>% su</code> Password:
<i>AaBbCc123</i> (斜體)	您應該以實際的名稱或值取代的指令或路徑名稱中的預留位置 (例如，變數)。 也可以是新專有名詞，或強調的字。	檔案位於 <code>msg_svr_base/bin</code> 目錄中。 這些稱為類別選項。 請勿儲存檔案。
「」	用於書名及章節名稱	參閱「使用者指南」的第六章。

符號

下列表格描述本指南中所使用的符號慣例。

表 3 符號慣例

符號	描述	範例	意義
[]	含有選用的指令選項。	ls [-l]	-l 選項不是必需的。
{ }	含有一組適用於所需指令選項的選擇。	-d {y n}	-d 選項要求您使用 y 引數或 n 引數。
-	同時按下多個按鍵。	Control-A	當您按住 A 鍵時按下 Control 鍵。
+	連續按下多個按鍵。	Ctrl+A+N	按下 Control 鍵，放開它，然後按下後續的鍵。
>	表示選取圖形化使用者界面上的功能表項目。	[檔案]>[開新檔案]>[範本]	從 [檔案] 功能表，選擇 [開新檔案]。從 [開新檔案] 子功能表，選擇 [範本]。

預設路徑和檔案名稱

下列表格描述本指南中所使用的預設路徑和檔案名稱。

表 4 預設路徑和檔案名稱

檔案名稱	描述
<i>msg_svr_base</i>	代表 Messaging Server 的基底安裝目錄。msg_svr_base 安裝的預設值如下： Solaris™ 系統：/opt/SUNWmsgsr Linux 系統：/opt/sun/messaging
<i>da_base</i>	代表 Delegated Administrator 的基底安裝目錄。Delegated Administrator 基底 (<i>da_base</i>) 代表您安裝 Delegated Administrator 的目錄路徑。da_base 的預設值是 /opt/SUNWcomm。

指令行提示符號

範例中沒有顯示指令行提示符號 (例如, % 用於 C-Shell 或 \$ 用於 Korn 或 Bourne shell)。根據您使用的作業系統, 您會看到各種不同的指令行提示符號。但是, 您應依文件所示輸入指令, 除非另有明確說明。

相關文件

您可從 <http://docs.sun.com> 網站存取 Sun 線上技術說明文件。您可以瀏覽歸檔或搜尋指定書名或主旨。

Messaging Server 文件

使用下列 URL 來查看全部的 Messaging Server 文件：

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

http://docs.sun.com/coll/MessagingServer_05q1_zh_TW

以下列出了可用的文件：

- Sun Java™ System Messaging Server 版本說明
- Sun Java™ System Messaging Server 管理指南
- Sun Java™ System Messaging Server Administration Reference
- Sun Java™ System Messaging Server MTA Developer's Reference
- Sun Java™ System Messenger Express Customization Guide

Messaging Server 產品套件含有其他產品, 例如 Sun Java™ System Directory Server 和 Administration Server。這些以及其他產品的文件可以在下列 URL 中找到：

<http://docs.sun.com/prod/entsys.05q1> 及

http://docs.sun.com/db/prod/entsys.05q1?l=zh_TW

除軟體文件之外, 請參閱 Messaging Server 軟體論壇, 以取得有關特定 Messaging Server 產品問題的技術說明。該論壇位於以下 URL 上：

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

Calendar Server 文件

使用下列 URL 來查看全部的 Calendar Server 文件：

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

http://docs.sun.com/coll/CalendarServer_05q1_zh_TW

以下列出了可用的文件：

- Sun Java™ System Calendar Server 版本說明
- Sun Java™ System Calendar Server 管理指南
- Sun Java™ System Calendar Server Developer's Guide

Communications Services 文件

使用下列 URL 其中之一來查看套用於全部 Communications Services 產品的文件：

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

http://docs.sun.com/coll/MessagingServer_05q1_zh_TW

或

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

http://docs.sun.com/coll/CalendarServer_05q1_zh_TW

以下列出了可用的文件：

- Sun Java™ System Communications Services Delegated Administrator 指南
- 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 管理指南
- Sun Java™ System Communications Express Customization Guide

存取 Sun 線上資源

如需產品下載、專業服務、修補程式與支援和其他開發者資訊，請至下列位址：

- 下載中心
<http://www.sun.com/software/download/>
- 專業服務
<http://www.sun.com/service/sunps/sunone/index.html>
- Sun Enterprise Services、Solaris 修補程式與支援
<http://sunsolve.sun.com/>
- 開發者資訊
<http://developers.sun.com/prodtech/index.html>

聯絡 Sun 技術支援

如果您在本文件中找不到所需之本產品相關技術問題的解答，請至 <http://www.sun.com/service/contacting>。

協力廠商責任

Sun 對於本文件中所提及之協力廠商網站的使用不承擔任何責任。Sun 對於此類網站或資源中的 (或透過它們所取得的) 任何內容、廣告、產品或其他材料不做背書，也不承擔任何責任。對於因使用或依靠此類網站或資源中的 (或透過它們所取得的) 任何內容、產品或服務而造成的或連帶產生的實際或名義上之損壞或損失，Sun 概不負責，也不承擔任何責任。

Sun 歡迎您提出寶貴意見

Sun 致力於提高文件品質，因此誠心歡迎您提出意見與建議。

如果您要提出意見，請至 <http://docs.sun.com> 並按一下 [傳送您的回饋意見]。請在線上表單中提供文件標題以及文件號碼。文件號碼是一個七位數或九位數的號碼，您可以在書籍的標題頁或文件頂端找到它。例如，本指南的標題是：「Sun Java System Communications Services 2005Q1 Delegated Administrator 指南」，而文件號碼是 819-1104。

提供意見與建議時，您可能需要在表單中提供文件的英文標題及文件號碼。此文件的英文文件號碼及標題為：819-0114，「Sun Java System Communications Services 2005Q1 Delegated Administrator Guide」。

Delegated Administrator 簡介

Communications Services Delegated Administrator 公用程式和主控台，可讓您在 Communications Services 應用程式 (如 Messaging Server) 所使用的 LDAP 目錄中佈建使用者、群組、網域和資源。

本章描述下列主題：

- [簡介](#)
- [佈建使用者的分析藍本](#)
- [管理員角色和目錄階層](#)
- [若原為 ipplanet Delegated Administrator 的使用者](#)
- [服務套裝軟體](#)

簡介

透過 Delegated Administrator，您可以將佈建作業分配給較低層、有管理 LDAP 目錄中特定社團組織權限的管理員。委託使用者管理的權限可提供下列優點：

- 將潛在的費時作業分配給許多的管理員，以佈建大型的目錄。數十個或數百個管理員可以在包含數千個或百萬個使用者的目錄中管理社團組織。
- 可讓您在目錄結構中建立社團組織，而這些社團組織可以做為明確的 (或唯一的) 單位來管理或佈建。這些社團組織包含了屬於客戶商務、公司部門或其他群組的使用者。

Delegated Administrator 對於在目錄中佈建使用者和社團組織，提供了兩種介面。

- [Delegated Administrator 公用程式](#)
- [Delegated Administrator 主控台](#)

我們將在之後的章節中提供這些介面的摘要。

Delegated Administrator 公用程式

Delegated Administrator 公用程式是一組佈建 Messaging Server 和 Calendar Server 使用者的指令行工具。(在之前的版本中，Delegated Administrator 公用程式稱為「使用者管理公用程式」。)

您可以使用 Delegated Administrator 公用程式來佈建社團組織、使用者、群組和行事曆資源。

注意 Delegated Administrator 公用程式提供了在 Communications Services 產品 (Messaging Server 6 2004Q2 和 Calendar Server 6 2004Q2) 之前的發行版本中所能使用的指令行功能。Delegated Administrator 公用程式並不提供相關指令來建立本指南中所描述的服務提供者角色和社團組織。若要建立並管理這些新角色和社團組織，您必須使用 Delegated Administrator 主控台。

使用 `commadmin` 指令呼叫此公用程式。

如需 `commadmin` 公用程式可用的語法和選項等相關資訊，請參閱第 5 章「[指令行公用程式](#)」。

Delegated Administrator 主控台

Delegated Administrator 主控台是一種圖形化使用者介面 (GUI)，用於佈建 Messaging Server 使用者和社團組織。

若要佈建群組和行事曆資源，請使用 Delegated Administrator 公用程式。請勿使用 Delegated Administrator 主控台。在此 Delegated Administrator 的發行版本中，您無法使用主控台來佈建群組和行事曆資源。

關於如何使用主控台的資訊，請參閱 Delegated Administrator 主控台線上說明。

Delegated Administrator 和 LDAP 目錄

Delegated Administrator 可讓您修改 LDAP 目錄以佈建使用者。您不需要直接修改目錄。然而，如果您能瞭解新增至使用者項目的 Delegated Administrator 屬性和目錄中較高層的節點，將會很有幫助。

有關 LDAP Schema 物件類別和支援 Delegated Administrator 的屬性等資訊，請參閱「Sun Java System Communications Services Schema Reference」中的第 5 章「Classes and Attributes Used by Communications Services Delegated Administrator (Schema 2)」。

佈建使用者的分析藍本

視您的業務需要而定，您可以建立一個由單一管理員所管理的簡易目錄結構，或者是委託較低層管理員進行佈建和管理作業的多層次目錄階層。

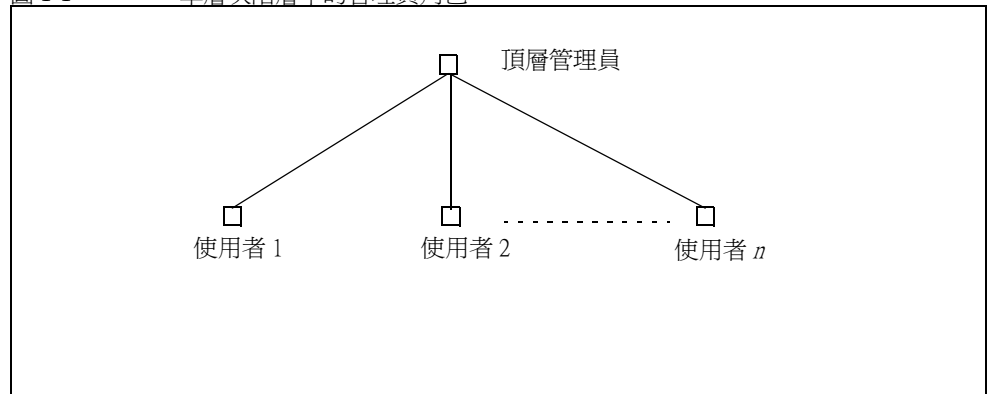
本節將針對三個遞增複雜性的分析藍本進行摘要。並進一步分析 Delegated Administrator 為支援這些分析藍本需求而提供的管理員角色和目錄結構。

單層次階層

在此分析藍本中，一個公司或社團組織可能會支援數百個或數千個員工或使用者。所有的使用者都會在單一社團組織中分組。單一管理員角色會檢視並管理整個群組。這裡並沒有委託的管理作業。

圖 1-1 顯示單層次階層之單一社團組織中的管理員角色範例。

圖 1-1 單層次階層中的管理員角色



此單層次階層中的管理員稱為「頂層管理員」(TLA)。

在圖 1-1 所顯示的範例中，TLA 會直接管理並佈建使用者 (使用者 1、使用者 2，一直到使用者 n)。

如果您在目錄中擁有一個社團組織，TLA 是您唯一需要的管理員。

如需更多資訊，請參閱以下各節：

- [支援單層次階層的目錄結構](#)
- [頂層管理員角色](#)

雙層次階層

在此分析藍本中，如網際網路服務提供者 (ISP) 之類的大型公司會將服務提供給各個企業。每個企業都有專屬於自己的網域，其中可能包含數千或數萬個使用者。

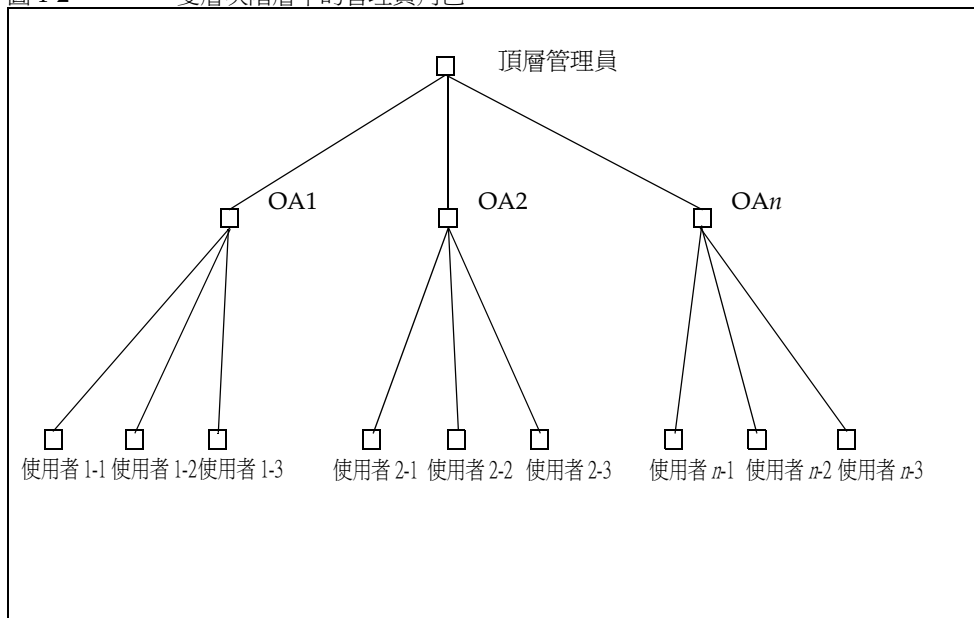
相對於依賴「單一頂層管理員」(TLA) 管理並佈建所有的網域，此分析藍本可支援將作業委託給較低層的管理員。

在雙層次階層中，目錄會包含多個社團組織。系統會為每個託管網域建立一個個別的社團組織。

每個社團組織都會被指定給一個「社團組織管理員」(OA)。OA 將對該社團組織中的使用者負責。OA 無法檢視或修改自己社團組織之外的目錄資訊。

圖 1-2 顯示雙層次階層中的管理員角色範例。

圖 1-2 雙層次階層中的管理員角色



在圖 1-2 所顯示的範例中，TLA 會建立並管理 OA1、OA2，一直到 OAn。每個 OA 都會管理一個社團組織中的使用者。

如果您在目錄中需要多個社團組織，您必須建立一個 TLA 和多個 OA 來管理社團組織和其中的使用者。

如需更多資訊，請參閱以下各節：

- [支援雙層次階層的目錄結構](#)
- [頂層管理員角色](#)
- [社團組織管理員角色](#)

三層次階層

在此分析藍本中，如 ISP 之類的公司會將服務提供給數百個或數千個小型企業，每個企業都需要專屬的社團組織。

ISP 可能會支援數百萬個需要郵件服務的一般使用者。此外，ISP 可能會與管理一般企業使用者的第三方轉售商合作。

每一天可能都會有許多新社團組織新增至目錄中。

在雙層次階層中，TLA 必須建立許多新的社團組織。

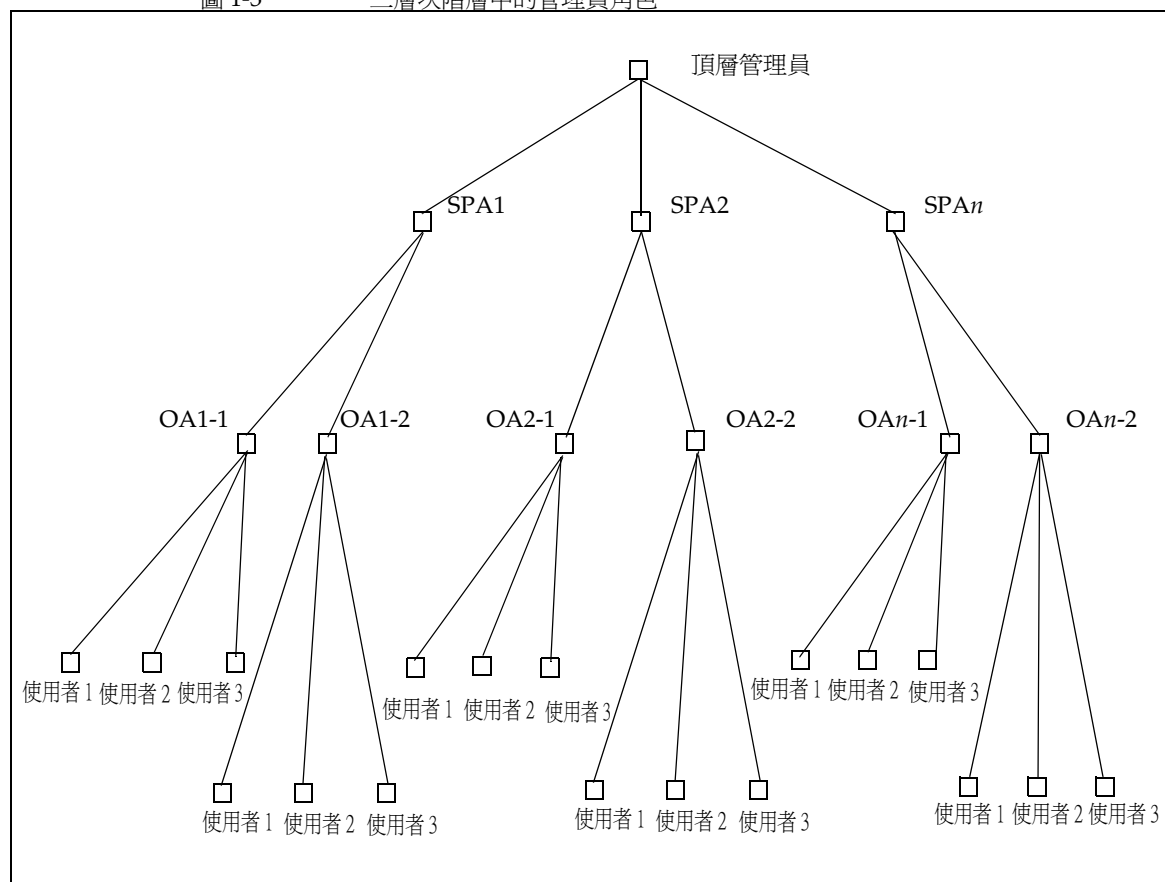
在三層次階層中，管理作業會委託給第二層級的管理員。在委託給第二層級後，可減輕由大型 LDAP 目錄所支援的大型客戶基底的管理作業。

爲了要支援此階層，Delegated Administrator 引進了「服務提供者管理員」(SPA) 的新角色。

SPA 的權限範圍介於頂層管理員 (TLA) 和社團組織管理員 (OA) 之間。

圖 1-3 顯示三層次階層中的管理員角色範例。

圖 1-3 三層次階層中的管理員角色



在三層次階層中，TLA 會將管理權限委託給「服務提供者管理員」(SPA)。SPA 會為新的客戶建立企業社團組織，並指定「社團組織管理員」(OA) 來管理這些企業社團組織中的使用者。

如果您需要多個社團組織能自行分配至子群組或社團組織中，您可以使用實作 TLA、SPA 和 OA 角色的三層次階層。

如需 SPA 角色的資訊，請參閱[附錄 A「服務提供者管理員及服務提供者社團組織」](#)。

管理員角色和目錄階層

本節顯示實作單層次和雙層次階層的「目錄資訊樹」範例。並進一步說明可由頂層管理員和社團組織管理員所執行的作業。

支援單層次階層的目錄結構

當您執行配置程式 `config-commda` 來配置 Delegated Administrator 時，也同時建立了頂層管理員 (TLA) 和預設社團組織。

單層次階層：根尾碼之下的預設社團組織

配置程式會依預設將預設社團組織放置在根尾碼之下。

目錄資訊樹看起來會和[圖 1-4](#) 中所顯示的相似。

[圖 1-4](#) 顯示在單層次階層 (預設配置) 中所組織的範例目錄資訊樹。

圖 1-4 單層次階層：目錄資訊樹範例 (預設)



單層次階層：根尾碼上的預設社團組織

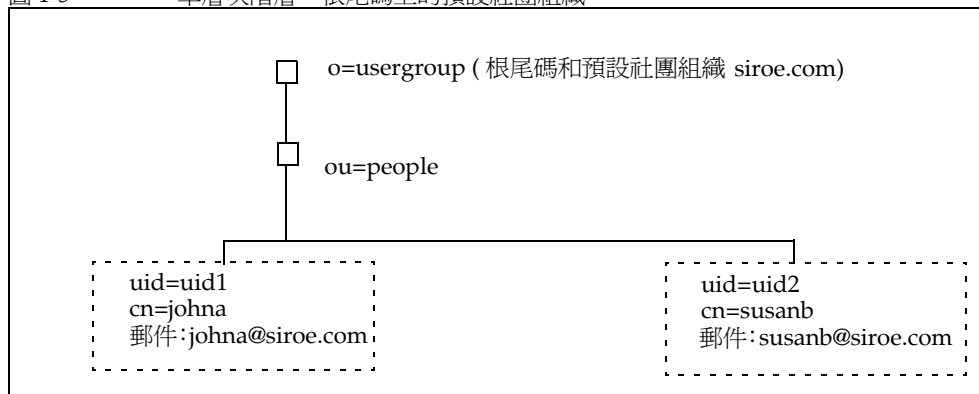
當您執行配置程式 (config-command) 時，您可以選擇將預設社團組織建立在根尾碼上，而不是它的下方。關於配置的詳細資訊，請參閱第 3 章「配置 Delegated Administrator」中的步驟 6，[社團組織辨別名稱 \(DN\)](#)。

在此情況下，目錄資訊樹看起來會和圖 1-5 中所顯示的相似。

然而，如果您將預設社團組織建立在根尾碼上，這個 LDAP 目錄的配置將無法支援多個託管網域。若要支援託管網域，預設社團組織必須在根尾碼之下。

圖 1-5 顯示一個單層次階層範例，其中的預設社團組織建立在根尾碼上。

圖 1-5 單層次階層：根尾碼上的預設社團組織

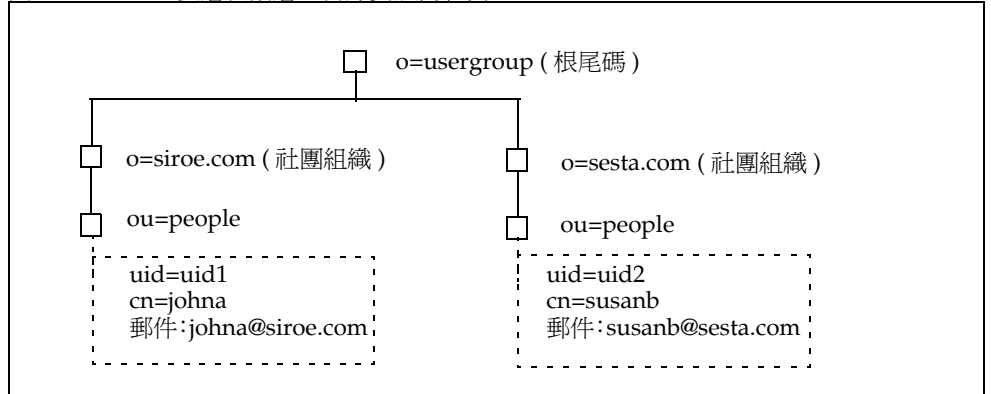


支援雙層次階層的目錄結構

在使用 `config-commda` 程式設置 Delegated Administrator 之後，TLA 可以建立額外的社團組織，如圖 1-6 所示。

圖 1-6 顯示在雙層次階層中所組織的目錄資訊樹範例。

圖 1-6 雙層次階層：目錄資訊樹範例



頂層管理員角色

TLA 擁有執行以下作業的權限：

- 建立、刪除和修改社團組織。

在圖 1-6 所顯示的範例中，TLA 可修改或刪除 `siroe.com` 或 `sesta.com`，並可建立額外的社團組織。

注意，在此範例中兩個社團組織也是唯一的（託管）網域。

- 建立、刪除和修改使用者。
- 將 OA 角色指定給使用者。例如，TLA 可將一個 OA 指定給 `siroe.com` 社團組織中的使用者 `johna`。

TLA 也可以移除使用者的 OA 角色。

- 將 TLA 角色指定給其他使用者。TLA 也可以移除使用者的 TLA 角色。
- 將服務套裝軟體指定給社團組織。

有關服務套裝軟體的資訊，請參閱本簡介後面的「[服務套裝軟體](#)」。

TLA 可將特定種類的服務套裝軟體指定給社團組織，並確定每個套裝軟體可在社團組織中使用的最大數目。

例如，TLA 可指定下列服務套裝軟體：

- 在 `siroe.com` 社團組織中：
 - 1,000 個 Gold 套裝軟體
 - 500 個 Platinum 套裝軟體
- 在 `sesta.com` 社團組織中：
 - 2,000 個 Silver 套裝軟體
 - 1,500 個 Gold 套裝軟體
 - 100 個 Platinum 套裝軟體

TLA 可使用 `Delegated Administrator` 主控台或執行 `Delegated Administrator` 公用程式 (`commadmin`) 指令來執行上述作業。

有關 `commadmin` 指令的描述，請參閱第 5 章「指令行公用程式」中的表 5-1，[Delegated Administrator 指令行介面](#)。

社團組織管理員角色

OA 擁有執行以下作業的權限：

- 建立、刪除和修改 OA 社團組織中的使用者
在圖 1-6 所顯示的範例中，如果使用者 `johna` 已指定為 `siroe.com` 社團組織中的 OA 角色，則 `johna` 可以管理 `siroe.com` 中的使用者。
- 將 OA 角色指定給 OA 社團組織中的其他使用者。
- OA 無法管理或無法將 OA 角色指定給在 OA 社團組織之外的使用者。
例如，`johna` 無法管理 `sesta.com` 中的使用者或為其指定 OA 角色。
- 指定和移除 OA 社團組織中使用者的服務套裝軟體。

OA 可使用 `Delegated Administrator` 主控台或執行 `Delegated Administrator` 公用程式 (`commadmin`) 指令來執行上述作業。

有關 `commadmin` 指令的描述，請參閱第 5 章「指令行公用程式」中的表 5-1，[Delegated Administrator 指令行介面](#)。

第 1 章 iPlanet Delegated Administrator 的用戶

Communications Services Delegated Administrator 是爲了佈建 LDAP Schema 2 目錄中的使用者而設計的。

擁有 LDAP Schema 1 目錄的上一版本 Messaging Server 使用者，可能已使用過 iPlanet Delegated Administrator 這個不建議再使用的工具。如果您仍擁有 Schema 1 目錄，您應該使用 iPlanet Delegated Administrator 來佈建使用者。

針對管理員角色，iPlanet Delegated Administrator 所使用的專有名詞與目前 Communications Service Delegated Administrator 所使用的有些微的不同。

表 1-1 列出並定義 Delegated Administrator 每個版本中的管理員角色。

表 1-1 iPlanet Delegated Administrator 和 Communications Services Delegated Administrator 中的管理員角色

iPlanet Delegated Administrator	Communications Services Delegated Administrator 管理員角色	Communications Services Delegated Administrator 管理員角色	定義
站台管理員	頂層管理員 (TLA)	頂層管理員 (TLA)	管理 Delegated Administrator 所支援的整個目錄，包含社團組織和使用者*。
(無)	(此發行版本不提供)	服務提供者管理員 (SPA)	管理提供者社團組織、提供者社團組織之下的共用及完整企業社團組織，以及這些企業社團組織中的使用者。
網域管理員	社團組織管理員 (OA)	社團組織管理員 (OA)	管理一個社團組織以及該組織中的使用者。

* 在此 Delegated Administrator 的發行版本中，TLA 無法建立提供者社團組織，或在提供者社團組織之下建立企業社團組織。

服務套裝軟體

服務套裝軟體是由 LDAP 目錄中的服務等級機制所實作的。此機制可讓您設定預先定義的屬性的值，在您配置 Delegated Administrator 時，這些屬性已安裝在目錄中。服務套裝軟體在使用者項目中新增了一些服務特性。

在 Delegated Administrator 主控台中，您執行以下的服務套裝軟體作業：

- 將服務套裝軟體配置給社團組織。在將一些 (或全部) 的套裝軟體配置給社團組織之後，社團組織中的使用者就能夠使用這些套裝軟體。您將針對每個套裝軟體配置特定數量的套裝軟體。

例如，您可能會為 ABC 社團組織配置 5,000 個 Gold 套裝軟體和 10,000 個 Silver 套裝軟體。

- 將服務套裝軟體指定給使用者。

針對您在 LDAP 目錄中佈建的每位使用者，您至少要配置一個服務。您可以將多個服務套裝軟體指定給一個使用者。

當您將服務套裝軟體指定給一個使用者時，服務套裝軟體中的所有屬性和值都會自動指定給該使用者。

服務等級定義

此發行版本會將一個服務等級定義提供給 Messaging Server 使用者。表 1-2 顯示為郵件使用者所定義的 LDAP 屬性：

表 1-2 可在服務套裝軟體中使用的郵件服務屬性

屬性	定義
mailMsgMaxBlocks	可傳送至使用者或群組的最大訊息大小 (以 MTA 區段為單位)。
mailAllowedServiceAccess	指定可用於存取指定服務的用戶端的篩選。例如： +imap:ALL\$+pop:ALL\$+smtp:ALL\$+http:ALL
mailMsgQuota	使用者可使用的訊息之最大數量 (包含所有使用者資料夾)。
mailQuota	使用者電子信箱可用的磁碟空間 (以位元組為單位)。

如需這些屬性的詳細資訊，請參閱「Sun Java System Communications Services Schema Reference」中的第 3 章「Attributes」。

這些郵件服務屬性已在稱為 standardMail 的服務等級定義中完成定義。當您配置 Delegated Administrator 時，standardMail 定義已安裝在目錄中。

standardMail 服務等級定義列示如下：

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

備註：當 Delegated Administrator 配置程式將 standardMail 定義安裝在目錄中時，上方所顯示的 <ugldapbasedn> 變數會由根尾碼（例如 o=usergroup）所取代。

除了郵件屬性以外，standardMail 定義會將服務類型定義為 daServiceType 屬性中的郵件使用者。

檢視延伸式服務套裝軟體的限制

您可以在定義項目中新增任何的屬性，以延伸 Delegated Administrator 服務套裝軟體的定義。

然而，在此 Delegated Administrator 的發行版本中，主控台只允許您檢視在配置 Delegated Administrator 時所提供的預先定義的屬性。Delegated Administrator 主控台不會顯示您在服務套裝軟體定義中新增的任何屬性。

針對此發行版本，在由 Delegated Administrator 提供的 standardMail 服務等級定義中，您不應該移除預先定義的屬性定義。

服務等級範本

根據服務等級定義中可用的屬性，您可以建立自己的服務套裝軟體，為不同的使用者定義不同的服務層級。

預設服務等級範本

依預設，Delegated Administrator 配置程式 (config-commda) 可在目錄中安裝一個 ldif 檔案 cos.default.ldif。此 ldif 檔案提供一個稱為 defaultmail 的通用服務等級範本。

以下的服務等級範本已包含在 cos.default.ldif 檔案中：

```
dn: cn=defaultmail,o=cosTemplates,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
mailquota: -2
cn: defaultmail
```

備註：當 Delegated Administrator 配置程式將 defaultmail 範本安裝在目錄中時，上方所顯示的 <ugldapbasedn> 變數會由根尾碼（例如 o=usergroup）所取代。

在預設的服務等級範本 (defaultmail) 中，只定義了一個郵件服務屬性，即 mailquota。它的值為 -2，表示此服務的郵件配額為系統所預設。

服務等級範本的範例

當您執行 Delegated Administrator 配置程式 config-commda 時，可以選擇載入額外的服務套裝軟體範例。（當您執行配置程式時，請在 [服務套裝軟體和社團組織範例] 面板中選取 [載入服務套裝軟體範例]。）配置程式會將 cos.sample.ldif 檔案新增至 LDAP 目錄樹中。

cos.sample.ldif 檔案包含了下列服務等級範本的範例：

- Platinum
- Gold
- Silver
- Bronze
- Ruby
- Topaz
- Diamond
- Emerald

每個範本都包含了服務等級定義中所列出的一個或多個屬性的特定值。這些範本為服務套裝軟體的原型範例。

例如，Platinum 的服務等級範本已包含在 `cos.sample.ldif` 檔案中：

```
dn: cn=platinum,o=cosTemplates,$rootSuffix
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: platinum
mailMsgMaxBlocks: 800
mailQuota: 400000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

備註：當 Delegated Administrator 配置程式將服務等級範例範本安裝在目錄中時，上方所顯示的 `$rootSuffix` 變數會由根尾碼（例如 `o=usergroup`）所取代。

如需所有服務等級範本範例的郵件服務值清單，請參閱位於本章結尾的「[服務等級範本範例中的郵件服務層級](#)」。

建立您自己的服務套裝軟體

在本章中所描述的服務等級範本旨在作為範例參考。您可能必須藉由在安裝過程中使用者所適用的屬性值，來建立您自己的服務套裝軟體。

若要建立您自己的服務套裝軟體，可以使用儲存在 `da.cos.skeleton.ldif` 檔案中的服務等級範本。建立該檔案的目的就是要做為寫入服務套裝軟體的範本。當配置 Delegated Administrator 時，該檔案並沒有安裝在 LDAP 目錄中。

您可以複製及編輯 `da.cos.skeleton.ldif` 檔案，並使用如 `ldapmodify` 的 LDAP 目錄工具，在目錄中安裝您的服務套裝軟體。

有關使用 `da.cos.skeleton.ldif` 檔案以配置您自己的服務套裝軟體的說明，請參閱第 3 章「[配置 Delegated Administrator](#)」中的「[建立服務套裝軟體](#)」。

指定至 LDAP 使用者項目的服務套裝軟體範例

當您使用 Delegated Administrator 將服務套裝軟體指定給使用者時，LDAP 目錄中的使用者項目會新增一個單一屬性 (inetCOS)。inetCOS 屬性的值會將整個服務套裝軟體指定給使用者。(inetCOS 是一個多重值屬性。)

例如，假設您將 Platinum 套裝軟體指定給使用者。以下的屬性會新增至使用者項目：

```
inetCOS:platinum
```

Platinum 套裝軟體包含了以下郵件服務屬性的值。因此，在您指定 Platinum 套裝軟體的同時，也會將這些屬性新增至使用者項目中。

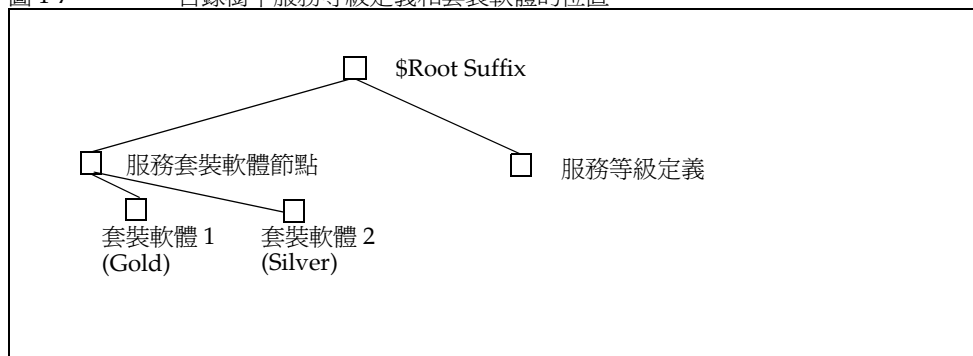
```
mailMsgMaxBlocks: 800
mailQuota: 4000000000
mailMsgQuota: 6000
mailAllowedServiceAccess:+imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

服務等級定義和套裝軟體的位置

在 LDAP 目錄資訊樹 (DIT) 中，服務等級定義位於根尾碼正下方的節點中。由於它就儲存在 DIT 的最上方，因此服務套裝軟體可以指定給目錄中所有的使用者項目。

圖 1-7 顯示 DIT 中服務定義和套裝軟體的位置。此處顯示兩個套裝軟體範例，Gold 和 Silver。

圖 1-7 目錄樹中服務等級定義和套裝軟體的位置



Delegated Administrator 使用典型的服務等級定義。

如需服務等級機制的詳細資訊，請參閱「Sun Java System Directory Server 管理指南」。特別是位於第 5 章「管理識別和角色」中的「定義服務等級 (CoS)」。

「Directory Server 管理指南」也描述了相關的主題。例如，如果在指定給使用者的服務套裝軟體中已定義的屬性，已存在於個別的使用者項目時，您要決定哪個服務屬性值優先。

服務等級範本範例中的郵件服務層級

本節列出由服務等級範本的範例所提供之郵件服務層級。這些範本中的屬性值只做為範例之用，且不是源自於實際的安裝作業。

Platinum

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess:+imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

Gold

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess:+imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

Silver

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

Bronze

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

Ruby

```
mailMsgMaxBlocks: 600  
mailquota: 1048576  
mailmsgquota: 2000  
mailAllowedServiceAccess: +pop:ALL$+smtp:ALL$+http:ALL
```

Emerald

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

Diamond

```
mailMsgMaxBlocks: 5000  
mailquota: 3145728  
mailmsgquota: 3000  
mailAllowedServiceAccess: +imap:ALL$+smtp:ALL$+http:ALL
```

Topaz

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

安裝和配置計劃

若要在 Solaris 系統上安裝 Sun Java System Communications Services Delegated Administrator，您必須使用 Sun Java Enterprise System 安裝程式，它也可以安裝其他 Sun 的元件產品。

若要安裝和配置 Delegated Administrator，請遵循這些步驟：

1. 取得您的 Delegated Administrator 配置資訊
2. 執行 Java Enterprise System 安裝程式
3. 執行 Directory Server 設定程序檔
4. 配置 Delegated Administrator
5. 配置 Messaging Server 和 Calendar Server

若要取得關於 Delegated Administrator 的最新資訊，請參閱「Sun Java System Messaging Server 版本說明」。

取得您的 Delegated Administrator 配置資訊

Delegated Administrator 元件

Delegated Administrator 包含下列元件：

- **Delegated Administrator 公用程式 (用戶端)** – 使用 `commadmin` 呼叫指令行介面。
必要的選項。您必須在所有已安裝 Delegated Administrator 的機器上配置公用程式。

- **Delegated Administrator 伺服器** – 需要 Delegated Administrator 伺服器元件以執行 Delegated Administrator 公用程式和主控台。
必要的選項。您必須至少在一台機器上配置 Delegated Administrator 伺服器。
- **Delegated Administrator 主控台** – Delegated Administrator 圖形化使用者介面 (GUI)。
選擇性選項。如果您只想使用 Delegated Administrator 公用程式，則不需要配置主控台。

Web 容器

此外，Delegated Administrator 伺服器和主控台必須部署在 Web 容器上。您可以將 Delegated Administrator 主控台和伺服器配置在

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

遵循這些指示：

- Delegated Administrator 伺服器必須部署在 Access Manager 所使用的 Web 容器上。
- 您可以在兩個不同的 Web 容器上、兩個不同的 Web 容器實例上，或者在相同的 Web 容器上部署 Delegated Administrator 主控台和伺服器。

配置資訊

在配置 Delegated Administrator 之前，您應該先收集配置資訊。

[表 2-1](#) 列出 Delegated Administrator 必要的配置選項。

[表 2-2](#) 列出在 Web Server 上進行部署的配置選項。

[表 2-3](#) 列出在 Application Server 7.x 上進行部署的配置選項。

[表 2-4](#) 列出在 Application Server 8.x 上進行部署的配置選項。

表 2-1 Delegated Administrator：必要的配置選項

選項	描述
配置目錄	儲存配置和資料檔案的目錄。
Access Manager 主機名稱	已安裝 Access Manager 的主機名稱。Delegated Administrator 伺服器必須安裝在相同的伺服器上。
Access Manager 連接埠號碼	Access Manager 連接埠號碼。Access Manager 連接埠號碼必須和 Web Server 的連接埠號碼相同。
預設網域	頂層管理員的預設網域。在執行 <code>commadmin</code> 命令行公用程式時，若沒有使用 <code>-n</code> 選項來特別指定網域，則這就是所使用的網域。
預設 SSL 連接埠	Delegated Administrator 用戶端所使用的 SSL 連接埠。
Access Manager 基底目錄	已安裝 Access Manager 的目錄。預設目錄為 <code>/opt/SUNWam</code> 。
LDAP URL	使用者和群組 Directory Server LDAP URL。
連結為	使用者和群組 Directory Server 的目錄管理員。例如，「 <code>cn=Directory Manager</code> 」。
LDAP 密碼	使用者和群組目錄管理員密碼。
Access Manager 頂層管理員使用者 ID 和密碼	Access Manager 頂層管理員的使用者 ID 和密碼。
Access Manager 內部 LDAP 認證使用者的密碼	Access Manager 所建立的使用者。這是 LDAP 服務的 BindDN 使用者。
社團組織名稱	用來命名 LDAP 子樹，所有屬於預設電子郵件網域的電子郵件使用者和群組都位於該子樹之下。
預設社團組織使用者 ID 和密碼的頂層管理員	將在預設社團組織中建立的頂層管理員使用者 ID 和密碼。
社團組織範例之喜好的郵件主機	已安裝 Messaging Server 的機器名稱。如果您選擇在目錄中安裝社團組織範例，您必須進入喜好的郵件主機。

表 2-2 Web Server 配置選項

選項	描述
Web Server 根 (實例) 目錄	Web Server 實例所常駐的目錄。Web Server 實例的檔案儲存在 Web Server 安裝目錄下的 <code>https-host.domain</code> 目錄中。

表 2-2 Web Server 配置選項 (續)

選項	描述
Web Server 實例識別碼	Web Server 實例的完全合格的網域名稱。這可以使用如 <code>west.sesta.com</code> 的 <i>host.domain</i> 名稱來指定。
虛擬伺服器識別碼	使用如 <code>https-west.sesta.com</code> 的 <i>https-host.domain</i> 名稱來指定。
HTTP 連接埠號碼	Web Server 的 HTTP 連接埠號碼。

表 2-3 Application Server 7.x 配置選項

選項	描述
Application Server 安裝目錄	已安裝 Application Server 7.x 的目錄。依預設，此目錄為 <code>/opt/SUNWappserver7</code> 。
Application Server 網域目錄	依預設，此目錄為 <code>/var/opt/SUNWappserver7/domains/domain1</code> 。
Application Server 文件根目錄	依預設，此目錄為 <code>/var/opt/SUNWappserver7/domains/domain1/server1/docroot</code> 。
Application Server 實例名稱	實例名稱。例如： <code>server1</code> 。
虛擬伺服器識別碼	Application Server 虛擬伺服器識別碼名稱。例如： <code>server1</code> 。
Application Server 實例 HTTP 連接埠號碼	Application Server 實例的 HTTP 連接埠號碼。
Administration Server 連接埠號碼	Application Server 7.x 的 Administration Server 實例連接埠號碼。例如： <code>4848</code> 。
Administration Server 管理員使用者 ID 和密碼。	Administration Server 管理員的使用者 ID 和密碼。使用者 ID 範例： <code>admin</code> 。
存取 Administration Server 實例的 HTTP 或 HTTPS	您將需要指定存取 Administration Server 實例的 HTTP 是否安全。

表 2-4 Application Server 8.x 配置選項

選項	描述
Application Server 安裝目錄	已安裝 Application Server 8.x 的目錄。依預設，此目錄為 /opt/SUNWappserver/appserver。
Application Server 網域目錄	依預設，此目錄為 /var/opt/SUNWappserver/domains/domain1。
Application Server 文件根目錄	依預設，此目錄為 /var/opt/SUNWappserver/domains/domain1/docroot。
Application Server 目標名稱	實例名稱。例如：server。
虛擬伺服器識別碼	Application Server 虛擬伺服器識別碼名稱。例如：server。
Application Server 目標 HTTP 連接埠號碼	Application Server 目標的 HTTP 連接埠號碼。
Administration Server 連接埠號碼	Application Server 8.x 的 Administration Server 實例連接埠號碼。例如：4849。
Administration Server 管理員使用者 ID 和密碼。	Administration Server 管理員的使用者 ID 和密碼。使用者 ID 範例：admin。
存取 Administration Server 實例的 HTTP 或 HTTPS	您將需要指定存取 Administration Server 實例的 HTTP 是否安全。

執行 Java Enterprise System 安裝程式

Java Enterprise System 安裝程式可安裝會互通的一系列產品、共用元件和程式庫。安裝程式也會檢查以確定您已安裝下列必要的支援元件：Sun Java System Directory Server 5.x 和以下其中一個 Web 容器：

- Sun Java System Web Server 6.1
- Sun Java System Application Server 7.x
- Sun Java System Application Server 8.x

備註 如果您要從前一個 Sun Java System 版本升級 Delegated Administrator，請參閱「Sun Java Enterprise System 升級和遷移指南」中的第 3 章「從前一個 Java Enterprise System 版本升級」。(在「升級和遷移指南」的第 3 章中，「升級 Delegated Administrator」部分會出現在「升級 Messaging Server」這一節中。)您可以在下列 URL 存取這本指南：
<http://docs.sun.com/doc/819-2238>

若要成功安裝並配置 Delegated Administrator，您必須透過 Java Enterprise System 安裝程式來安裝下列元件：

- Sun Java System Access Manager

(在前一個發行版本中，Access Manager 稱為 Identity Server。)

由於 Delegated Administrator 需要您使用 LDAP Schema 2 提供使用者和群組，因此您必須透過 Java Enterprise System 安裝程式來安裝 Access Manager。Delegated Administrator 隨同 Access Manager 一起安裝。

Java Enterprise System 安裝程式在稱為 *da_base* 的目錄中安裝 Delegated Administrator (例如，預設為 /opt/SUNWcomm)。

Delegated Administrator 為 Messaging Server 和 Calendar Server 提供的工具。因此，若要成功地使用 Delegated Administrator，您必須透過 Java Enterprise System 安裝程式來安裝以下的元件：

- Sun Java System Messaging Server 和 Sun Java System Calendar Server 的其中一個或兩個都安裝。

備註 我們不建議您將 Messaging Server 或 Calendar Server 安裝在和 Access Manager 相同的系統中。

請參閱「Sun Java System Messaging Server 管理指南」以取得配置 Messaging Server 的說明。請參閱「Sun Java System Calendar Server 管理指南」以取得配置 Calendar Server 的說明。

關於 Java Enterprise System 安裝程式的詳細資訊，請參閱「Sun Java Enterprise System 安裝指南」(<http://docs.sun.com/doc/819-0811>)。

執行 Directory Server 設定程序檔

在配置 Delegated Administrator、Messaging Server 或 Calendar Server 之前，您只能執行一次 Directory Server Preparation Tool 程序檔 (comm_dssetup.pl)。這個程序檔會將 LDAP Directory Server 設定成與 Delegated Administrator、Messaging Server 或 Calendar Server 配置一起運作。comm_dssetup.pl 指令檔會設定新的模式、索引和配置資料以準備 Directory Server。

請參閱「Sun Java System Messaging Server 管理指南」或「Sun Java System Calendar Server 管理指南」以取得 comm_dssetup.pl 程序檔的說明和選項。

爲了要執行 Delegated Administrator，在執行 comm_dssetup.pl 指令檔時，您必須選取「Schema 2」模式類型。

在目錄中合併計算 ACI

若要對 Access Manager、Messaging Server 和 LDAP Schema 2 目錄進行大規模的安裝，您可能需要在目錄中合併計算 Access Control Instructions (ACI)。

當您使用 Messaging Server 安裝 Access Manager 時，目錄中已安裝數量龐大的 ACI。Messaging Server 不需要或者不使用許多的預設 ACI。您可以合併計算或減少目錄中預設 ACI 的數量，以增進 Directory Server 以及 Messaging Server 的效能。

有關如何合併計算及捨棄未使用的 ACI 之詳細資訊，請參閱本指南的附錄 D「ACI 合併計算」。

配置 Delegated Administrator

在安裝 Delegated Administrator 之後，請使用「[取得您的 Delegated Administrator 配置資訊](#)」中的資訊來執行 Delegated Administrator 配置程式。

有關配置程式的資訊，請參閱第 3 章「[配置 Delegated Administrator](#)」。

配置 Messaging Server 和 Calendar Server

請參閱「Sun Java System Messaging Server 管理指南」以取得配置 Messaging Server 的說明。請參閱「Sun Java System Calendar Server 管理指南」以取得配置 Calendar Server 的說明。

配置 Delegated Administrator

Delegated Administrator 配置程式 (config-commda) 會根據您的特定需求建立新的配置。初始執行階段配置程式會執行最小配置。

在執行程式之後，請遵循「[配置後作業](#)」中所描述的步驟完成初始配置。

您可以執行「初始化 Delegated Administrator」中所描述的作業，進一步自訂您的 Delegated Administrator。

您可能需要執行額外的配置，如「[Sun Java System Messaging Server 管理指南](#)」中所描述的一樣。

本章說明下列主題：

- [選擇要配置的元件](#)
- [執行配置程式](#)
- [執行無訊息安裝](#)
- [配置後作業](#)

Delegated Administrator 配置程式尚未本土化，為使本章內容更易理解，對於相關軟體介面使用了中文釋意。

選擇要配置的元件

配置程式中的第三個面板會詢問您要配置哪一個 Delegated Administrator 元件：

- **Delegated Administrator 公用程式 (用戶端)** – 使用 `commadmin` 呼叫指令行介面。
- **Delegated Administrator 伺服器** – 需要 Delegated Administrator 伺服器元件以執行 Delegated Administrator 公用程式和主控台。

- **Delegated Administrator 主控台** – Delegated Administrator 圖形化使用者介面 (GUI)。

配置程式會根據您所選取的元件，顯示不同面板。

以下的步驟會依不同的配置選擇進行摘要。每個摘要步驟都可連結至本章後段的小節，引導您檢視真實的配置面板。

1. 啟動配置

輸入這些面板所要求的資訊，開始進行配置。

2. 配置 Delegated Administrator 公用程式

這些面板會出現在 [選取要配置的元件] (Select Components to Configure) 面板之後，並會詢問用來配置 Delegated Administrator 公用程式的資訊。

Delegated Administrator 是必要的公用程式，且必須配置在所有要安裝 Delegated Administrator 元件 (伺服器或主控台) 的機器上。

因此，您必須在這些面板中輸入資訊。

3. 配置 Delegated Administrator 主控台

這些面板出現在配置公用程式的面板之後。

您可以選擇是否要配置 Delegated Administrator 主控台。

- 如果您將 Delegated Administrator 主控台和伺服器部署在相同的機器上，則必須在 [選取要配置的元件] (Select Components to Configure) 面板上選取主控台和伺服器。
- 您也可以將 Delegated Administrator 主控台和伺服器部署在不同的機器上。

在部署主控台的機器上，在 [選取要配置的元件] (Select Components to Configure) 的面板上您只能選取主控台。(公用程式為自動選取。)

在此條件下，您必須在部署伺服器的機器上再執行一次配置程式。

如果您將主控台和伺服器部署在不同的機器上，公用程式將會配置在這兩台機器上。

配置程式會根據您為主控台所選取的 Web 容器不同，顯示不同面板。您可以部署在下列其中一個 Web 容器上：

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

- Sun Java System Application Server 8.x

如果您正在一台機器上配置 Delegated Administrator 伺服器 and 主控台，您將會執行這些配置程序兩次(一次伺服器，一次主控台)。

4. 配置 Delegated Administrator 伺服器

這些面板出現在配置主控台的面板之後。

您可以選擇是否要將 Delegated Administrator 伺服器配置在指定的機器上。

如果您選擇不將 Delegated Administrator 伺服器配置在指定的機器上，配置程式會警告您必須將其配置在另一台機器上。您需要伺服器元件來執行公用程式和主控台。

其他與部署伺服器有關的注意事項與部署主控台時相同(「[配置 Delegated Administrator 主控台](#)」中提供了相關描述)。

請注意，伺服器所使用的 Web 容器與 Access Manager 相同。(配置程式會在要求 Access Manager 基底目錄之後要求 Web 容器的資訊。)

5. 完成配置

輸入這些面板所要求的資訊以完成配置。

執行配置程式

本節所描述的步驟將引導您配置 Delegated Administrator。

若要執行配置程式，請以超級使用者的身分(或成為超級使用者)登入，並移至 /opt/SUNWcomm/sbin 目錄。然後輸入指令：

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

在執行 config-commda 指令之後，配置程式將會啟動。

接下來的各節將引導您檢視配置面板：

啟動配置

遵循這些步驟：

1. 歡迎

配置程式中的第一個面板為版權頁。按 [下一步] (Next) 以繼續，或按 [取消] (Cancel) 結束。

2. 選取儲存配置和資料檔案的目錄

選取您要儲存 **Delegated Administrator** 配置和資料檔案的目錄。預設配置目錄為 `//var/opt/SUNWcomm`。此目錄必須與 `da_base` 目錄 (`//opt/SUNWcomm`) 分隔開來。

輸入目錄名稱，或保留預設，然後按 [下一步] (Next) 以繼續。

如果目錄不存在，會出現一個對話方塊，詢問您是否要建立目錄，或選擇一個新目錄。按一下 [建立目錄] (Create Directory) 以建立目錄，或按一下 [選擇新目錄] (Choose New) 輸入一個新的目錄。

接下來會出現一個對話方塊，表示您正在載入一些元件。這將需要幾分鐘的時間。

3. 選取要配置的元件

選取一個或多個要配置在元件面板上的元件。

- **Delegated Administrator 公用程式 (用戶端)** – 使用 `commadmin` 呼叫指令行介面。此元件為必要元件，且為依照預設所選取。您無法將其取消選取。
- **Delegated Administrator 伺服器** – 需要 **Delegated Administrator 伺服器** 元件以執行 **Delegated Administrator 主控台**。
- **Delegated Administrator 主控台** – **Delegated Administrator** 圖形化使用者介面 (GUI)。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

如需如何選擇元件的詳細資訊，請參閱「[選擇要配置的元件](#)」。

如果您選擇不配置 **Delegated Administrator 伺服器**，則會出現一個對話方塊，警告您必須將 **Delegated Administrator 伺服器** 配置在另一台機器上。伺服器必須配置成能夠啟用 **Delegated Administrator 公用程式** 和 **主控台** 進行運作。

配置 Delegated Administrator 公用程式

請遵循這些步驟：

1. Access Manager 主機名稱和連接埠號碼

輸入 Access Manager (之前稱為 Identity Server) 主機名稱和連接埠號碼。如果您正在安裝 Delegated Administrator 伺服器元件，您必須將其安裝在與 Access Manager 相同的主機上。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

2. 預設網域

輸入頂層管理員的預設網域。在執行 `commadmin` 指令行公用程式時，若沒有使用 `-n` 選項來特別指定網域，則這就是所使用的網域。這也稱為預設社團組織。如果指定的網域不存在於目錄中，系統會自動建立一個。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

3. 用戶端的預設 SSL 連接埠

輸入 Delegated Administrator 公用程式所使用的預設 SSL 連接埠。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

4. 如果您選擇只配置 Delegated Administrator 公用程式，請移至

[完成配置](#)

如果您選擇同時配置 Delegated Administrator 主控台和伺服器，或者選擇只配置主控台，請移至

[配置 Delegated Administrator 主控台](#)

如果您選擇只配置 Delegated Administrator 伺服器 (與必要的 Delegated Administrator 公用程式一起配置)，請移至

[配置 Delegated Administrator 伺服器](#)

配置 Delegated Administrator 主控台

現在配置程式顯示以下的面板：

為 Delegated Administrator 選取一個 Web 容器 (Select a Web Container for Delegated Administrator)

選取一個您將在其中部署 Delegated Administrator 主控台的 Web 容器。您可以將 Delegated Administrator 配置在

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

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

此面板以及之後的面板會收集關於 Delegated Administrator 主控台的 Web 容器資訊。請遵循適當章節中的說明：

- [Web Server 配置](#)
- [Application Server 7.x 配置](#)
- [Application Server 8.x 配置](#)

您可以在兩個不同的 Web 容器上、兩個不同的 Web 容器實例上，或者在相同的 Web 容器上部署 Delegated Administrator 主控台和伺服器。

如果您選擇在面板 3 上同時配置 Delegated Administrator 主控台和 Delegated Administrator 伺服器，第二階段的面板將會詢問您關於伺服器的 Web 容器資訊。

因此，您將會看到 Web 容器配置面板兩次。請遵循適當的說明，以部署每個 Delegated Administrator 元件。

當您完成 Web 容器配置面板時：

- 如果您選擇同時配置 Delegated Administrator 主控台和伺服器，請移至 [配置 Delegated Administrator 伺服器](#)
- 如果您選擇只配置 Delegated Administrator 主控台 (與必要的 Delegated Administrator 公用程式一起配置)，請移至 [完成配置](#)

Web Server 配置

如果您正在 Web Server 上部署 Delegated Administrator 伺服器或主控台，請遵循這些步驟：

1. Web Server 配置詳細資訊

面板中的文字會告訴您，是否正在輸入 Delegated Administrator 伺服器或主控台所需的 Web Server 配置資訊。

輸入 Web Server 根目錄。您可以進行瀏覽以選取目錄。

輸入 Web Server 實例識別碼。這可以使用 *host.domain* 名稱 (如 *west.sesta.com*) 來指定。

輸入虛擬伺服器識別碼。這可以使用 *https-host.domain* 名稱 (如 *https-west.sesta.com*) 來指定。

有關 Web Server 實例識別碼和虛擬伺服器識別碼的詳細資訊，請參閱 Web Server 文件。

Web Server 實例的檔案儲存在 Web Server 安裝目錄下的 *https-host.domain* 目錄中。例如，*/opt/SUNWwbsvr/https-west.sesta.com*。

輸入 Web Server 的 HTTP 連接埠號碼。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

配置程式會檢查您指定的值是否有效。如果目錄或識別碼無效或不存在，會出現一個對話方塊，指示您選擇一個新的值。

接下來，配置程式會檢查 Web Server 實例連線是否有作用。如果沒有作用，對話方塊會警告您，配置程式無法連線至指定的實例，您的配置可能無法完成。您可以接受指定的值，或選擇新的 Web Server 配置值。

2. 預設網域分隔符

只有當您配置 Delegated Administrator 主控台時才會出現此面板。您需要網域分隔符來配置主控台，此資訊與 Web 容器並沒有關係。

輸入在使用者登入時供認證使用的預設網域分隔符。例如：*@*。

daconfig.properties 檔案中已包含了網域分隔符的值。您可以在執行配置程式之後編輯此特性值。如需更多資訊，請參閱「自訂 Delegated Administrator」。

3. 如果您正在配置 Delegated Administrator 主控台：

- 如果您選擇同時配置 Delegated Administrator 主控台和伺服器，請移至 [配置 Delegated Administrator 伺服器](#)
- 如果您選擇只配置 Delegated Administrator 主控台 (與必要的 Delegated Administrator 公用程式一起配置)，請移至 [完成配置](#)

如果您正在配置 Delegated Administrator 伺服器：

請移至

[配置 Delegated Administrator 伺服器](#) 中的步驟 3，[Directory \(LDAP\) Server](#)。

Application Server 7.x 配置

如果您在 Application Server 7.x 上部署 Delegated Administrator 伺服器或主控台，請遵循這些步驟：

1. Application Server 7.x 配置詳細資訊

面板中的文字會告訴您，是否正在輸入 Delegated Administrator 伺服器或主控台所需的 Application Server 7.x 配置資訊。

輸入 Application Server 安裝目錄。依預設，此目錄為 `/opt/SUNWappserver7`。

輸入 Application Server 網域目錄。依預設，此目錄為 `/var/opt/SUNWappserver7/domains/domain1`。

輸入 Application Server 文件根目錄。依預設，此目錄為 `/var/opt/SUNWappserver7/domains/domain1/server1/docroot`。

您可以進行瀏覽以選取這些目錄。

輸入 Application Server 實例名稱。例如：`server1`。

輸入 Application Server 虛擬伺服器識別碼。例如：`server1`。

輸入 Application Server 實例的 HTTP 連接埠號碼。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

配置程式會檢查您指定的目錄是否有效。如果目錄無效或不存在，會出現一個對話方塊，指示您選擇一個新的目錄。

接下來，配置程式會檢查 Application Server 實例連線是否有作用。如果沒有作

用，對話方塊會警告您，配置程式無法連線至指定的實例，您的配置可能無法完成。您可以接受指定的值，或選擇新的 Application Server 配置值。

2. Application Server 7.x：管理實例詳細資訊

輸入 Administration Server 連接埠號碼。例如：4848。

輸入 Administration Server 管理員使用者 ID。例如：admin。

輸入管理員使用者密碼。

如果您正在使用安全 Administration Server 實例，請選取 [安全 Administration Server 實例] (Secure Administration Server Instance) 方塊。如果您並沒有使用，請勿核取此方塊。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

3. 預設網域分隔符

只有當您配置 Delegated Administrator 主控台時才會出現此面板。您需要網域分隔符來配置主控台，此資訊與 Web 容器並沒有關係。

輸入在使用者登入時供認證使用的預設網域分隔符。例如：@。

4. 如果您正在配置 Delegated Administrator 主控台：

- 如果您選擇同時配置 Delegated Administrator 主控台和伺服器，請移至 [配置 Delegated Administrator 伺服器](#)
- 如果您選擇只配置 Delegated Administrator 主控台 (與必要的 Delegated Administrator 公用程式一起配置)，請移至 [完成配置](#)

如果您正在配置 Delegated Administrator 伺服器：

請移至

[配置 Delegated Administrator 伺服器](#) 中的步驟 3，Directory (LDAP) Server。

Application Server 8.x 配置

如果您在 Application Server 8.x 上部署 Delegated Administrator 伺服器或主控台，請遵循這些步驟：

1. Application Server 8.x 配置詳細資訊

面板中的文字會告訴您，是否正在輸入 Delegated Administrator 伺服器或主控台所需的 Application Server 8.x 配置資訊。

輸入 Application Server 安裝目錄。依預設，此目錄為
`/opt/SUNWappserver/appserver`。

輸入 Application Server 網域目錄。依預設，此目錄為
`/var/opt/SUNWappserver/domains/domain1`。

輸入 Application Server 文件根目錄。依預設，此目錄為
`/var/opt/SUNWappserver/domains/domain1/docroot`。

您可以進行瀏覽以選取這些目錄。

輸入 Application Server 目標名稱。例如：`server`。

輸入 Application Server 虛擬伺服器識別碼。例如：`server`。

輸入 Application Server 目標的 HTTP 連接埠號碼。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

配置程式會檢查您指定的目錄是否有效。如果目錄無效或不存在，會出現一個對話方塊，指示您選擇一個新的目錄。

接下來，配置程式會檢查 Application Server 目標連線是否有作用。如果沒有作用，對話方塊會警告您，配置程式無法連線至指定的目標，您的配置可能無法完成。您可以接受指定的值，或選擇新的 Application Server 配置值。

2. Application Server 8.x：管理實例詳細資訊

輸入 Administration Server 連接埠號碼。例如：`4849`。

輸入 Administration Server 管理員使用者 ID。例如：`admin`。

輸入管理員使用者密碼。

如果您正在使用安全 Administration Server 實例，請選取 [安全 Administration Server 實例] (Secure Administration Server Instance) 方塊。如果您並沒有使用，請勿核取此方塊。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

3. 預設網域分隔符

只有當您配置 Delegated Administrator 主控台時才會出現此面板。您需要網域分隔符來配置主控台，此資訊與 Web 容器並沒有關係。

輸入在使用者登入時供認證使用的預設網域分隔符。例如：@。

4. 如果您正在配置 Delegated Administrator 主控台：

- 如果您選擇同時配置 Delegated Administrator 主控台和伺服器，請移至 [配置 Delegated Administrator 伺服器](#)
- 如果您選擇只配置 Delegated Administrator 主控台 (與必要的 Delegated Administrator 公用程式一起配置)，請移至 [完成配置](#)

如果您正在配置 Delegated Administrator 伺服器：

請移至

[配置 Delegated Administrator 伺服器](#)中的步驟 3，Directory (LDAP) Server。

配置 Delegated Administrator 伺服器

如果您選擇配置 Delegated Administrator 伺服器，配置程式會顯示以下的面板。輸入這些面板所要求的資訊：

1. Access Manager 基底目錄

輸入 Access Manager 基底目錄。預設目錄為 /opt/SUNWam。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

配置程式會檢查您是否已指定了一個有效的 Access Manager 基底目錄。如果不是，對話方塊會指示您必須選取一個現存的 Access Manager 基底目錄。

2. 接下來會出現 Web 容器的 [配置詳細資訊] (Configuration Details) 面板。

如果您選擇配置主控台和伺服器，將第二次出現 Web 容器的 [配置詳細資訊] (Configuration Details) 面板。

Delegated Administrator 伺服器已部署到與 Access Manager 相同的 Web 容器中。(您不能為 Delegated Administrator 伺服器選擇 Web 容器。)

請遵循適當章節中的說明：

- [Web Server 配置](#)
- [Application Server 7.x 配置](#)
- [Application Server 8.x 配置](#)

3. Directory (LDAP) Server

面板會詢問您關於連線至使用者 / 群組尾碼的 LDAP Directory Server 之資訊。

在文字方塊中輸入使用者與群組 Directory Server LDAP URL (**LdapURL**)、Directory Manager (**連結為**) 和密碼。

Directory Manager 在 Directory Server 和所有使用 Directory Server 的 Sun Java System 伺服器 (例如, Delegated Administrator) 上, 都擁有完整的管理員權限, 且能夠以管理員的身分存取 Directory Server 中的所有項目。預設以及建議的辨別名稱 (DN) 為 cn=Directory Manager。

按 [下一步] (Next) 以繼續, 或按 [上一步] (Back) 回到前一個面板, 或按 [取消] (Cancel) 結束。

4. Access Manager 頂層管理員

輸入 Access Manager 頂層管理員的使用者 ID 和密碼。使用者 ID 和密碼會在安裝 Access Manager 的同時建立。預設的使用者 ID 為 amadmin。

按 [下一步] (Next) 以繼續, 或按 [上一步] (Back) 回到前一個面板, 或按 [取消] (Cancel) 結束。

5. Access Manager 內部 LDAP 認證密碼

輸入 Access Manager 內部 LDAP 認證使用者的密碼。

認證使用者名稱為程序內定的 amldapuser。這是由 Access Manager 安裝程式所建立, 並且為 LDAP 服務的連結 DN 使用者。

按 [下一步] (Next) 以繼續, 或按 [上一步] (Back) 回到前一個面板, 或按 [取消] (Cancel) 結束。

6. 社團組織辨別名稱 (DN)

輸入預設網域的社團組織 DN。例如，如果您的社團組織 DN 為 `o=siroe.com`，所有該組織中的使用者都會被放置在 LDAP DN 「`o=siroe.com, o=usergroup`」之下，其中 `o=usergroup` 為您的根尾碼。

依預設，配置程式會在 LDAP 目錄中的根尾碼下新增預設網域。

如果您要在根尾碼上 (不是在其下方) 建立預設網域，請在 [社團組織辨別名稱 (DN)] 文字方塊的 DN 中刪除該社團組織名稱。

例如，如果您的社團組織 DN 為 `o=siroe.com`，而根尾碼為 `o=usergroup`，請在文字方塊的 DN 中刪除 `o=siroe.com`，只留下 `o=usergroup`。

如果您選擇將預設網域建立在根尾碼上，並隨後決定使用託管網域，您將很難將其遷移到託管網域配置。`config-commda` 程式顯示以下的警告：

「您所選擇的社團組織 DN 為使用者 / 群組尾碼。雖然這是個有效的選擇，然而如果您以後決定使用託管網域，遷移的作業將變得很困難。如果您確定要使用託管網域，請在使用者 / 群組尾碼的下一層指定一個 DN。」

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

如需更多資訊，請參閱第 1 章「[Delegated Administrator 簡介](#)」中的「[支援單層次階層的目錄結構](#)」。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

7. 預設社團組織的頂層管理員

輸入將在預設網域 (社團組織) 中建立的頂層管理員使用者 ID 和密碼。

按 [下一步] (Next) 以繼續，或按 [上一步] (Back) 回到前一個面板，或按 [取消] (Cancel) 結束。

8. 服務套裝軟體和社團組織範例

您可以選擇新增服務套裝軟體範例和社團組織範例到 LDAP 目錄中。

載入服務套裝軟體範例。如果您要使用或修改服務套裝軟體範本範例，以建立您自己的服務等級套裝軟體，請選取此選項。(在 [Delegated Administrator](#) 中，您至少要將一個服務等級套裝軟體指定給 LDAP 目錄中的每個使用者。)

載入社團組織範例。如果您希望 LDAP 目錄樹中能包含服務提供者社團組織和企業社團組織的節點範例，請選取此選項。

您可以選取

- 服務套裝軟體範例和社團組織範例兩者
- 僅這些選項其中之一
- 全都不選

喜好的郵件主機範例。輸入已安裝 Messaging Server 的機器名稱。

例如：mymachine.siroe.com

如果您選擇將社團組織範例載入到 LDAP 目錄中，您必須為這些範例輸入喜好的郵件主機名稱。

有關服務套裝軟體和社團組織的詳細資訊，請參閱第 2 章：「Delegated Administrator 簡介」。

在執行配置程式之後，您必須修改服務套裝軟體範本以建立您自己的服務等級套裝軟體。有關此配置後作業，請參閱「[建立服務套裝軟體](#)」。

完成配置

若要完成配置，請執行這些步驟：

1. 準備配置

驗證面板會顯示將配置的項目。

按 [現在配置] (Configure Now) 以開始配置，按 [上一步] (Back) 回到前一個面板以變更資訊，或按 [取消] (Cancel) 結束。

2. 作業序列

[作業序列] (Task Sequence) 面板會顯示正在執行的作業序列。這時候才會開始實際的配置。

當面板顯示 [已傳送所有作業] (All Tasks Passed) 時，可以按 [下一步] (Next) 以繼續，或按 [取消] (Cancel) 停止執行並結束。

此時會出現一個對話方塊，提醒您重新啟動 Web 容器，使配置的變更能夠生效。

3. 安裝摘要

[安裝摘要] (Installation Summary) 面板會顯示已安裝的產品，[詳細資訊 . . .] (Details...) 按鈕會顯示關於配置的詳細資訊。

config-commda 的記錄檔會建立在 /opt/SUNWcomm/install 目錄中。記錄檔的名稱為 commda-config_YYYYMMDDHHMMSS.log，其中 YYYYMMDDHHMMSS 標示配置的年 (四位數)、月、日、小時、分鐘和秒。

按一下 [關閉] (Close) 以完成配置。

重新啟動 Web 容器

在完成 Delegated Administrator 的配置之後，您必須重新啟動已部署 Delegated Administrator 的 Web 容器 (下列其中一個)：

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

由 config-commda 程式所建立的配置和記錄檔

配置檔

config-commda 程式會使用您在面板中所提供的資訊，為三個 Delegated Administrator 元件建立以下的配置檔：

- Delegated Administrator 公用程式：
 - 配置檔名稱：cli-usrprefs.properties
 - 預設的位置：/var/opt/SUNWcomm/config
- Delegated Administrator 伺服器：
 - 配置檔名稱：resource.properties
 - 預設的位置：
 - /opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet
 - 或
 - /var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet

- Delegated Administrator 主控台：

配置檔名稱：daconfig.properties

預設的位置：

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

或

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

針對這些檔案、檔案中所包含的特性，以及如何編輯這些特性以自訂您的配置，請參閱「自訂 Delegated Administrator」以取得詳細資訊。

記錄檔

Delegated Administrator 主控台建立一個執行階段記錄檔：

預設記錄檔名稱：da.log

預設的位置：/opt/SUNWcomm/log

如需這個與其他 Delegated Administrator 記錄檔的詳細資訊，請參閱[附錄 C 「除錯 Delegated Administrator」](#)。

執行無訊息安裝

Delegated Administrator 公用程式初始執行階段配置程式會自動建立一個無訊息安裝狀態檔（稱為 saveState）。這個檔案包含了配置程式的內部資訊，並用來執行無訊息安裝。

無訊息安裝 saveState 檔案儲存在

/opt/SUNWcomm/data/setup/commda-config_YYYYMMDDHHMMSS/ 目錄中，其中 YYYYMMDDHHMMSS 標示 saveState 檔案的年（四位數）、月、日、小時、分鐘和秒。

例如，只要您執行過 config-commda 程式一次，您就能以無訊息安裝模式執行它。

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

fullpath 變數為 saveState 檔案所在的完整目錄路徑。

執行 Delegated Administrator 主控台和公用程式

啟動主控台

若要啟動 Delegated Administrator 主控台，請執行這些步驟：

1. 移至以下 URL：

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

其中

host 為 Web 容器主機電腦

port 為 Web 容器連接埠

例如：

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

出現 Delegated Administrator 主控台登入視窗。

2. 登入 Delegated Administrator 主控台。

您可以使用在 Delegated Administrator 配置程式中所指定的頂層管理員 (TLA) 使用者 ID 和密碼。以下的面板會要求您提供此資訊：

預設社團組織的頂層管理員 (Top-Level Administrator for the default organization)

執行指令行公用程式

若要執行 Delegated Administrator 公用程式 (commadmin)，請執行這些步驟：

1. 請移至 *da_base/bin/* 目錄。例如，移至 */opt/SUNWcomm/bin/*。
2. 輸入 commadmin 指令。

例如：

```
commadmin -D userid -w password
```

其中，*userid* 和 *password* 為 Delegated Administrator 配置程式中所指定的頂層管理員 (TLA) 使用者 ID 和密碼。以下的面板會要求您提供此資訊：

預設社團組織的頂層管理員 (Top-Level Administrator for the default organization)

配置後作業

在您執行 Delegated Administrator 配置程式後，應該執行以下的作業：

- [在預設網域中新增郵件和行事曆服務](#)
- [建立服務套裝軟體](#)

只有當您在 Schema 2 相容性模式中使用 LDAP 目錄時，才執行以下的作業：

- [新增 Schema 2 相容性模式的 ACI](#)

在預設網域中新增郵件和行事曆服務

config-commda 程式會建立一個預設網域。

如果您要透過預設網域中的郵件服務或行事曆服務建立使用者，您首先必須將郵件服務和行事曆服務新增到網域中。

若要執行此作業，請使用 `commadmin domain modify` 指令以及 `-S mail` 和 `-S cal` 選項。

以下的範例顯示您要如何使用 `commadmin domain modify` 將郵件和行事曆服務新增到預設網域：

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

如需 `commadmin` 的指令語法和詳細資訊，請參閱第 5 章「[指令行公用程式](#)」。

建立服務套裝軟體

每個由 Delegated Administrator 佈建在 LDAP 目錄中的使用者都應該擁有一個服務套裝軟體。一個使用者可以擁有一個以上的服務套裝軟體。

預先定義服務等級範本

當您執行 Delegated Administrator 配置程式 (`config-commda`) 時，LDAP 目錄中已安裝了一個服務等級範本 (`defaultmail`)。您也可以選擇使用 `config-commda` 程式將一組八個服務等級範例安裝在目錄中。

有關服務等級範本和服務套裝軟體中可用的郵件屬性之資訊，請參閱第 1 章「[Delegated Administrator 簡介](#)」中的「[服務套裝軟體](#)」。

您可以將服務等級範本做為服務套裝軟體使用。然而，這些範本旨在作為範例參考。

建立您自己的服務套裝軟體

您可能必須藉由在安裝過程中使用者所適用的屬性值，來建立您自己的服務套裝軟體。

若要建立您自己的服務套裝軟體，可以使用儲存在 `da.cos.skeleton.ldif` 檔案中的服務等級範本。

建立該檔案的目的就是要做為寫入服務套裝軟體的範本。當配置 **Delegated Administrator** 時，該檔案並沒有安裝在 LDAP 目錄中。

`da.cos.skeleton.ldif` 檔案中的服務等級範本如下所示：

```
# Template for creating a COS template for a service package.
#
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
# Consult documentation for values for the attributes. Documentation
# includes units and default values.
#
# The finished COS derived from this skeleton is added to the directory with
# the following command:
#
# ldapmodify -D <directory manager> -w <password>
# -f <cos.finished.template.ldif>
#
dn: cn=<service package name>,o=cosTemplates,<rootSuffix>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailQuota: <mailQuotaValue>
mailMsgQuota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
```

若要建立您自己的服務套裝軟體，請遵循這些步驟：

1. 複製並重新命名 `da.cos.skeleton.ldif` 檔案。

當您安裝 **Delegated Administrator** 時，`da.cos.skeleton.ldif` 檔案已安裝在以下的目錄中：

```
da_base/lib/config-templates
```

2. 在 `da.cos.skeleton.ldif` 檔案的副本中編輯下列項目：

- `<rootSuffix>`

變更根尾碼參數 `rootSuffix` 為您的根尾碼 (如 `o=usergroup`)。

`<rootSuffix>` 參數出現在 DN 中。

- `<service package name>`

將 `<service package name>` 參數變更為您自己的服務套裝軟體名稱。

`<service package name>` 參數出現在 DN 和 `cn` 中。

- 郵件屬性值：

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

編輯這些值以符合您的規格。

例如，您可以輸入以下的值做為郵件屬性：

```
mailMsgMaxBlocks: 400  
mailQuota: 40000000  
mailMsgQuota: 5000  
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

有關這些屬性的定義和描述，請參閱「[Sun Java System Communications Services Schema Reference](#)」中的第 3 章「[Attributes](#)」。

您不需要在服務套裝軟體中使用全部四種郵件屬性。您可以刪除服務套裝軟體中的一種或多種屬性。

3. 使用 LDAP 目錄工具 `ldapmodify` 將服務套裝軟體安裝在目錄中。

例如，您可以執行下列指令：

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

其中

`<directory manager>` 是 Directory Server 管理員的名稱。

`<password>` 是 Directory Server 管理員的密碼。

`<cos.finished.template.ldif>` 為已編輯的 ldif 檔案名稱，該檔案將做為服務套裝軟體安裝在目錄中。

新增 Schema 2 相容性模式的 ACI

如果您在 Schema 2 相容性模式中使用 LDAP 目錄，您必須以手動的方式新增 ACI 到目錄中，以啟用 Delegated Administrator 在目錄中進行佈建。採取下列步驟：

1. 新增下列兩個 ACI 到 OSI 根。您可以在位於 `/opt/SUNWcomm/config` 目錄的 `usergroup.ldif` 檔案中找到下列兩個 ACI。

確定要以 `usergroup` 根尾碼來替代 `ugldapbasedn`。將已編輯的 `usergroup.ldif` 新增到 LDAP 目錄中。

```
#
# acis to limit Org Admin Role
#
#####
# dn: <local.ugldapbasedn>
#####
dn: <ugldapbasedn>
changetype: modify
add: aci
```

```

aci: (target="ldap:///($dn),<ugldapbasedn>") (targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>");

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

```

2. 新增下列兩個 ACI 到 DC 樹的根尾碼。您可以在位於 /opt/SUNWcomm/config 目錄的 dctree.ldif 檔案中找到下列兩個 ACI。

確定要以 DC 樹的根尾碼來替代 *dctreebasedn*，並以 *usergroup* 根尾碼來替代 *ugldapbasedn*。將已編輯的 *dctree.ldif* 新增到 LDAP 目錄中。

```

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

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

```


3. 新增下列額外的 ACI 到 DC 樹的根尾碼。(這些 ACI 並不在 `dctree.ldif` 檔案中。)

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

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

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

4. 將 `AMConfig.properties` 檔案中的 `com.iplanet.am.domaincomponent` 特性設定成 DC 樹的根尾碼。例如，修改 `<IS_base_directory>/lib/AMConfig.properties` 檔案中的以下行：

```
將
com.iplanet.am.domaincomponent=o=isp
修改成
com.iplanet.am.domaincomponent=o=internet
```

5. 啟用 Access Manager (之前稱為 Identity Server) 以使用相容性模式。在 Access Manager 主控台的 [管理主控台服務] (Administration Console Service) 頁中，核取 (啟用) [已啟用網域元件樹] (Domain Component Tree Enabled) 核取方塊。

6. 新增 `inetdomain` 物件類別到所有的 DC 樹節點中 (例如 `dc=com,o=internet`)，如下範例所示：

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

7. 重新啓動 Web 容器。

三言 Delegated Administrator

在使用配置程式 (config-commda) 安裝和配置 Delegated Administrator 之後，您可以自訂您的配置以符合特殊需求。本章提供如何自訂某些 Delegated Administrator 功能的範例。

本章描述下列主題：

- 使用服務整體的預設值配置喜好的郵件主機
- 為 Delegated Administrator 新增外掛程式
- 自訂使用者登入

使用服務整體的預設值配置喜好的郵件主機

如果您希望使用伺服器整體的預設值設定 [喜好的郵件主機] 和 [喜好的郵件儲存]，您可以執行這一節所描述的作業。

如果您需要從主控台 (具體而言，從 [建立新社團組織] 精靈與 [社團組織特性] 螢幕) 移除 [喜好的郵件主機] 欄位，您應採取下列步驟：

- 編輯 Security.properties 檔案。此步驟將在本節中描述。
- 啟用 MailHostStorePlugin。此步驟將在下一節「為 Delegated Administrator 新增外掛程式」中描述。

Security.properties 檔案可讓您為所有或個別角色自訂 Delegated Administrator 主控台。

Security.properties 檔案位於
da_base/da/WEB-INF/classes/com/sun/comm/da/resources 目錄中。

若要從主控台移除喜好的郵件主機，請將下列顯示的指令行新增到 Security.properties 檔案：

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

注意：您可以依自訂將指令行新增到這個檔案，但請勿編輯已經存在的指令行。編輯現有的指令行可能會導致主控台上丟出異常。

檔案中的特性格式：*Security Element Name=Permission*

「安全性元素名稱」的格式：

Role Name.Container View Name.Console Element Name

安全性元素可指定正在為其定義權限的主控台元素與角色。如果您不知道元素名稱，請檢視頁面原始檔，來比對頁面上的名稱和您感興趣的主控台元素。

頁面上的名稱是完全合格的名稱。您只需選擇最後兩個名稱元素，即構成 *Container View Name.Console Element Name* 的元素。

有效的 Delegated Administrator 角色名稱列示如下：

「ProviderAdminRole」（SPA）。有關此角色的資訊，請參閱 [附錄 A](#)，「服務提供者管理員及服務提供者社團組織」。

「OrganizationAdminRole」（OUA）

「Top-levelAdminRole」（TLA）

「*」（套用權限到所有角色，除非因為特定角色而置換它）

權限必須是下列字串之一：

- EDITABLE — 代表安全性元素是可編輯的。
- NONEDITABLE — 代表安全性元素是唯讀的。
- VISIBLE — 代表安全性元素是可視且唯讀的。
- INVISIBLE — 代表安全性元素不是可視的。

Delegated Administrator 新增外掛程式

您可以自訂 Delegated Administrator 以支援下列外掛程式：

- MailHostStorePlugin
依照預設，會停用此外掛程式。如果建立企業社團組織時未提供 preferredmailhost，將會產生異常。如果啟用此外掛程式，則只有缺少對應的屬性時，才會使用平面檔案中的值（在本節稍後描述）。
- MailDomainReportAddressPlugin
使用網域值來傳回您想要的 DSN 位址。預設實作是傳回字串 MAILER-DAEMON@<domain>。
- UidPlugin
產生唯一的 ID 字串。預設的實作是產生一個 GUID 來傳回給呼叫者。
- VolInternalLoginPlugin
使用「volmaillogin」屬性值（由 Delegated Administrator 主控台所傳入）與在 volinternalloginpluginfile. 中找到的值，來設定屬性「volinternallogin」。volinternallogin 屬性的格式是 <volmaillogin value>@<value-found in file>。如需 volinternalloginpluginfile 的詳細資訊，請參閱本節後面的「[兩個外掛程式的其他平面檔案](#)」。
在 resource.properties 檔案中，attr-loginid 必須設為 volmaillogin。
- ObjectclassPlugin
將「volperson」物件類別新增到每個建立的使用者。

啓用此外掛程式

如果要啓用這些外掛程式，請編輯 commcli servlet resource.properties 檔案。該檔案位於下列目錄中：

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

（依照預設，da_base 是 /opt/SUNWcomm。）

此外掛程式位於 resource.properties 檔案中以下列標頭啓始的部分：

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

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

```
jdapi-mailhoststoreplugin=disabled
```

```
jdapi-mailhoststorepluginclass=sun.comm.cli.server.util.MailHostStorePlugin
jdapi-mailhoststorepluginfile=/tmp/mailhostmailstore
jdapi-volinternalloginplugin=disabled
jdapi-volinternalloginpluginclass=sun.comm.cli.server.util.
    VolInternalLoginPlugin
jdapi-volinternalloginpluginfile=/tmp/volinternalloginplugin
jdapi-objectclassplugin=disabled
jdapi-objectclasspluginclass=sun.comm.cli.server.util.ObjectClassPlugin
jdapi-maildomainreportaddressplugin=enabled
jdapi-maildomainreportaddresspluginclass=sun.comm.cli.server.
    util.MailDomainReportAddressPlugin
jdapi-uidautogenerationplugin=disabled
jdapi-uidautogenerationpluginclass=sun.comm.cli.server.util.UidPlugin
```

外掛程式格式

每個外掛程式都至少有兩個指令行，格式如下：

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

如果要啓用外掛程式，請將「disabled」變更為「enabled」。

本節中列出的所有外掛程式均提供外掛程式類別。類別位於下列目錄中：

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

您不需要對這些類別進行任何操作。

兩個外掛程式的其他平面檔案

MailHostStorePlugin 與 VolInternalLoginPlugin 這兩個外掛程式需要一個平面檔案，該檔案包含在外掛程式的第三列中。外掛程式會讀取平面檔案中的值，並用它來設定屬性值。如果啓用外掛程式，則該檔案必須存在，否則將會發生錯誤。

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

- `jdapi-volinternalloginplugin`
 - `jdapi-volinternalloginpluginfile=<full file name>`
 - file has one line
 - value is that for
 - right hand side of `volinternallogin` attribute

自訂使用者登入

當您執行 Delegated Administrator 配置程式 (`config-commda`) 時，您用來登入 Delegated Administrator 的值會設為 `uid`。

例如，如果您想以 TLA 身份登入，而且 TLA 的 `uid` 是 `john.doe`，則您要使用 `john.doe` 登入 Delegated Administrator。

您可以自訂 Delegated Administrator 以讓您可使用其他的使用者登入值。例如，您可以新增郵件位址 (`mail`)。

如何設定使用者登入值

`config-commda` 程式使用 `resource.properties` 檔案中的 `loginAuth-idAttr` 特性將此值設為 `uid`，如下列範例所示：

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

其中，`<$rootSuffix>` 是您目錄中的根尾碼。

`resource.properties` 檔案位於
`/var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet/`
`resource.properties`。

新增使用者登入值

您可以編輯 `resource.properties` 檔案來設定其他的使用者登入值。

例如，為了讓您能使用郵件位址 (例如 `john.doe@sesta.com`) 來登入，您可以新增下列指令行到 `resource.properties` 檔案：

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

其中，<\$rootSuffix> 是您目錄中的根尾碼。

請注意，您必須為每個新值新增一個遞增量到 loginAuth-idAttr 特性。在此範例中新增了第二個值，所以您要將 -2 新增到 loginAuth-idAttr。

您可以新增多個 loginAuth-idAttr 特性的實例：

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


指令行公用程式

Delegated Administrator 指令行公用程式使管理員可以針對使用者、群組、網域及社團組織來管理不同的通訊服務。本章討論用來執行大量作業 (例如建立、修改、刪除和搜尋使用者、群組、網域及社團組織) 的指令行工具集。

這些指令行在表 5-1 中。此表格包含三個欄位，第一個欄位列出指令，第二個是指令的描述，第三個則列出可以執行指令的管理員類型。

commadmin 公用程式位於 /opt/SUNWcomm/bin 目錄。

表 5-1 Delegated Administrator 指令行介面

指令	描述	執行的權限*
<code>commadmin admin add</code>	授予「社團組織管理員」權限給使用者	頂層管理員
<code>commadmin admin remove</code>	撤銷使用者的「社團組織管理員」權限	頂層管理員
<code>commadmin admin search</code>	搜尋和顯示擁有「社團組織管理員」權限的使用者	頂層管理員、社團組織管理員
<code>commadmin domain create</code>	建立網域	頂層管理員
<code>commadmin domain delete</code>	刪除網域	頂層管理員
<code>commadmin domain modify</code>	修改網域	頂層管理員
<code>commadmin domain purge</code>	清除網域	頂層管理員
<code>commadmin domain search</code>	搜尋網域	頂層管理員
<code>commadmin group create</code>	建立群組	頂層管理員、社團組織管理員和和郵件清單所有者
<code>commadmin group delete</code>	刪除群組	頂層管理員、社團組織管理員和和郵件清單所有者

表 5-1 Delegated Administrator 命令行介面 (續)

指令	描述	執行的權限*
<code>commadmin group modify</code>	修改群組	頂層管理員、社團組織管理員和和郵件清單所有者
<code>commadmin group search</code>	搜尋群組	任何人
<code>commadmin resource create</code>	建立資源	頂層管理員、社團組織管理員
<code>commadmin resource modify</code>	修改資源	頂層管理員、社團組織管理員
<code>commadmin resource delete</code>	刪除資源	頂層管理員、社團組織管理員
<code>commadmin resource search</code>	搜尋資源	任何人
<code>commadmin user create</code>	建立使用者	頂層管理員、社團組織管理員
<code>commadmin user delete</code>	刪除使用者	頂層管理員、社團組織管理員
<code>commadmin user search</code>	搜尋使用者	任何人
<code>commadmin user modify</code>	修改使用者	頂層管理員、社團組織管理員

* 這個版本的 Delegated Administrator 不支援服務提供者管理員使用 `commadmin` 公用程式。

執行模式

命令行執行有三種可能的模式：

- 以檔案中指定的選項執行
`commadmin object task -i inputfile`
 分析 *inputfile* 並加以執行。
- 互動式
`commadmin object task`
 查詢管理員以取得選項和屬性剩餘的項目。
- 立即或 shell 執行
`commadmin object task [options]`

指令檔格式

選項可在檔案中使用 `-i` 選項指定。

在檔案中，選項名稱以空格分隔選項值。選項值以第一個非空格字元開頭，延伸到行尾字元。選項集以空行分隔。

一般語法為：

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

在指令行中指定的選項值，會成為每個選項集的預設值。另外，也可以為每個選項集指定這些選項。該值會覆寫指令行中指定的任何預設值。

下列是 `comadmin user add` 指令的 `-i` 選項所指定的檔案格式和語法的範例。

```
l newuser1
F new
L user1
W secret

l newuser2
F new
L user2
W secret

l newuser3
F new
L user3
W secret

<and so forth...>
```

指令描述

本節提供指令行工具的描述、語法及範例。

重要的 commadmin 選項

下列是用來驗證管理員或使用者的必要選項。

選項	描述
-D <i>userid</i>	用來連結到目錄的使用者 ID。
-w <i>password</i>	用來驗證存取目錄的使用者 ID 的密碼。 您也可以透過文字檔 <i>password.txt</i> 指定密碼。
-n <i>domain</i>	管理員所屬的網域。

Access Manager 主機 (-x)、Access Manager 連接埠 (-p) 以及預設網域 (-n) 值均是在安裝過程中指定的，並且儲存在 `cli-userprefs.properties` 檔案中。

備註	如果 -x、-p 以及 -n 選項不是在執行 <code>commadmin</code> 指令時指定的，則其值是從 <code>cli-userprefs.properties</code> 檔案中所擷取。
-----------	--

commadmin admin add

`commadmin admin add` 指令可授予使用者特定網域的「社團組織管理員」權限。只有頂層管理員或 ISP 管理員可以執行這個指令。

語法

```
comadmin admin add -D login -l login -n domain -w password -d domain
[-h]
[-i inputfile] [-p IS Port] [-X IS Host] [-?] [-s] [-v] [-V]
```

選項

下列是必要選項：

選項	描述
-D <i>login</i>	頂層管理員的使用者 ID。
-l <i>login</i>	您要授予社團組織管理員權限的使用者之使用者 ID。使用者應該存在目錄中，而且是 -d 選項所指定網域的一部分。
-n <i>domain</i>	頂層管理員的網域。如果未指定，會使用儲存在 <code>cli-userprefs.properties</code> 檔案中的預設網域。
-w <i>password</i>	頂層管理員的密碼。
-d <i>domain</i>	您要授予管理員權限的網域。如果未指定，會使用 -n 選項指定的網域。

下列是非必要選項：

選項	描述
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從命令行。
-p <i>IS Port</i>	使用此選項指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> 。
-h, -?	列印指令用途語法。
-V	列印公用程式及其版本的相關資訊。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啟動除錯輸出。

範例

下列授予「社團組織管理員」權限給使用者 ID 為 admin1 的使用者。

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

下列授予「社團組織管理員」權限給網域 florizel.com 中使用者 ID 為 admin2 的使用者。

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

commadmin admin remove

commadmin admin remove 指令可移除現有「社團組織管理員」的「社團組織管理員」權限。只有「頂層管理員」可以執行這個指令。

如果要移除多個使用者的「社團組織管理員」權限，請使用 -i 選項。

語法

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

選項

下列是必要選項：

選項	描述
-D <i>login</i>	頂層管理員的使用者 ID。
-l <i>login</i>	需要撤銷其管理員權限的使用者之使用者 ID。
-n <i>domain</i>	頂層管理員的網域。
-w <i>password</i>	頂層管理員的密碼。
-d <i>domain name</i>	要撤銷其管理員權限的網域。如果未指定 -d，會使用 -n 指定的網域。

下列是非必要選項：

選項	描述
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS Port</i>	使用此選項指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager 。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。

範例

下列指令可移除使用者 ID 為 admin5 的管理員的「社團組織管理員」權限：

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

commadmin admin search

commadmin admin search 指令可搜尋和顯示網域的特定或所有「社團組織管理員」。

語法

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

選項

下列是必要選項：

選項	描述
-D <i>login</i>	有權限執行這個指令的使用者之使用者 ID。
-n <i>domain</i>	以 -D 選項指定的使用者之網域。
-w <i>password</i>	以 -D 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-l <i>login</i>	搜尋的「社團組織管理員」的使用者 ID。如果未指定 -l，或 -l 是以萬用字元運算子 (-l * 或 -l '*') 指定的，則會顯示網域的所有「社團組織管理員」。
-d <i>domain</i>	搜尋擁有特定網域的「社團組織管理員」權限的使用者。如果未指定 -d，會使用 -n 指定的網域。

範例

如果要搜尋 test.com 網域的所有「社團組織管理員」：

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

commadmin domain create

commadmin domain create 指令可在 Access Manager 上建立單一網域。如果要建立多個網域，請使用 -i 選項。

語法

```

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

```

選項

下列是必要選項：

選項	描述
-D <i>login</i>	頂層管理員的使用者 ID。
-d <i>domain name</i>	要建立的網域的 DNS 網域名稱。
-n <i>domain</i>	頂層管理員的網域。
-w <i>password</i>	頂層管理員的密碼。

下列是非必要選項：

選項	描述
-A [+] <i>attributename:value</i>	要修改的屬性。 <i>attributename</i> 定義在 LDAP Schema 中，而且指定的 <i>value</i> 會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。 <i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。 如果未指定動作值 (+)，預設動作是新增現有值。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-o <i>organization RDN</i>	指定網域的社團組織 RDN。例如 <code>o=varrius.florizel.com</code> 。 如果未指定此選項，社團組織會建立在 <code>osi suffix</code> 下，顯示為 <code>o= 網域名稱 (o=osiSuffix)</code>

選項	描述
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-x <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。
-S <i>service</i>	<p>指定要新增至網域的一或多個服務。</p> <p><i>service</i> 可擁有單一服務或多個服務的值。有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。</p> <p>如果指定 -S mail 選項，則必須指定 -H 選項。</p> <p>可用逗號分隔清單的方式列出。</p> <p>例如：</p> <pre>-S mail,cal</pre> <p>將使用 Identity Sever 配置檔案中存在的特定服務定義的值所提及的服務建立網域。</p>
如果指定 -S mail 選項，則只允許下列選項：	
-H <i>preferred mailhost</i>	<p>喜好的網域郵件主機。主機必須是完全合格的主機名稱，例如 mailhost.sesta.com。</p> <p>如果指定 -S mail 選項，則此選項是必要的。</p>
如果指定 -S cal 選項，則只允許下列選項：	
-B <i>backend calendar data server</i>	指定預設的後端主機以指定給網域中的使用者或資源。
-C <i>searchable domains</i>	指定尋找行事曆或使用者時所要搜尋的網域。
-g <i>access control string</i>	為新建的使用者行事曆指定「存取控制清單」(ACL)。
-P <i>propertyname[:value]</i>	為多重值與位元導向的屬性設定值。請參閱表 B-1 (在第 141 頁) 以取得屬性、描述與值。
-R <i>right[:value]</i>	設定行事曆網域屬性 icsAllowRights。屬性含有一個點陣圖值。請參閱表 B-2 (在第 142 頁) 以取得屬性、值及描述的清單。

選項	描述
<code>-T calendar time zone string</code>	指定匯入檔案時所使用的時區 ID。 請參閱「 行事曆時區字串 」(在第 143 頁)以取得有效的時區字串的清單。

範例

如果要建立含有郵件與行事曆服務的新網域，請輸入：

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

commadmin domain delete

`commadmin domain delete` 指令可將單一託管網域標示為從伺服器刪除。如果要將多個託管網域標示為刪除，請使用 `-i` 選項。

`commadmin domain purge` 指令將永久移除網域。

若要使社團組織管理員停用例如行事曆服務或郵件服務，請使用 `-s` 選項。這裡的 `s` 是以大寫表示。

語法

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

選項

下列是必要選項：

選項	描述
<code>-D login</code>	頂層管理員的使用者 ID。
<code>-d domain name</code>	正在刪除的 DNS 網域名稱。如果未指定 <code>-d</code> ，會使用 <code>-n</code> 指定的網域。
<code>-n domain</code>	頂層管理員的網域。

選項	描述
<code>-w password</code>	頂層管理員的密碼。

下列是非必要選項：

選項	描述
<code>-h, -?</code>	列印指令用途語法。
<code>-i inputfile</code>	從檔案讀取指令資訊，而不是從命令行。
<code>-p IS Port</code>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果在安裝過程未配置預設值，則使用連接埠 80。
<code>-s</code>	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
<code>-S service</code>	將指定的服務狀態屬性值修改為「deleted」。 以逗號分隔多個服務。有效的 <i>service</i> 值是 <i>mail</i> 與 <i>cal</i> 。這些值不區分大小寫。
<code>-v</code>	啓動除錯輸出。
<code>-V</code>	列印公用程式及其版本的相關資訊。
<code>-X IS Host</code>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <i>localhost</i> 。

範例

若要刪除現有網域：

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

若只要刪除 *florizel.com* 網域中的郵件服務：

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

commadmin domain modify

commadmin domain modify 指令可修改單一網域目錄項目的屬性。如果要修改多個網域，請使用 -i 選項。

語法

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

選項

下列是必要選項：

選項	描述
-D <i>login</i>	頂層管理員的使用者 ID。
-d <i>domain</i>	要修改的 DNS 網域名稱。如果未指定 -d，會使用 -n 指定的網域。
-n <i>domain</i>	頂層管理員的網域。
-w <i>password</i>	頂層管理員的密碼。

下列是非必要選項：

選項	描述
-A [+ -] <i>attributename:value</i>	<p>要修改的屬性。<i>attributename</i> 定義在 LDAP Schema 中，而且值會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。</p> <p><i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。「-」表示移除值。</p> <p>在指令行中指定指令時，如果使用「-」，它的前面必須是兩個反斜線。如果是在輸入檔中提供選項，「-」符號前面必須有一個反斜線。</p> <p>如果未指定動作值 (+ 或 -)，預設動作是取代現有值。</p>
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <i>localhost</i> 。
-S <i>service</i>	<p>在修改過程中，將一或多個指定的服務新增到網域。</p> <p>有效的 <i>service</i> 值是 <i>mail</i> 與 <i>cal</i>。這些值不區分大小寫。</p> <p>使用 -S 選項列出的服務會以逗號分隔。</p> <p>如果指定 -S <i>mail</i> 選項，必須指定 -H 選項。</p>
新增服務時，如果指定 -S <i>mail</i> 選項，則只允許下列選項：	
-H <i>preferred mailhost</i>	<p>喜好的網域郵件主機。</p> <p>如果指定 -S <i>mail</i> 選項，則此選項是必要的。</p>
新增服務時，如果指定 -S <i>cal</i> 選項，則只允許下列選項：	
-B <i>backend calendar data server</i>	指定給網域中使用者或資源的預設後端主機。
-C <i>cross domain search domains</i>	指定尋找行事曆或使用者時所要搜尋的網域。
-g <i>access string</i>	為新建的使用者行事曆指定「存取控制清單」(ACL)。

選項	描述
-P <i>[action]propertyname[:value]</i>	為多重值與位元導向的屬性設定值。請參閱表 B-1 (在第 141 頁) 以取得 <i>propertyname</i> 的描述與值。
-T <i>calendar time zone string</i>	匯入檔案時所使用的時區 ID。 請參閱「行事曆時區字串」(在第 143 頁) 以取得有效的時區字串的清單。
-R <i>propertyname[:value]</i>	設定行事曆網域屬性 <i>icsAllowRights</i> 。屬性含有一個點陣圖值。請參閱表 B-2 (在第 142 頁) 以取得特性名稱、值及描述的清單。

範例

若要修改現有網域：

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

commadmin domain purge

`commadmin domain purge` 指令可永久移除標示為刪除的所有項目或項目服務。這包含網域、使用者、群組以及資源。如果網域標示為刪除，則無論該網域中的所有項目與服務是否標示為刪除，一律都會被移除。

做為定期維護作業的一部分，請使用 `commadmin domain purge` 指令移除刪除週期已超過指定寬限期的所有項目。

您可以隨時手動呼叫指令來執行清除。

當您呼叫指令時，會搜尋目錄並建立一個網域清單，其中的項目包含標示為刪除週期超過指定寬限期的網域。寬限期的預設值在最初安裝時設為 10 天。

如果指定 `-d*` 選項，會搜尋使用者的所有網域及標示為刪除的網域。標示為刪除的使用者將自其網域中移除，但除非網域也標示為刪除，否則將不會被清除。如果網域標示為刪除，連同該網域中的所有使用者將一併被清除。

在服務標示為刪除之後，必須先執行移除資源（例如電子信箱或行事曆）的公用程式，才能從目錄中清除服務。對於郵件服務，此程式的名稱是 `msuserpurge`。請參閱「Sun Java System Messaging Server Administration Reference」以取得關於 `msuserpurge` 公用程式的資訊。對於行事曆服務，此程式的名稱是 `csclean`。請參閱「Sun Java System Calendar Server 管理指南」以取得關於 `csclean` 公用程式的資訊。

備註 `commadmin domain purge` 指令必須由頂層管理員執行。

語法

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

選項

下列是必要選項：

選項	描述
<code>-D login</code>	頂層管理員的使用者 ID。
<code>-n domain</code>	頂層管理員的網域。
<code>-w password</code>	頂層管理員的密碼。
<code>-d domain</code>	清除指定的網域。* 運算子 (<code>-d*</code>) 可用來搜尋式樣。

下列是非必要選項：

選項	描述
<code>-g grace</code>	清除網域之前的寬限期（天）。網域標示為刪除的時間若少於 <code>grace</code> 天，將不會被清除。0 表示立即清除。預設值是從伺服器上的配置檔案中讀取的。安裝時，預設值設為 10 天。
<code>-h, -?</code>	列印指令用途語法。
<code>-i inputfile</code>	從檔案讀取指令資訊，而不是從指令行。
<code>-p IS Port</code>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <code>IS Port</code> ，或者如果安裝時未配置預設值，則使用連接埠 80。

選項	描述
-S <i>service</i>	從網域中移除服務相關的物件類別與屬性。如果網域包含使用者與資源，則它會從目錄中移除這些使用者和資源的服務特定資料。 服務清單是以逗號 (,) 分割元做分隔。 有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。
-s	使用 SSL (Secure Socket Layer, 安全套接層) 連線至 Access Manager。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。

範例

在下列範例中，siroe.com 網域會被清除，同時也會移除該網域中的所有項目：

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

commadmin domain search

commadmin domain search 指令可取得與單一網域相關的所有目錄特性。如果要取得多個網域的所有目錄特性，請使用 -i 選項。當這個指令中指定 -s 時，只會顯示具有使用中的指定服務的網域。

語法

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

選項

下列是必要選項：

選項	描述
-d <i>login</i>	有權限執行這個指令的使用者之使用者 ID。
-n <i>domain</i>	以 -D 選項指定的使用者之網域。
-w <i>password</i>	以 -D 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-d <i>domain</i>	搜尋此網域。如果未指定 -d，或已指定 -d*，會顯示所有網域。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-S <i>service</i>	<p>指定要在使用中的網域搜尋的服務。</p> <p><i>service</i> 可擁有單一服務或多個服務的值。有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。</p> <p>服務清單是以逗號 (,) 分割元做分隔。</p> <p>例如：</p> <p>-S mail,cal</p>
-t <i>Search template</i>	指定要使用的搜尋範本名稱來取代預設的搜尋範本。在搜尋之後只會顯示使用中的網域。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。

commadmin group create

`commadmin group create` 指令可在 Access Manager 新增單一群組。如果要建立多個群組，請使用 `-i` 選項。

如果建立不含任何成員的群組，依照預設，其為靜態群組。

注意 群組不能同時包含靜態與動態成員。

電子郵件發行清單是一種類型的群組。當訊息傳送至群組位址時，Access Manager 會將訊息傳送至群組中的所有成員。

語法

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

選項

下列是必要選項：

選項	描述
<code>-D login</code>	有權限執行這個指令的使用者之使用者 ID。
<code>-n domain</code>	以 <code>-D</code> 選項指定的使用者之網域。
<code>-G groupname</code>	群組的名稱 (例如 <code>mktg-list</code>)。
<code>-w password</code>	以 <code>-D</code> 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-A [+] <i>attributename:value</i>	要修改的屬性。 <i>attributename</i> 定義在 LDAP Schema 中，而且 <i>value</i> 會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。 <i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。
-d <i>domain</i>	完全合格的群組網域名稱 (例如 varrius.com)。預設值是本機網域。如果未指定 -d，會使用 -n 指定的網域。
-f <i>ldap-filter</i>	建立動態群組。 指定屬性或屬性組合來設定 LDAP 篩選器。 您可以指定多個 -f 指令來對群組成員定義許多 LDAP 篩選器。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-m <i>internal -member</i>	新增至此群組的內部成員的使用者 ID。如果要新增一個以上的成員，請使用多個 -m 選項。 應使用此選項來建立靜態群組。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-S <i>service</i>	指定要新增至「群組」的服務。 <i>service</i> 可擁有單一服務或多個服務的值。有效的服務值是 mail 與 cal。這些值不區分大小寫。 服務清單是以逗號 (,) 分割元做分隔。 例如： -S mail,cal

如果指定 -S mail 選項，則只允許下列選項：

選項	描述
-H <i>mailhost</i>	此群組回應的郵件主機 (例如 <code>mailhost.varrius.com</code>)。預設值是本機郵件主機。
-E <i>email</i>	群組的電子郵件地址。
-M <i>external-member</i>	新增至此群組的外部成員的使用者 ID。如果要新增一個以上的成員，請使用多個 -M 選項。
-o <i>owner</i>	群組所有者的電子郵件地址。所有者是對通訊群組清單負責的個人。 所有者可以新增或刪除通訊群組清單成員。
-r <i>moderator</i>	管理者電子郵件地址。

範例

如果要在 `sesta.com` 網域中建立 `testgroup` 群組：

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

commadmin group delete

`commadmin group delete` 指令可將單一群組標示為刪除。如果要將多個群組標示為刪除，請使用 -i 選項。

如果要使群組停用服務 (例如 Calendar Server 或 Messaging Server)，請使用 -s 選項。這裡的 s 是以大寫表示。

備註 爲了永久移除群組，您必須執行 `commadmin domain purge` 指令。

語法

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

選項

下列是必要選項：

選項	描述
-D <i>login</i>	有權限執行這個指令的使用者之使用者 ID。
-G <i>groupname</i>	要標示為刪除的群組之名稱。例如 <code>mktg-list</code> 。
-n <i>domain</i>	以 -D 選項指定的使用者之網域。
-w <i>password</i>	以 -D 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-d <i>domain</i>	群組的網域。如果未指定 -d，會使用 -n 選項指定的網域。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-S <i>service</i>	將指定的服務狀態屬性值修改為「deleted」。
	使用 -S 選項列出的服務會以逗號分隔。有效的 <i>service</i> 值是 <code>mail</code> 與 <code>cal</code> 。這些值不區分大小寫。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。

選項	描述
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。

範例

若要將群組 testgroup@varrius.com 標示為刪除：

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

下列範例會將 testgroup@varrius.com 的郵件服務標示為刪除：

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

commadmin group modify

commadmin group modify 指令可以變更已經存在於 Access Manager 中的單一群組之屬性。如果要變更多個群組的屬性，請使用 -i 選項。

電子郵件清單是一種類型的群組。當訊息傳送至群組位址時，Access Manager 會將訊息傳送至群組中的所有成員。

語法

```

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

```

選項

下列是必要選項：

選項	描述
-D <i>login</i>	有權限執行這個指令的使用者之使用者 ID。
-G <i>groupname</i>	要修改的群組之名稱。例如 <code>mktg-list</code> 。
-n <i>domain</i>	以 -D 選項指定的使用者之網域。
-w <i>password</i>	以 -D 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-A [+ -] <i>attributename:value</i>	<p>要修改的屬性。<i>attributename</i> 定義在 LDAP Schema 中，而且值會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。</p> <p><i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。「-」表示移除值。在指令行中指定指令時，如果使用「-」，它的前面必須是兩個反斜線。如果是在輸入檔中提供選項，「-」符號前面必須有一個反斜線。</p>
-d <i>domain</i>	群組的網域。如果未指定 -d，會使用 -n 選項指定的網域。
-f [<i>action</i>] <i>ldap-filter</i>	<p>指出 ldap 篩選器是否已新增到群組或已自群組中移除。</p> <p><i>ldap-filter</i> 之前的「+」表示它將要新增至現有的篩選器。「-」表示移除現有的篩選器。輸入 -f-* 移除所有篩選器。在指令行中指定指令時，如果使用「-」，它的前面必須是兩個反斜線或為其加上引號。</p> <p>如果未指定 <i>action</i>，依照預設，如果篩選器不存在的話，會新增篩選器。否則會出現一個錯誤訊息。</p>

選項	描述
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-m [<i>action</i>] <i>internal-member</i>	指出是否要新增或移除內部成員。 <i>internal-member</i> 的值不是郵件地址就是使用者 ID。 以下的 <i>action</i> 值中： + 會將成員新增到現有的內部成員清單。 - 會將成員從現有的內部成員清單中移除。在指令行中指定指令時，如果使用「-」，它的前面必須是兩個反斜線或對其加上引號。 -m-* 可移除所有內部成員。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <i>localhost</i> 。
-S <i>mail</i>	驗證郵件服務是否存在之後，會在修改時將郵件服務新增到群組。如果服務存在，會出現一個錯誤訊息。 -S 唯一的有效值是 <i>mail</i> 。
如果指定 -S <i>mail</i> 選項，則只允許下列選項：	
-o <i>owner</i>	群組所有者的電子郵件地址。所有者是對通訊群組清單負責的個人。 所有者可以新增或刪除通訊群組清單成員。
-E <i>email</i>	群組的電子郵件地址。
-H <i>mailhost</i>	群組的郵件主機。預設值是本機郵件主機。
-M <i>external-member</i>	新增外部成員。 <i>external-member</i> 的值是使用者電子郵件地址。

選項	描述
-r <i>moderator</i>	管理者的使用者 ID。如果管理者在不同的網域中，請輸入電子郵件地址。 必須使用此選項指定 -S mail 選項。

範例

如果要移除 varrius.com 網域中 testgroup 群組的內部成員 (jsmith)：

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

commadmin group search

commadmin group search 指令可取得與單一群組相關的所有目錄特性。如果要取得多個群組的所有目錄特性，請使用 -i 選項。

語法

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

選項

下列是必要選項：

選項	描述
-D <i>login</i>	有權限執行這個指令的使用者之使用者 ID。
-n <i>domain</i>	以 -D 選項指定的使用者之網域。
-w <i>password</i>	以 -D 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-d <i>domain</i>	要搜尋的群組之網域。如果未指定 -d，會搜尋所有網域。
-E <i>string</i>	群組的電子郵件地址。字串中的任一部分可使用萬用字元運算子 (*)。
-G <i>string</i>	要搜尋的群組之名稱。例如 <code>marketing-list</code> 。如果未指定 -G，會顯示 -d 指定之網域中的所有群組。字串中的任一部分可使用萬用字元運算子 (*)。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS Port</i>	指定 IS 伺服器正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-S <i>service</i>	指定要搜尋的服務。 <i>service</i> 唯一的有效值是 <code>mail</code> 。該值不區分大小寫。 例如： -S mail 只會顯示具有使用中的服務的群組。
-t <i>Search Template</i>	指定要使用的搜尋範本名稱來取代預設的搜尋範本。這是目錄中的一個項目，可定義篩選器來搜尋。只會搜尋使用中的群組。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <code>localhost</code> 。

範例

如果要搜尋 `siroe.com` 網域下名為 `developers` 的群組：

```
commadmin group search -D chris -n sesta.com -w password -G
developers \
-d siroe.com
```

commadmin resource create

`commadmin resource create` 指令可為資源建立目錄項目。

如需有關建立資源的說明，請參閱「[建立資源](#)」。

語法

```
commadmin resource create -D login -n domain -w password -u identifier -N
name
-o owner [-A [+]attributename:value] [-c calendar identifier] [-C DWPHost]
[-d domainname] [-h] [-?] [-i inputfile] [-p IS Port] [-s] [-T time zone]
[-v]
[-V] [-X IS Host]
```

選項

下列是必要選項：

選項	描述
<code>-D login</code>	有權限執行這個指令的使用者之使用者 ID。
<code>-n domain</code>	以 <code>-D</code> 選項指定的使用者之網域。
<code>-w password</code>	以 <code>-D</code> 選項指定的使用者之密碼。
<code>-u identifier</code>	資源的唯一識別碼。 這個 <code>identifier</code> 值在網域名稱空間中或行事曆以行事曆模式管理的所有使用者及資源中應該是唯一的。 如果未指定 <code>-c</code> 選項，會使用 <code>-u</code> 選項指定的識別碼做為行事曆識別碼。
<code>-N name</code>	在行事曆 GUI 中用來顯示資源的易記名稱。
<code>-o owner</code>	資源的所有者。這個使用者 ID 必須存在於建立資源的網域下。

下列是非必要選項：

選項	描述
-A [+] <i>attributename:value</i>	要修改的屬性。 <i>attributename</i> 定義在 LDAP Schema 中，而且 <i>value</i> 會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。 <i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。
-c <i>calendar identifier</i>	此資源行事曆的識別碼。 這個識別碼值在 Calendar Server 管理的所有行事曆當中應該是唯一的。
-C <i>DWPHost</i>	代管使用者行事曆的後端 Calendar Server 之 DNS 名稱。 如果未指定後端 Calendar Server 之 DNS 名稱，會使用儲存在伺服器中的 <i>ics.conf</i> 檔案中的值做為預設值。
-d <i>domain name</i>	資源的網域。如果未指定 -d，會使用 -n 指定的網域。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-T <i>time zone</i>	在行事曆的使用者介面中，用來顯示資源行事曆的時區。 請參閱「行事曆時區字串」(在第 143 頁)以取得有效的時區字串的清單。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <i>localhost</i> 。

範例

如果要在網域下的行事曆 cal.siroe.com 中建立名稱爲 peter 的資源：

```
comadmin resource create -D chris -n sesta.com -w bolton -o
ownerid \
-d varrius.com -u id -N peter -C cal.siroe.com
```

建立資源

資源包含兩種資料描述：Calendar Server 資料庫中的目錄項目和行事曆。目錄項目具有一種屬性 icsCalendar，其值爲資源相關的行事曆之名稱。

您可以使用下列一種方法，建立具有兩種資料描述的資源：

- 使用 csresource 公用程式，可建立一個目錄項目和一個行事曆。

請注意下列事項：

- 您必須在 csresource 中指定和 comadmin resource create 中相同的所有者。所有者是以兩種指令中的 -o 選項指定的。
- 資源名稱的值 (在 csresource 中的 create 指令後) 必須和 comadmin resource create 中 -u 選項使用的值相同。
- 使用 comadmin resource create 可建立目錄項目，而使用 cscal 公用程式可建立行事曆。例如：

- a. 使用 comadmin resource create 可建立目錄項目：

```
comadmin resource create -D amadmin -w ampassword -n
blink.sesta.com \
-X blink -p 5555 -d varrius.com -o test1 -u resourceOne -N
firstResource
```

目錄項目列示如下：

```
dn:uid=resourceONE,ou=People,o=varrius,o=domainroot
uid:resrouceONE
objectClass:icsCalendarResource
objectClass:top
cn:firstResource
icsStatus:active
icsCalendar:test1@varrius.com:resourceOne
```

b. 使用 `cscal` 可建立行事曆：

```
cscal -D varrius.com -o test1 -n firstResource create resourceOne
```

`cscal` 清單中的行事曆描述為：

```
test1@varrius.com:resourceOne:owner=test1@varrius.com
status=enabled
```

您現在可使用任何使用者的身份登入，並邀請資源加入事件。

請參閱「Sun Java System Calendar Server 管理指南」中的「Calendar Server 指令行公用程式」以取得 `csresource` 與 `cscal` 公用程式的詳細描述。

commadmin resource delete

`commadmin resource delete` 指令可將資源標示為刪除。

備註 如果要永久移除資源，請執行 `commadmin domain purge` 指令。

語法

```
commadmin resource delete -D login -u identifier -n domain -w password [-d
domainname]
[-h] [-?] [-i inputfile] [-p IS Port] [-s] [-v] [-V] [-X IS Host]
```

選項

下列是必要選項：

選項	描述
<code>-D login</code>	有權限執行這個指令的使用者之使用者 ID。
<code>-n domain</code>	以 <code>-D</code> 選項指定的使用者之網域。
<code>-w password</code>	以 <code>-D</code> 選項指定的使用者之密碼。
<code>-u identifier</code>	資源的唯一識別碼。

下列是非必要選項：

選項	描述
-d <i>domainname</i>	資源的網域。如果未指定 -d，會使用 -n 指定的網域。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。

範例

如果要將資源標示為刪除：

```
commadmin resource delete -D chris -n sesta.com -w bolton -u
bill1023
```

commadmin resource modify

commadmin resource modify 指令可修改資源。

語法

```
commadmin resource modify -D login -n domain -w password -u identifier
[-A [+|-]attributename:value] [-d domainname] [-h] [-?] [-i inputfile]
[-N name] [-p IS Port] [-s] [-T time zone] [-v] [-V] [-X IS Host]
```

選項

下列是必要選項：

選項	描述
-D <i>login</i>	有權限執行這個指令的使用者之使用者 ID。
-n <i>domain</i>	以 -D 選項指定的使用者之網域。
-w <i>password</i>	以 -D 選項指定的使用者之密碼。
-u <i>identifier</i>	資源的唯一識別碼。

下列是非必要選項：

選項	描述
-A [+ -] <i>attributename:value</i>	要修改的屬性。 <i>attributename</i> 定義在 LDAP Schema 中，而且值會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。 <i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。「-」表示移除值。 在指令行中指定指令時，如果使用「-」，它的前面必須是兩個反斜線。如果是在輸入檔中提供選項，「-」符號前面必須有一個反斜線。
-d <i>domainname</i>	資源的網域。如果未指定 -d，會使用 -n 指定的網域。
-h, -?	列印指令用途語法。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-N <i>name</i>	在行事曆使用者介面中用來顯示資源的一般名稱。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer, 安全套接層) 連線至 Access Manager。

選項	描述
-T <i>time zone</i>	在行事曆 GUI 中，用來顯示資源行事曆的時區。 請參閱「 行事曆時區字串 」(在第 143 頁)以取得有效的時區字串的清單。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <i>localhost</i> 。

範例

如果要以新的一般名稱 *bjones* 修改唯一識別碼為 *bill023* 的資源：

```
commadmin resource modify -D chris -n sesta.com -w bolton -d
test.com \
-u bill023 -N bjones
```

commadmin resource search

`commadmin resource search` 指令可搜尋資源。

語法

```
commadmin resource search -D login -n domain -w password [-d domain]
[-h] [-?]
[-i inputfile] [-N string] [-p IS Port] [-s] [-t Search Template] [-u string]
[-V] [-v]
[-X IS Host]
```

選項

下列是必要選項：

選項	描述
-D <i>login</i>	有權限執行這個指令的使用者之使用者 ID。

選項	描述
<code>-n domain</code>	以 <code>-D</code> 選項指定的使用者之網域。
<code>-w password</code>	以 <code>-D</code> 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
<code>-d domain</code>	資源的網域。搜尋只能在網域中執行。如果未指定 <code>-d</code> ，或已指定 <code>-d*</code> ，會搜尋所有網域。
<code>-h, -?</code>	列印指令用途語法。
<code>-i inputfile</code>	從檔案讀取指令資訊，而不是從指令行。
<code>-N string</code>	輸入資源的一般名稱。字串中的任一部分可使用萬用字元運算子 (*)。
<code>-p IS Port</code>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
<code>-s</code>	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
<code>-t Search Template</code>	指定要使用的搜尋範本名稱來取代預設的搜尋範本。這是目錄中的一個項目，可定義篩選器來搜尋。只會搜尋使用中的資源。
<code>-u string</code>	指定的資源識別碼對網域名稱空間或行事曆所管理的所有使用者與資源而言，必須是唯一的。 字串中的任一部分可使用萬用字元運算子 (*)。 如果未指定識別碼或已指定 <code>-l*</code> ，會在搜尋時顯示所有資源。
<code>-v</code>	啓動除錯輸出。
<code>-V</code>	列印公用程式及其版本的相關資訊。
<code>-X IS Host</code>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 <code>localhost</code> 。

範例

如果要在網域 `sesta.com` 中搜尋資源 `arabella`：

```
commadmin resource search -D serviceadmin -w serviceadmin -n
sesta.com \
-d sesta.com -u arabella
```

commadmin user create

`commadmin user create` 指令可在 Access Manager 系統上建立單一使用者。如果要建立多個使用者，請使用 `-i` 選項。

語法

```
commadmin user create -D login -F firstname -n domain -L lastname -l userid
-w password -W password [-A [+]attributename:value] [-d domain]
[-I initial] [-h] [-?] [-i inputfile] [-p IS Port] [-s] [-v] [-V] [-X IS
Host]
[-S mail [-E email] [-H mailhost]]
[-S cal [-B DWPHost] [-E email] [-k calid_type] [-J First Daylof Week]
[-T time zone]
```

選項

下列是必要選項：

選項	描述
<code>-D login</code>	有權限執行這個指令的使用者之使用者 ID。
<code>-F firstname</code>	使用者的名字，必須是不含空格的單字。
<code>-n domain</code>	以 <code>-D</code> 選項指定的使用者之網域。
<code>-l userid</code>	使用者的登入名稱。
<code>-w password</code>	以 <code>-D</code> 選項指定的使用者之密碼。
<code>-W password</code>	正在建立的使用者之密碼。
	您也可以透過文字檔 <code>password.txt</code> 指定密碼。
<code>-L lastname</code>	使用者的姓氏。

下列是非必要選項：

選項	描述
-A [+] <i>attributename:value</i>	要修改的屬性。 <i>attributename</i> 定義在 LDAP Schema 中，而且 <i>value</i> 會取代目錄中這個屬性的所有目前值。重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。 <i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。
-d <i>domain</i>	使用者的網域。如果未指定 -d，會使用 -n 指定的網域。
-i <i>inputfile</i>	從檔案讀取指令資訊，而不是從指令行。
-I <i>initial</i>	使用者的中間名縮寫。
-h, -?	列印指令用途語法。
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。
-S <i>service</i>	在建立過程中，將指定的服務新增至使用者。 <i>service</i> 可擁有單一服務或多個服務的值。有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。 服務清單是以逗號 (,) 分割元做分隔。 例如： -S mail,cal
如果指定 -S mail 選項，則只允許下列選項：	
-E <i>email</i>	使用者的電子郵件地址。
-H <i>mailhost</i>	使用者的郵件主機。
如果指定 -S cal 選項，則只允許下列選項：	
-B <i>DWPHost</i>	代管使用者行事曆的後端行事曆之 DNS 名稱。
-E <i>email</i>	行事曆使用者的電子郵件地址。
-J <i>First Day of Week</i>	行事曆顯示在 Calendar Server 使用者介面時，所顯示星期的第一天。有效值為 0-6 (0 是星期天、1 是星期一等)。

選項	描述
<code>-k calid_type</code>	<p>指定建立的行事曆 ID 類型。接受的值為 <code>legacy</code> 與 <code>hosted</code>。如果指定 <code>-k legacy</code>，只會使用行事曆 ID (例如 <code>jsmith</code>)。如果指定 <code>-k hosted</code>，會使用行事曆 ID 加上網域 (例如 <code>jsmith@sesta.com</code>)。</p> <p>如果未指定 <code>-k</code> 選項，預設值是使用行事曆 ID 加上網域 (<code>hosted</code>)。</p> <p>如果未指定 <code>-k</code> 選項，您可以設定建立的行事曆 ID 類型的值。如果要執行這項操作，請將下列參數新增到 <code>resource.properties</code> 檔案：</p> <pre>switch-catype=<i>value</i></pre> <p>其中，<code>value</code> 是 <code>"hosted" "legacy"</code>。</p> <p><code>resource.properties</code> 檔案位於下列目錄：</p> <pre>da_base/data/WEB-INF/classes/sun/comm/cli/server/se rvlet/ resource.properties</pre>
<code>-T time zone</code>	<p>顯示使用者行事曆的時區。</p> <p>請參閱「行事曆時區字串」(在第 143 頁)以取得有效的時區字串的清單。</p>

範例

如果要建立新使用者 `smith`，請輸入：

```
commadmin user create -D chris -n sesta.com -w secret -F smith -l
john \
-L major -W secret -S mail -H mailhost.siroe.com
```

commadmin user delete

`commadmin user delete` 指令可將單一使用者標示為刪除。如果要將多個使用者標示為刪除，請使用 `-i` 選項。

沒有取消刪除的公用程式。不過，您可以使用 `ldapmodify` 指令，在清除寬限期過期之前與將清除設為針對項目執行之前，隨時將使用者項目的狀態屬性變更為 `active`。

移除使用者的程序包含下列三個步驟：

1. 透過執行 `commadmin user delete` 指令，將使用者標示為刪除。
2. 移除使用者中的資源。

資源可以是電子郵件信箱或行事曆。對於郵件服務，此程式的名稱是 `msuserpurge`。請參閱「Sun Java System Messaging Server Administration Reference」以取得關於 `msuserpurge` 公用程式的資訊。對於行事曆服務，此程式的名稱是 `csclean`。請參閱「Sun Java System Calendar Server 管理指南」以取得關於 `csclean` 公用程式的資訊。

3. 呼叫 `commadmin domain purge` 指令可永久移除使用者。

語法

```
commadmin user delete -D login -n domain -l login name -w password [-d
domain]
[-h] [-?] [-i inputfile] [-p IS Port] [-s] [-S service] [-v] [-V] [-X IS
Host]
```

選項

下列是必要選項：

選項	描述
<code>-D login</code>	有權限執行這個指令的使用者之使用者 ID。
<code>-n domain</code>	以 <code>-D</code> 選項指定的使用者之網域。
<code>-w password</code>	以 <code>-D</code> 選項指定的使用者之密碼。
<code>-l userid</code>	要刪除的使用者之使用者 ID。

下列是非必要選項：

選項	描述
<code>-d domain</code>	使用者的網域。如果未指定 <code>-d</code> ，會使用 <code>-n</code> 指定的網域。
<code>-h, -?</code>	列印指令用途語法。
<code>-i inputfile</code>	從檔案讀取指令資訊，而不是從指令行。

選項	描述
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-S <i>service</i>	<p>指定要從使用者移除的服務。使用者仍保持為使用中，但只有指定的服務是停用中。如果未指定 -S，會刪除使用者。</p> <p><i>service</i> 可擁有單一服務或多個服務的值。有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。</p> <p>服務清單是以逗號 (,) 分割元做分隔。</p> <p>例如：</p> <p>-S mail,cal</p>
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。

範例

如果要將現有使用者標示為刪除：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith
```

如果只要從使用者 smith 刪除郵件服務：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail
```

commadmin user modify

commadmin user modify 指令可修改單一使用者目錄項目的屬性。如果要修改多個使用者，請使用 -i 選項。

語法

```

commadmin user modify -D login -n domain -l userid -w password
[-A [+|-]attributename:value] [-d domain] [-h] [-?][-i inputfile] [-p IS
Port] [-s]
[-v] [-V] [-X IS Host]
[-S mail -H mailhost [-E email]]
[-S cal [-B DWPHost] [-E email] [-k calid_type] [-J First Day of Week]
[-T time zone]]

```

選項

下列是必要選項：

選項	描述
-D login	有權限執行這個指令的使用者之使用者 ID。
-n domain	以 -D 選項指定的使用者之網域。
-w password	以 -D 選項指定的使用者之密碼。
-l userid	使用者的登入 ID。

下列是非必要選項：

選項	描述
-A [+ -]attributename:value	要修改的屬性。 <i>attributename</i> 定義在 LDAP Schema 中，而且值會取代目錄中這個屬性的所有目前值。您可以重複此選項以同時修改多個屬性，或為同一個屬性指定多個值。 <i>attributename</i> 之前的「+」，表示新增值到目前的屬性清單中。「-」表示移除值。 在指令行中指定指令時，如果使用「-」，它的前面必須是兩個反斜線。如果是在輸入檔中提供選項，「-」符號前面必須有一個反斜線。
-d domain	使用者或群組的網域。如果未指定 -d，會使用 -n 指定的網域。
-h, -?	列印指令用途語法。
-i inputfile	從檔案讀取指令資訊，而不是從指令行。

選項	描述
-p <i>IS Port</i>	指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-v	啟動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。
-S <i>service</i>	<p>在以 -S 選項驗證使用者是否擁有指定的服務之後，將指定的服務新增到使用者。如果使用者已擁有服務，會出現一個錯誤訊息。</p> <p><i>services</i> 可擁有單一服務或多個服務的值。有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。</p> <p>服務清單是以逗號 (,) 分割元做分隔。</p> <p>例如：</p> <p>-S mail,cal</p>
如果指定 -S mail 選項，則只允許下列選項：	
-E <i>email</i>	指定使用者的電子郵件地址。
-H <i>mailhost</i>	<p>使用者的郵件主機。</p> <p>如果指定 -S mail 選項，則此選項是必要的。</p>
如果指定 -S cal 選項，則只允許下列選項：	
-B <i>DWPHost</i>	<p>指定代管這個使用者行事曆的後端 Calendar Server 之 DNS 名稱。</p> <p>備註：如果這個屬性已經存在，則只能新增而不能修改該屬性。</p>
-E <i>email</i>	指定行事曆使用者的電子郵件地址。
-J <i>First Day of Week</i>	行事曆顯示在 Calendar Server 使用者介面時，所顯示星期的第一天。有效值為 0-6 (0 是星期天、1 是星期一等)。

選項	描述
-k <i>calid_type</i>	<p>指定建立的行事曆 ID 類型 (新增行事曆服務時)。接受的值為 legacy 與 hosted。如果指定 -k legacy，只會使用行事曆 ID (例如 jsmith)。如果指定 -k hosted，會使用行事曆 ID 加上網域 (例如 jsmith@sesta.com)。</p> <p>如果未指定 -k 選項，預設值是使用行事曆 ID 加上網域 (hosted)。</p> <p>如果未指定 -k 選項，您可以設定建立的行事曆 ID 類型的值。如果要執行這項操作，請將下列參數新增到 resource.properties 檔案：</p> <pre>switch-catype=<i>value</i></pre> <p>其中，<i>value</i> 是 "hosted" "legacy"。</p> <p>resource.properties 檔案位於下列目錄：</p> <pre>da_base/data/WEB-INF/classes/sun/comm/cli/server/se rvlet/ resource.properties</pre>
-T <i>time zone</i>	<p>使用者行事曆會顯示在此時區。</p> <p>請參閱「行事曆時區字串」(在第 143 頁)以取得有效的時區字串的清單。</p>

範例

下列範例中，為使用者 smith 新增郵件服務：

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A description:"new description" -S mail -H mailhost.siroe.com
```

在此範例中，為使用者 smith 新增了郵件轉寄地址。

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A +mailforwardingaddress:tsmith@siroe.com
```

commadmin user search

commadmin user search 指令可取得與單一使用者相關的所有目錄特性。如果要取得多個使用者的所有目錄特性，請使用 -i 選項。在搜尋之後只會顯示使用中的使用者。

語法

```
commadmin user search -D login -n domain -w password [-d domain] [-E string]
  [-F string] [-h] [-?] [-i inputfile] [-L string] [-l string] [-p IS Port]
  [-s]
  [-S service] [-t Search Template] [-v] [-V] [-X IS Host]
```

選項

下列是必要選項：

選項	描述
-D login	有權限執行這個指令的使用者之使用者 ID。
-n domain	以 -D 選項指定的使用者之網域。
-w password	以 -D 選項指定的使用者之密碼。

下列是非必要選項：

選項	描述
-d domain	使用者的網域。只在指定的網域中搜尋使用者。 如果未指定 -d，會搜尋所有網域。
-E string	搜尋使用者郵件地址。字串中的任一部分可使用萬用字元運算子 (*)。
-F string	搜尋使用者名字。字串中的任一部分可使用萬用字元運算子 (*)。
-h, -?	列印指令用途語法。
-i inputfile	從檔案讀取指令資訊，而不是從指令行。
-L string	搜尋使用者姓氏。字串中的任一部分可使用萬用字元運算子 (*)。

選項	描述
-l <i>string</i>	搜尋使用者的登入名稱。字串中的任一部分可使用萬用字元運算子 (*)。
-p <i>IS Port</i>	使用此選項指定 Access Manager 正在監聽的替代 TCP 連接埠。如果未指定，會使用預設的 <i>IS Port</i> ，或者如果安裝時未配置預設值，則使用連接埠 80。
-s	使用 SSL (Secure Socket Layer，安全套接層) 連線至 Access Manager。
-S <i>service</i>	指定與使用者搜尋相符的服務。 <i>services</i> 可擁有單一服務或多個服務的值。有效的 <i>service</i> 值是 mail 與 cal。這些值不區分大小寫。 服務清單是以逗號 (,) 分割元做分隔。 例如： -S mail,cal
-t <i>Search template</i>	指定要使用的搜尋範本名稱來取代預設的搜尋範本。這是目錄中的一個項目，可定義篩選器來搜尋。只會搜尋使用中的使用者。
-v	啓動除錯輸出。
-V	列印公用程式及其版本的相關資訊。
-X <i>IS Host</i>	指定正在執行 Access Manager 的主機。如果未指定，會使用預設的 <i>IS Host</i> ，或者如果安裝時未配置預設值，則使用 localhost。

範例

下列範例搜尋 varrius.com 網域中的使用者：

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

指令描述

服務提供者管理員及服務提供者社團組織

Delegated Administrator 主控台提供了能在目錄中建立之新的管理員角色，服務提供者管理員 (SPA)，以及新的社團組織類型。

本附錄描述下列主題：

- [服務提供者管理員](#)
- [服務提供者管理員所管理的社團組織](#)
- [建立提供者社團組織及服務提供者管理員](#)
- [範例服務提供者社團組織資料](#)

本附錄描述服務提供者管理員角色及新的社團組織類型，並且說明如何在 Delegated Administrator 中建立它們。

服務提供者管理員

Delegated Administrator 主控台讓您委託管理作業給新的服務提供者管理員 (SPA) 角色，這個角色能夠建立及管理下層社團組織的新類型。

SPA 的權限範圍介於頂層管理員 (TLA) 和社團組織管理員 (OA) 之間。

您可以使用 SPA 建立三層次的管理階層，如第 1 章「[Delegated Administrator 簡介](#)」中的「[三層次階層](#)」所述。

在委託給第二層級後，可減輕由大型 LDAP 目錄所支援的大型客戶基底的管理作業。例如，ISP 可能會提供服務給上百或上千個小型企業，而每一個都需要它們自己的社團組織。每一天可能都會有許多新的社團組織新增至目錄中。

如果您使用雙層次階層，TLA 必須建立所有這些新的社團組織。現在 TLA 可以委託這些作業給 SPA。

SPA 可以為新客戶建立下層社團組織，並指定 OA 來管理那些社團組織中的使用者。

圖 A-1 顯示一個三層次組織階層的邏輯檢視範例。

圖 A-1 使用服務提供者管理員之目錄：邏輯檢視

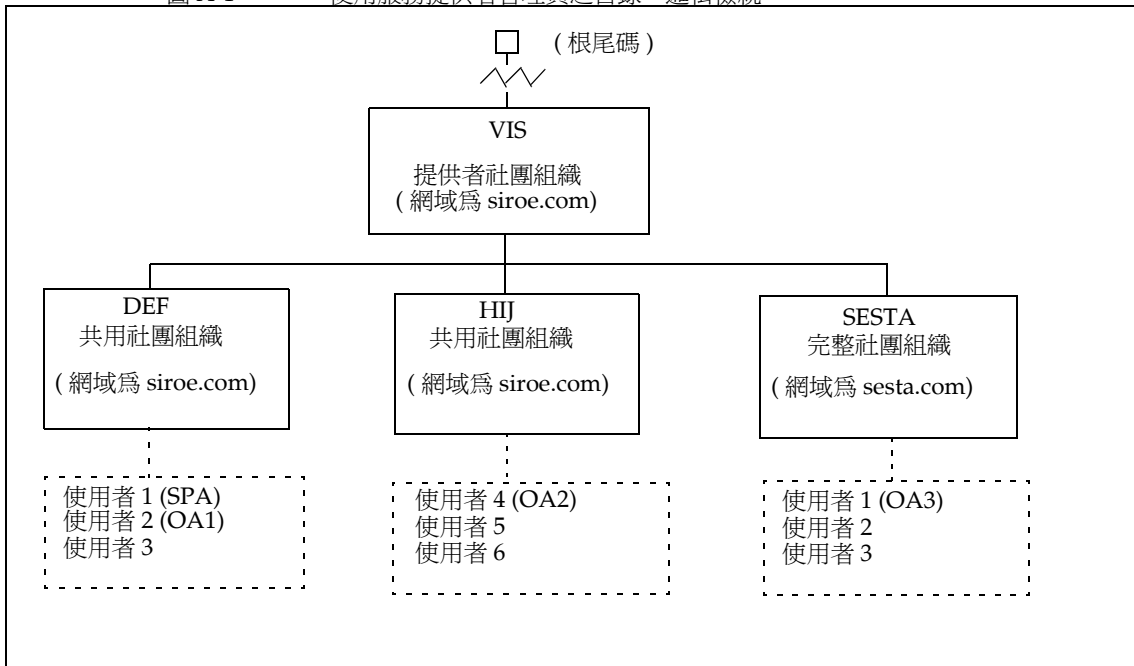


圖 A-1 中的範例顯示一個提供者社團組織。但是，一個目錄可以包含多個提供者社團組織。

在這個範例中，管理作業之委託如下：

- SPA 有權限來管理 VIS 提供者社團組織及其下所有的社團組織。SPA 角色指派給 DEF 社團組織中的使用者 1。
- 名為 OA1 的社團組織管理員管理 DEF，DEF 是一個共用社團組織。此 OA 角色指派給 DEF 社團組織中的使用者 2。
- OA2 管理 HIJ，HIJ 是一個共用社團組織。此 OA 角色指派給 HIJ 社團組織中的使用者 4。

- OA3 管理 SESTA，SESTA 是一個完整社團組織。此 OA 角色指定給 SESTA 社團組織中的使用者 1。

SESTA 是一個完整社團組織並且有它自己獨特的名稱空間。SESTA 中 (在 `sesta.com` 網域中) 的使用者 1 有一個獨特的使用者 ID。

如需提供者及下層社團組織的定義，請參閱「[服務提供者管理員所管理的社團組織](#)」。

服務提供者管理員角色

SPA 可以執行下列作業：

- 建立、刪除及修改在提供者社團組織中 SPA 有管理權限的共用及完整社團組織。

在圖 A-1 中顯示的範例中，VIS 提供者社團組織的 SPA 可以

- 修改或刪除 DEF、HIJ 及 SESTA 社團組織
- 在 VIS 提供者社團組織之下建立額外的社團組織。

- 建立、刪除及修改在提供者社團組織之下任何社團組織中的使用者。
- 將 OA 角色指定給使用者。

例如，在圖 A-1 中顯示的範例社團組織中，SPA 可以指定一個 OA 角色給 SESTA 社團組織中的使用者 2。然後使用者 2 就可以管理 SESTA 社團組織中的使用者。

SPA 也可以移除使用者的 OA 角色。

- 指定 SPA 角色給提供者社團組織下的其他合法使用者 (及移除 SPA 角色)。
- 將服務等級套裝軟體配置給社團組織。

關於服務等級套裝軟體的資訊，請參閱第 1 章「[Delegated Administrator 簡介](#)」中的「[服務套裝軟體](#)」。

SPA 可將特定種類的服務等級套裝軟體指定給社團組織，並確定每個套裝軟體可在社團組織中使用的最大數目。

例如，SPA 可指定下列服務等級套裝軟體：

- 在 DEF 社團組織中：
 - 1,000 個 Gold 套裝軟體
 - 500 個 Platinum 套裝軟體

- 在 HIJ 社團組織中：
 - 2,500 個 Topaz 套裝軟體
 - 500 個 Platinum 套裝軟體
 - 500 個 Emerald 套裝軟體
 - 1,000 個 Ruby 套裝軟體
- 在 SESTA 社團組織中：
 - 2,000 個 Silver 套裝軟體
 - 1,500 個 Gold 套裝軟體
 - 100 個 Platinum 套裝軟體

SPA 可以使用 **Delegated Administrator** 主控台來執行這些作業。在此發行版本中，**Delegated Administrator** 公用程式不包含執行這些作業的指令選項。

備註

TLA 可以修改或刪除任何現有的共用社團組織或完整社團組織。
TLA 也可以管理那些社團組織中的使用者。

TLA 可以透過主控台從一個使用者上移除 SPA 角色但不能指定 SPA 角色。如需此 **Delegated Administrator** 發行版本中的限制清單，請參閱「[此發行版本的注意事項](#)」。

如需 TLA 所執行的管理作業之完整描述，請參閱第 1 章「[Delegated Administrator 簡介](#)」中的「[管理員角色和目錄階層](#)」。

指定 SPA 角色給一個使用者

SPA 角色必須指定給派定給 SPA 的社團組織以及 SPA 所管理的提供者社團組織之下層社團組織中的使用者。

在圖 A-1 中顯示的範例中，假設您必須為提供者社團組織建立一個名為 VIS 的 SPA。您可以指定 SPA 角色給社團組織 DEF 中的使用者 1。

SPA 必須常駐在下層社團組織中，因為提供者社團組織節點不包含任何使用者。

因此，在 SPA 能夠管理提供者社團組織之前，在它下面至少必須建立一個社團組織。此社團組織應該派定為保留被指定為 SPA 角色的使用者。如需詳細資訊，請參閱此附錄後面的「[建立提供者社團組織及服務提供者管理員](#)」。

此發行版本的注意事項

在此 Delegated Administrator 發行版本中，您不能使用 Delegated Administrator 主控台或公用程式來建立 SPA 或提供者社團組織。

若要建立 SPA 或提供者社團組織，您必須手動修改自訂的服務提供者範本，`da.provider.skeleton.ldif`。

如需使用自訂服務提供者範本來執行這些作業的說明，請參閱此附錄後面的「[建立提供者社團組織及服務提供者管理員](#)」。

服務提供者管理員所管理的社團組織

SPA 可以建立、修改及刪除 SPA 提供者社團組織下層的下列社團組織類型：

- [完整社團組織](#)
- [共用社團組織](#)

提供者社團組織、完整社團組織及共用社團組織於下列各節中描述。

提供者社團組織

提供者社團組織是 LDAP 目錄中在邏輯上包含完整社團組織及共用社團組織的節點。提供者社團組織節點有允許 SPA 管理下層社團組織的屬性。

在 LDAP 目錄中，提供者社團組織必須位於郵件網域之下。如需範例，請參閱此附錄後面的「[範例服務提供者社團組織資料](#)」。

提供者社團組織不能包含使用者項目。而是由在提供者社團組織下建立的社團組織中所提供。

提供者社團組織儲存關於在其下建立的社團組織之目錄資訊。例如：

- 提供者社團組織是否可以包含共用社團組織、完整社團組織，或是兩者皆可
- 在此提供者社團組織下建立的共用社團組織所能夠使用的網域名稱
- 在此提供者社團組織下建立的社團組織所能夠使用的服務等級套裝軟體數目及類型
- 此提供者社團組織之 SPA 主要的指派社團組織。

完整社團組織

完整社團組織有下列特性：

- 它是提供者社團組織的下層並且由 SPA 所建立的。
- 使用者可以在完整社團組織中提供。

在圖 A-1 中顯示的範例中，使用者 2 屬於 `sesta.com` 網域並且有一個 `user2@sesta.com` 的郵件位址。

- 作為一個完整社團組織，它有它自己的網域且是其他社團組織所不能分享的，以及它自己唯一的名稱空間。

在圖 A-1 中顯示的範例中，完整網域 SESTA 有 `sesta.com` 的網域名稱。

共用社團組織

共用社團組織有下列特性：

- 它是提供者社團組織的下層並且由 SPA 所建立的。
- 使用者可以在共用社團組織中提供。

在圖 A-1 中顯示的範例中，使用者 5 屬於 `siroe.com` 網域並且有一個 `user5@siroe.com` 的郵件位址。

- 它使用由提供者社團組織所提供的清單上的一個或多個共用網域名稱。

在圖 A-1 中顯示的範例中，共用社團組織 DEF 使用 `siroe.com` 的網域名稱。

- 其他共用社團組織可以分享此社團組織所使用的的網域名稱。

在圖 A-1 中顯示的範例中，DEF 和 HIJ 社團組織都屬於 `siroe.com` 網域。

- 共用社團組織沒有唯一的名稱空間。

建立提供者社團組織及服務提供者管理員

在此 Delegated Administrator 的發行版本中，您必須使用 Delegated Administrator 所提供的自訂服務提供者範本 (`da.provider.skeleton.ldif`) 來建立您自己的提供者社團組織及 SPA。

注意 您也可以執行 **Delegated Administrator** 配置程式時，在目錄中安裝提供者社團組織的範例 (有下層社團組織的) 及 **SPA** 範例。您可以在配置程式中選擇 [載入範例社團組織] 來執行此操作。

但是，範例社團組織範本 (da.sample.data.ldif) 是用來作為範例的，而不是建立您自己的提供者社團組織之範本。如需關於此範例的詳細資訊，請參閱此附錄後面的「[範例服務提供者社團組織資料](#)」。

一旦您建立了提供者社團組織及 **SPA**，**SPA** 可以登入 **Delegated Administrator** 主控台、建立及管理下層社團組織、並且指定 **SPA** 角色給 **SPA** 社團組織中的其他使用者。但是，這些 **SPA** 只能夠管理相同的提供者社團組織。

若要建立另一個提供者社團組織及 **SPA** 來管理它，您應該再使用一次自訂服務提供者範本。

本節描述下列主題：

- 「[範本所建立的項目](#)」顯示一個在編輯過版本的範本安裝到目錄上時建立的社團組織範例。
- 「[建立提供者社團組織、下層社團組織及 SPA 所需的資訊](#)」定義範本中建立提供者社團組織、下層共用社團組織以及 **SPA** 所需要的參數。
- 「[建立提供者社團組織及服務提供者管理員的步驟](#)」解釋如何編輯範本及安裝資訊至您的目錄中。
- 「[自訂服務提供者範本](#)」為範本清單。

範本所建立的項目

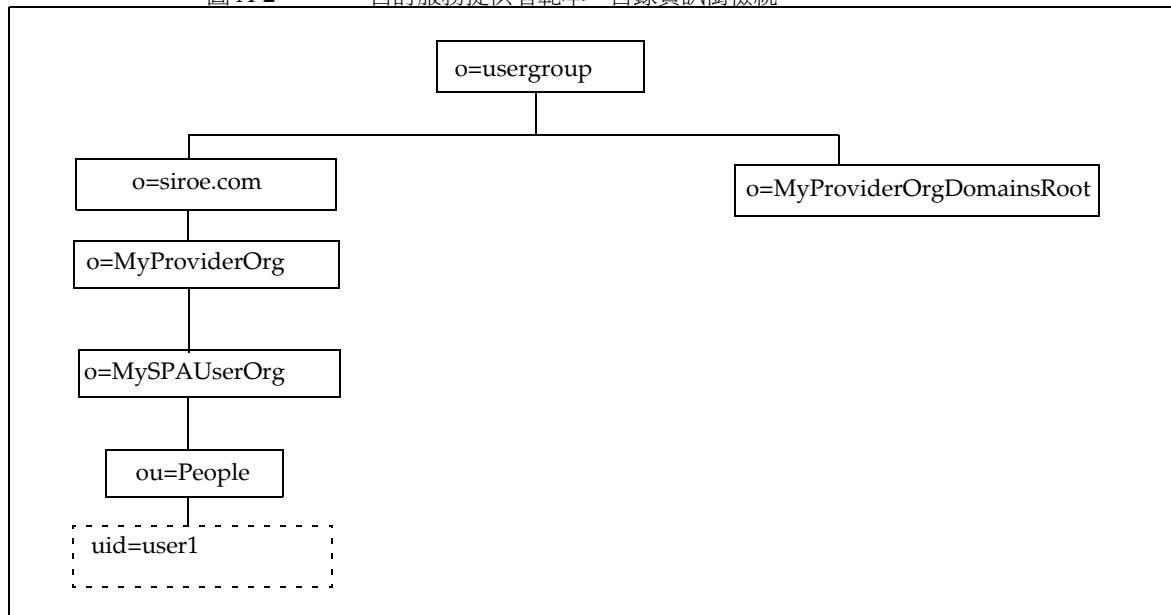
當您在目錄中安裝編輯過版本的自訂服務提供者範本時，會建立下列項目：

- 提供者社團組織
- 派定為保留 **SPA** 使用者的下層共用社團組織
- 下層社團組織中指定為 **SPA** 角色的一個使用者
- 一個能夠建立完整社團組織的萬用字元節點。**SPA** 會替這個提供者社團組織管理這些完整社團組織。

圖 A-2 顯示安裝範本所建立的項目之範例。它是這個社團組織的目錄資訊樹 (DIT) 檢視。

圖 A-2 只是一個範例。您的社團組織名稱、SPA 使用者名稱及 DIT 結構應該為您自己的安裝所特有的。

圖 A-2 自訂服務提供者範本：目錄資訊樹檢視



範例中安裝自訂服務提供者範本的節點

圖 A-2 中顯示的範例中之節點如下：

- o=usergroup — 使用者 / 群組資料的根尾碼。
- o=siroe.com — 提供者社團組織使用的郵件網域。
- o=MyProviderOrg — 提供者社團組織節點。
- o=MySPAUserOrg — 派定為保留提供者社團組織使用者，包括指定為 SPA 角色的使用者的下層共用社團組織。
- ou=people — 包含使用者所需的標準 LDAP 社團組織單位。
- uid=user1 — 在 MySPAUserOrg 社團組織中指定為 SPA 的使用者之 uid。
- o=MyProviderOrgDomainsRoot — 保留 MyProviderOrg 提供者社團組織下層的完整社團組織之萬用字元節點。

建立提供者社團組織、下層社團組織及 SPA 所需的資訊

若要建立一個提供者社團組織、一個下層社團組織及一個 SPA，必須以您安裝特有的資訊取代在自訂服務提供者範本中的參數。

在您閱讀關於這些參數的同時，您可以參閱「[自訂服務提供者範本](#)」所顯示的 `da.provider.skeleton.ldif` 清單。或開啓實際的 `ldif` 檔案，位於下列目錄中：

`da_base/lib/config-templates`

如需與這些參數相關聯之屬性的定義，請參閱「[Sun Java System Communications Services Schema Reference](#)」中的第 5 章「[Classes and Attributes Used by Communications Services Delegated Administrator \(Schema 2\)](#)」及第 3 章「[Attributes](#)」。

定義提供者及下層社團組織之參數

若要建立提供者社團組織及下層社團組織，請編輯下列參數：

- `ugldapbasedn`

您目錄中使用者 / 群組資料的根尾碼。

範例：

`o=usergroup`

`dc=red,dc=iplanet,dc=com`

- `maildomain_dn`

完成將在其下建立提供者社團組織的郵件網域之 DN。

範例：

`o=siroe.com, o=usergroup`

`o=sesta.com,o=SharedDomainsRoot,o=Business,dc=red,dc=iplanet,dc=com`

- `maildomain_dn_str`

郵件網域 DN 以底線符號 (`_`) 取代全部的逗號 (`,`)。

例如，如果郵件網域 DN 為

`o=siroe.com,o=SharedDomainsRoot,o=Business,dc=red,dc=iplanet,dc=com`

郵件網域 DN 字串將會是

```
o=siroe.com_o=SharedDomainsRoot_o=Business_dc=red_dc=iplanet_dc=com
```

- *providerorg*

提供者社團組織名稱。提供者社團組織位於的目錄節點將獲得此名稱。

此參數在 `da.provider.skeleton.ldif` 範本中使用多次。

範例：

```
sunProviderOrgDN: o=MyProviderOrg,o=siroe.com,o=usergroup
```

```
o=MyProviderOrg
```

```
sunBusinessOrgBase: o=MyProviderOrgdomainsroot, o=usergroup
```

- *servicepackage*

能夠被指定給提供者社團組織之下層社團組織中使用者的服務套裝軟體名稱。這是一個多重值的參數。

在 `da.provider.skeleton.ldif` 檔案中的「提供者社團組織」節，您會看到下列屬性：

```
sunIncludeServices: <servicepackage>
```

在您要包含在提供者社團組織之中的每一個服務套裝軟體中，加入一個 `sunIncludeServices` 屬性及 `servicepackage` 參數的實例。只有列在這裡的服務套裝軟體能夠指派給下層社團組織中的使用者。

範例：

```
sunIncludeServices: Gold
```

```
sunIncludeServices: Platinum
```

```
sunIncludeServices: Ruby
```

```
sunIncludeServices: Silver
```

如果您不使用 `sunIncludeServices` 屬性 (如果您刪除含有 `servicepackage` 參數的那一行)，目錄中所有的服務套裝軟體都可以被指定。

- *domain_name*

能夠被指定給提供者社團組織之下層社團組織的網域名稱。這是一個多重值的參數。

在 `da.provider.skeleton.ldif` 檔案中的「提供者社團組織」節，您會看到下列屬性：

```
sunAssignableDomains: <domain_name>
```


`sunAssignableDomains` 屬性中的網域名稱是列於郵件網域社團組織的 `sunPreferredDomain` 和 `associatedDomain` 屬性中的名稱之子集 (一些或全部)。(郵件網域為在其下建立此提供者社團組織之社團組織。)

在您要包含在提供者社團組織之中的每一個網域名稱中，加入一個 `sunAssignableDomains` 屬性及 `domain_name` 參數的實例。只有列在這裡的網域名稱能夠指派給下層社團組織。

範例：

```
sunAssignableDomains: siroe.com
sunAssignableDomains: siroe.net
sunAssignableDomains: varrius.com
sunAssignableDomains: sesta.com
sunAssignableDomains: sesta.net
```

- *provider_sub_org*

SPA 使用者所位於的共用社團組織名稱。當您安裝編輯過的 `ldif` 資訊於目錄中時，此社團組織被建立為提供者社團組織的共用及下層社團組織。它是派定為包含 SPA 使用者的社團組織。其他指定為此提供者社團組織的 SPA 角色必須位於此下層共用社團組織中。

在 `da.provider.skeleton.ldif` 檔案中的「提供者社團組織」節，您會看到下列屬性：

```
sunProviderOrgDN:
o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
```

`sunProviderOrgDN` 屬性識別派定給提供者社團組織使用者的社團組織，特別是 SPA 使用者。

範例：

```
sunProviderOrgDN:
o=MySPAUserOrg,o=MyProviderOrg,o=siroe.com,o=usergroup
```

- *preferredmailhost*

提供者社團組織之下層社團組織的慣用郵件主機的機器名稱 (SPA 使用者所在處)。您必須使用完整格式網域名稱 (FQDN)。

在 `da.provider.skeleton.ldif` 檔案中的「下層共用社團組織」節，您會看到下列屬性：

```
preferredMailHost: <preferredmailhost>
```

範例：

```
preferredMailHost: mail.siroe.com
```

- *available_domain_name*

可以指定給特定下層社團組織中的使用者之網域名稱。這是一個多重值的參數。

用於 *available_domain_name* 的數值為給 `sunAssignableDomains` 數值的適當子集：`<domain_name>` 屬性和參數。而 *domain_name* 套用在整個提供者社團組織上，*available_domain_name* 套用在單一下層社團組織上。

在 `da.provider.skeleton.ldif` 檔案中的「下層共用社團組織」節，您會看到下列屬性：

```
sunAvailableDomainNames: <available_domain_name>
```

為每一個您要此下層社團組織從提供者社團組織的 `sunAssignableDomains` 屬性中的網域名稱清單繼承的網域名稱，加入一個 `sunAvailableDomains` 屬性及 *available_domain_name* 參數的實例。只有列在這裡的網域名稱能夠指派給下層社團組織。

範例：

```
sunAvailableDomainNames: siroe.com
sunAvailableDomainNames: siroe.net
sunAvailableDomainNames: varrius.com
```

- *available_services*

特定下層社團組織可用的服務套裝軟體。這是一個多重值的參數。

指定給下層社團組織的服務套裝軟體是那些指定給有 `sunIncludeServices` 屬性之整個提供者社團組織的子集。

在 `da.provider.skeleton.ldif` 檔案中的「下層共用社團組織」節，您會看到下列屬性：

```
sunAvailableServices: <available_services>
```

available_services 參數的格式為

```
Service package name: count
```

其中 *count* 為一個整數。如果沒有計數，預設值為未限制的數目。

為每一個您要此下層社團組織從提供者社團組織的 `sunIncludeServices` 屬性中可用的服務套裝軟體中繼承的服務套裝軟體，加入一個 `sunAvailableServices` 屬性及 *available_services* 參數的實例。

範例：

```
sunAvailableServices: Gold: 1500
sunAvailableServices: Platinum: 2000
sunAvailableServices: Silver: 5000
```

定義 SPA 的參數

若要建立 SPA，編輯下列參數：

- *spa_uid*
SPA 使用者的使用者 ID。
範例：
uid: user1
- *spa_password*
SPA 使用者的密碼。
範例：
userPassword: x12P3&qrS
- *spa_firstname*
SPA 使用者的名字。
範例：
givenname: John
- *spa_lastname*
SPA 使用者的姓氏。
範例：
sn: Smith
- *spa_servicepackage*
指定給 SPA 使用者的服務套裝軟體。關於服務套裝軟體的資訊，請參閱第 1 章「[Delegated Administrator 簡介](#)」中的「[服務套裝軟體](#)」。
範例：
inetCos: platinum
- *spa_mailaddress*
SPA 使用者的郵件位址。郵件位址的網域部分必須為取代 *available_domain_name* 參數的網域值之一。也就是說，它必須是 SPA 使用者所位於的下層社團組織中能夠使用的網域。如需更多資訊，請參閱「[available_domain_name](#)」。
範例：

郵件：user1@siroe.com

如需如何編輯自訂服務提供者範本和在您的目錄中安裝資訊的說明，請參閱「[建立提供者社團組織及服務提供者管理員的步驟](#)」。

建立提供者社團組織及服務提供者管理員的步驟

若要建立提供者社團組織和服務提供者管理員，請遵循這些步驟：

1. 在目錄中建立郵件網域。

如果您尚未如此做，則請在您的目錄中建立郵件網域。提供者社團組織及它的下層共用社團組織將會使用此郵件網域。

2. 複製並重新命名 `da.provider.skeleton.ldif` 檔案。

當您安裝 **Delegated Administrator** 時，`da.provider.skeleton.ldif` 檔案安裝在下列目錄中：

```
da_base/lib/config-templates
```

3. 在您的 `da.provider.skeleton.ldif` 檔案複本中編輯下列參數。用正確的參數值來進行您的安裝。

如需這些參數的定義，請參閱「[建立提供者社團組織、下層社團組織及 SPA 所需的資訊](#)」。

某些參數在 `ldif` 檔案中使用超過一次。您必須搜尋並取代每一個參數的全部實例。

一些參數代表多重值屬性之值。您可以複製和編輯這些參數，以及與它們相關聯的屬性名稱的參數，以允許這些屬性的多個實例在您的 `ldif` 檔案中。多重值的參數在下面備註。

- `<ugldapbasedn>`
- `<maildomain_dn>`
- `<maildomain_dn_str>`
- `<providerorg>`
- `<servicepackage>` (多重值)
- `<domain_name>` (多重值)
- `<provider_sub_org>`
- `<preferredmailhost>`

- <available_domain_name> (多重值)
- <available_services> (多重值)
- <spa_uid>
- <spa_password>
- <spa_firstname>
- <spa_lastname>
- <spa_servicepackage>
- <spa_mailaddress>

如需與這些參數相關聯之屬性的定義，請參閱「Sun Java System Communications Services Schema Reference」中的第 5 章「Classes and Attributes Used by Communications Services Delegated Administrator (Schema 2)」及第 3 章「Attributes」。

4. 使用 LDAP ldapmodify 目錄工具來安裝提供者社團組織及 SPA 到目錄中。

例如，您可以執行下列指令：

```
ldapmodify -D <directory manager> -w <password>
-f <da.provider.finished.ldif>
```

其中

<directory manager> 是 Directory Server 管理員的名稱。

<password> 是 Directory Server 管理員的密碼。

<da.provider.finished.ldif> 是作為新的提供者社團組織及 SPA 到安裝目錄中之編輯過的 ldif 檔案名稱。

自訂服務提供者範本

此範本 (da.provider.skeleton.ldif) 包含您建立提供者社團組織及 SPA 所必須修改的參數。

下面列表顯示 ldif 檔案有參數的區段。此列表不包含整個檔案。支援 Access Manager 必需的項目和 ACI 不包含在這裡。

您應該只修改 ldif 檔案中的參數。請勿修改檔案中與 Access Manager 相關的區段。

da.provider.skeleton.ldif 檔案 (相關的區段)

```

#
# The following parameterized values must be replaced.
#
# <ugldapbasedn>          :: Root suffix for user/group data
# <maildomain_dn>         :: Complete dn of the mail domain underneath which the
#                           provider organization will be created.
# <maildomain_dn_str>     :: The maildomain dn with all ',' replaced by '_'. E.g.
#                           dn --> o=siroe.com,o=SharedDomainsRoot,o=Business,
#                           dc=red,dc=iplanet,dc=com
#                           dn_str --> o=siroe.com_o=SharedDomainsRoot_o=Business_
#                           dc=red_dc=iplanet_dc=com
# <providerorg>           : Organization value for provider node.
# <servicepackage>       :: One for each service package to include.
#                           All service packages in the system may be assigned
#                           by leaving this value empty.
# <domain_name>          :: One for each DNS name which may be assigned to a
#                           subordinate organization.
#                           These names form a proper subset (some or all) of the
#                           names listed in the <maildomain> organization's
#                           sunpreferreddomain and associateddomain attributes.
# <provider_sub_org>     :: Organization value for the shared subordinate
#                           organization in which the Provider Administrator resides.
# <preferredmailhost>    :: Name of the preferred mail host for the provider's
#                           subordinate organization.
# <available_domain_name> :: one for each DNS name that an organization allows an
#                           organization admin to use when creating a user's mail
#                           address. This is a proper subset of the values given
#                           for <domain_name> (sunAssignableDomains attribute).
# <available_services>   :: One for each service packags available to an
#                           organization (sunAvailableServices attribute). These
#                           service packages form a proper subset of the ones
#                           assigned to a provider organization - <servicepackage>
#                           (sunIncludeServices attribute). Form is
#                           <service package name>:<count>
#                           where count is an integer. If count is absent then
#                           default is unlimited.
# <spa_uid>              :: The uid for the service provider administrator.
# <spa_password>         :: The password for the service provider administrator.
# <spa_firstname>       :: First name of the service provider administrator.
# <spa_lastname>        :: Last name of the service provider administrator.
# <spa_servicepackage>   :: Service package assigned to the service provider
#                           administrator.
# <spa_mailaddress>     :: The spa's mail address. The domain part of the mail
#                           address must be one of the values used for
#                           <available_domain_name>.
#
#
#

```

```

# Provider Organization
#
dn: o=<providerorg>,<maildomain_dn>
changetype: add
o: <providerorg>
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunManagedProvider
sunAllowBusinessOrgType: full
sunAllowBusinessOrgType: shared
sunBusinessOrgBase: o=<providerorg>domainsroot,<ugldapbasedn>
sunIncludeServices: <servicepackage>
sunAssignableDomains: <domain_name>
sunAllowMultipleDomains: true
sunAllowOutsideAdmins: false
sunProviderOrgDN: o=<provider_sub_org>,<providerorg>,<maildomain_dn>
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Full Organizations node
#
dn: o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
o: <providerorg>DomainsRoot
objectClass: top
objectClass: organization
objectClass: sunmanagedorganization
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Provider Admin Role shared organizations
#
dn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top

```

```

iplanet-am-role-description: Provider Admin

#
# Provider Admin Role full organizations
#
dn: cn=Provider Admin Role,o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Shared Subordinate Organization. Includes 1 users who is the Provider Administrator.
#
dn: o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
preferredMailHost: <preferredmailhost>
sunNameSpaceUniqueAttrs: uid
o: <provider_sub_org>
objectClass: inetdomainauthinfo
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunnamespace
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunDelegatedOrganization
objectClass: sunMailOrganization
sunAvailableDomainNames: <available_domain_name>
sunAvailableServices: <available_services>
sunOrgType: shared
sunMaxUsers: -1
sunNumUsers: 1
sunMaxGroups: -1
sunNumGroups: 0
sunEnableGAB: true
sunAllowMultipleServices: true
inetDomainStatus: active
sunRegisteredServiceName: GroupMailService
sunRegisteredServiceName: DomainMailService
sunRegisteredServiceName: UserMailService
sunRegisteredServiceName: iPlanetAMAuthService
sunRegisteredServiceName: UserCalendarService
sunRegisteredServiceName: iPlanetAMAuthLDAPService
sunRegisteredServiceName: DomainCalendarService
# .
# .

```



```

# [Entries and ACIs required by Access Manager]
# .
# .

dn: ou=People,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: People
objectClass: iplanet-am-managed-people-container
objectClass: organizationalUnit
objectClass: top

dn: ou=Groups,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: Groups
objectClass: iplanet-am-managed-group-container
objectClass: organizationalUnit
objectClass: top
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# User - provider administrator
#
dn: uid=<spa_uid>,ou=People,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
sn: <spa_lastname>
givenname: <spa_firstname>
cn: <spa_firstname> <spa_lastname>
uid: <spa_uid>
iplanet-am-modifiable-by: cn=Top-level Admin Role,<ugldapbasedn>
objectClass: inetAdmin
objectClass: top
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: iPlanetPreferences
objectClass: person
objectClass: organizationalPerson
objectClass: inetuser
objectClass: inetOrgPerson
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: inetSubscriber
objectClass: userPresenceProfile
objectClass: icsCalendarUser
mailhost: <preferredmailhost>
mail: <spa_mailaddress>
maildeliveryoption: mailbox

```

```
mailuserstatus: active
inetCos: <spa_servicepackage>
inetUserStatus: Active
nsroledn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
userPassword: <spa_password>
```

範例服務提供者社團組織資料

當您執行 Delegated Administrator 配置程式 config-commda 時，您可以選擇安裝範例社團組織資料（於一個 ldif 檔案中定義）至您的目錄中。（當您執行配置程式時，在 [服務套裝軟體及社團組織範例] 面板中選取 [載入範例社團組織]。）配置程式將 da.sample.data.ldif 檔案新增至 LDAP 目錄樹中。

此 ldif 檔案是用來做為範例，不是做為建立您自己的提供者社團組織之範本。若要建立新的提供者社團組織，請參閱「[建立提供者社團組織、下層社團組織及 SPA 所需的資訊](#)」。

範例資料所提供的社團組織

圖 A-1 顯示範例 ldif 檔案所提供的組織結構之邏輯檢視。（圖 A-1 新增一個不存在此檔案中的共用社團組織 HIJ。）

範例 ldif 檔案包含下列在根尾碼節點之下的社團組織：

- VIS 提供者社團組織。下列社團組織是由 SPA 為 VIS 提供者社團組織所管理的：
 - SESTA，一個完整社團組織。SESTA 社團組織有它自己的網域 sesta.com。
 - DEF，一個共用社團組織。DEF 社團組織使用共用網域 siroe.com。
- ESG 提供者社團組織。此提供者社團組織沒有定義下層社團組織。

ldif 檔案為這些社團組織定義下列管理員角色：

- 一個給 VIS 提供者社團組織的 SPA
- 一個給 ESG 提供者社團組織的 SPA
- 一個給 SESTA 社團組織的 OA
- 一個給 DEF 社團組織的 OA

邏輯階層結構和目錄資訊樹

在三層次目錄階層結構中，目錄資訊樹 (DIT) 看起來和圖 A-1 中所顯示的邏輯檢視並不完全一樣。社團組織在 DIT 中實行於一個稍微不同的階層結構中。

例如，DIT 內完整的網域必需直接位於根尾碼之下。因此，網域節點新增至根尾碼下面來為共用網域 (為共用社團組織所使用) 及完整社團組織 (有它們自己的網域) 儲存 LDAP 資訊。

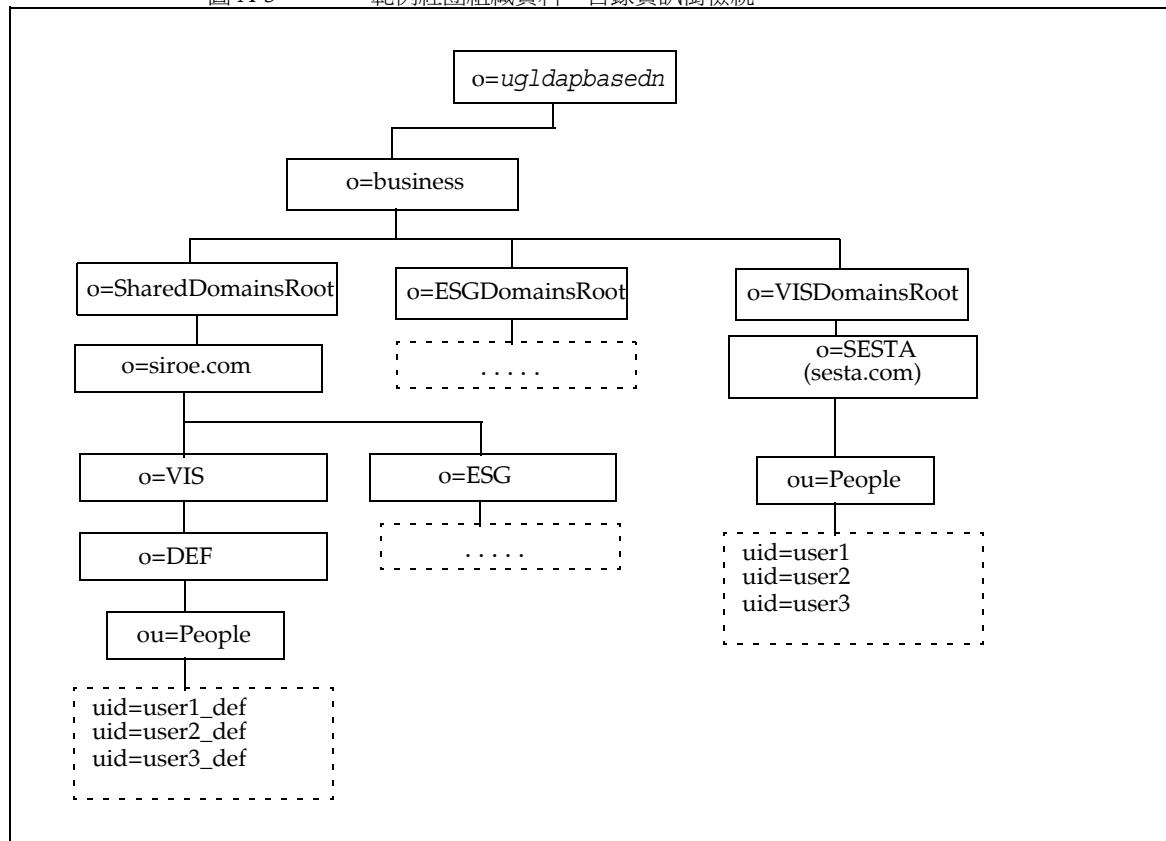
範例社團組織資料：目錄資訊樹檢視

圖 A-3 顯示範例社團組織資料的目錄資訊樹 (DIT) 檢視。

圖 A-3 中顯示的範例中，如同圖 A-1 中顯示的邏輯檢視，包含下列社團組織：

- VIS 和 ESG (提供者社團組織)
- DEF，一個 VIS 提供者社團組織下層的共用社團組織。
- SESTA，一個 VIS 提供者社團組織下層的完整社團組織。

圖 A-3 範例社團組織資料：目錄資訊樹檢視



範例目錄資訊樹檢視中的節點

範例社團組織檔案 (da.sample.data.ldif) 中的節點如下：

- `ugldapbasedn` — 此參數代表根尾碼。
- `o=business` — 包含目錄中全部商務的節點。
- `o=SharedDomainsRoot` — 包含共用社團組織使用網域所需的節點。

在目錄資訊樹中，不同服務提供者組織下層的共用社團組織可以使用相同的共用網域。能夠如此做是因為兩個提供者社團組織都有節點在 `SharedDomainsRoot` 節點之下。

- `o=ESGDomainsRoot` 和 `o=VISDomainsRoot` — 這些節點含有 ESG 和 VIS 提供者社團組織下層任何的完整社團組織。

每一個管理完整社團組織的提供者社團組織必須在此層級有一個節點（位於根尾碼之下）。

多個完整社團組織，每一個有它自己的網域，可以存在於 ESGDomainsRoot 或 VISDomainsRoot 之下。

- o=siroe.com — 共用網域。它為共用社團組織 DEF 所使用。
- o=VIS 和 o=ESG — 這些提供者社團組織節點包含 VIS 和 ESG 提供者社團組織下層任何共用社團組織。

例如，共用社團組織 DEF，是 VIS 提供者社團組織的下層。

- o=SESTA — 完整社團組織。它有它自己的網域，sesta.com。
- o=DEF — 共用社團組織。它使用網域 siroe.com。
- ou=people — 包含使用者所需的標準 LDAP 社團組織單位。

範例目錄資訊樹檢索中的使用者 DN

圖 A-3 範例社團組織檔案中顯示的一些使用者 DN 如下：

- 用於名為 user1_def 的使用者，屬於 DEF 社團組織：

```
dn:uid=user1_def,ou=People,o=DEF,o=VIS,o=siroe.com,  
o=SharedDomainsRoot,o=Business,ugldapbasedn
```
- 用於名為 user1_def 的使用者，屬於 SESTA 社團組織：

```
dn:uid=user1,ou=People,o=SESTA,o=VISDomainsRoot,  
o=Business,ugldapbasedn
```


屬性值和行事曆等項

屬性值

在表 B-1 中列出的屬性可以和 -P 選項一起使用於下列指令：`commadmin domain create` 和 `commadmin domain modify`。這些屬性為位元導向屬性或多重值屬性。

表 B-1 用於 -P 選項之屬性

屬性	值	描述
<code>createLowerCase</code>	是 / 否	指定是否為新的使用者建立小寫行事曆。並且，當查詢行事曆時，是否查詢小寫行事曆。
<code>filterPrivateEvents</code>	是 / 否	指定當查詢伺服器時是否篩選私有或機密事件
<code>fbIncludeDefCal</code>	是 / 否	指定使用者的預設行事曆是否包含在使用者的 <code>freebusy-calendar-list</code> 中。
<code>subIncludeDefCal</code>	是 / 否	指定使用者的預設行事曆是否包含在使用者的 <code>subscribed-calendar-list</code> 中。
<code>resourceDefaultAcl</code>	是 / 否	指定是否使用預設 ACL 於資源行事曆。
<code>calmasterCred</code>	字串	被指定為「Calendar Server 管理員」使用者的憑證。
<code>calmasterUid</code>	字串	<code>service.admin.calmaster.userid</code>
<code>calmasterAccessOverride</code>	是 / 否	指定 Calendar Server 管理員是否可以置換存取控制。
<code>setPublicRead</code>	是 / 否	設定預設使用者行事曆為公用讀取或私有寫入。如果選取 [否]，會設定使用者行事曆為私有讀取或私有寫入。

表 B-1 用於 -P 選項之屬性 (續)

屬性	值	描述
uiBaseUrl	字串	BaseServerAddress，例如，「https://proxyserver/」
uiConfigFile	字串	用於使用者介面之配置檔案。
uiProxyUrl	字串	附加在 HTML 使用者介面的 JavaScript 檔案中之代理伺服器位址。例如，https://web_portal.iplanet.com/
domainAccess	字串	用於網域之存取控制字串。使用在交互網域搜尋中。
uiAllowAnyone	是 / 否	指定是否允許 HTML 使用者介面顯示和使用「所有人」ACL。
allowProxyLogin	是 / 否	指定是否允許代理登入

在表 B-2 中列出的屬性可以和 -R 選項一起使用於下列指令：`comadmin domain create` 和 `comadmin domain modify`。這些屬性有位元導向值。

如需關於 WCAP 和 WCAP `set-userprefs` 指令的資訊，請參閱「Delegated Administrator 指南」。

表 B-2 用於 -R 選項之屬性

屬性	值	描述
allowUserDoubleBook	8 位元	允許此行事曆在同一個時段有一個以上的排程。
allowResourceDoubleBook	9 位元	允許此資源行事曆在同一個時段有一個以上的排程。
allowModifyUserPreferences	4 位元	允許 Calendar Server 管理員 <code>get/set userprefs</code> 應該為使用者從 WCAP 取得。
allowModifyPassword	5 位元	允許使用者透過此伺服器變更他們的密碼。
allowCalendarCreation	0 位元	允許建立行事曆。
allowCalendarDeletion	1 位元	允許刪除行事曆。
allowPublicWritableCalendars	2 位元	允許使用者擁有可公用寫入的行事曆。
allowSetCn	10 位元	允許 <code>set-userprefs.wcap</code> 修改 <code>cn</code> 使用者喜好設定。
allowSetGivenName	11 位元	允許 <code>set_userprefs.wcap</code> 修改 <code>givenname</code> 使用者喜好設定。

表 B-2 用於 -R 選項之屬性 (續)

屬性	位	描述
allowSetGivenMail	12 位元	允許 set_userprefs.wcap 修改 mail 使用者喜好設定。
allowSetPrefLang	13 位元	允許 set_userprefs.wcap 修改 preferredlanguage 使用者喜好設定。
allowSetSn	14 位元	允許 set-userprefs.wcap 修改 sn 使用者喜好設定。

行事曆時區字串

下列時區字串可以與 -T 時區選項一同用在 `comadmin domain create`、`comadmin domain modify`、`comadmin resource create`、`comadmin resource modify`、`comadmin user create` 和 `comadmin user modify` 指令中：

- Africa/Cairo
- Africa/Casablanca
- Africa/Johannesburg
- Africa/Lagos
- Africa/Tripoli
- Africa/Windhoek
- America/Adak
- America/Anchorage
- America/Buenos_Aires
- America/Caracas
- America/Chicago
- America/Costa_Rica
- America/Cuiaba
- America/Denver
- America/Godthab
- America/Grand_Turk

- America/Halifax
- America/Havana
- America/Indianapolis
- America/Los_Angeles
- America/Miquelon
- America/New_York
- America/Phoenix
- America/Port-au-Prince
- America/Santiago
- America/Sao_Paulo
- America/St_Johns
- Asia/Alma-Ata
- Asia/Amman
- Asia/Anandyr
- Asia/Aqtau
- Asia/Aqtobe
- Asia/Baku
- Asia/Bangkok
- Asia/Beirut
- Asia/Bishkek
- Asia/Calcutta
- Asia/Dacca
- Asia/Irkutsk
- Asia/Jerusalem
- Asia/Kabul
- Asia/Kamchatka
- Asia/Karachi

- Asia/Katmandu
- Asia/Krasnoyarsk
- Asia/Magadan
- Asia/Novosibirsk
- Asia/Rangoon
- Asia/Riyadh
- Asia/Shanghai
- Asia/Tokyo
- Asia/Ulan_Bator
- Asia/Vladivostok
- Asia/Yakutsk
- Asia/Yekaterinburg
- Asia/Yerevan
- Atlantic/Azores
- Atlantic/Cape_Verde
- Atlantic/South_Georgia
- Atlantic/Stanley
- Australia/Adelaide
- Australia/Brisbane
- Australia/Darwin
- Australia/Hobart
- Australia/Lord_Howe
- Australia/Sydney
- Europe/Bucharest
- Europe/Istanbul
- Europe/London
- Europe/Minsk

- Europe/Moscow
- Europe/Paris
- Europe/Riga
- Europe/Samara
- Europe/Simferopol
- Europe/Warsaw
- Pacific/Apia
- Pacific/Auckland
- Pacific/Chatham
- Pacific/Easter
- Pacific/Fiji
- Pacific/Gambier
- Pacific/Guadalcanal
- Pacific/Honolulu
- Pacific/Kiritimati
- Pacific/Marquesas
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pitcairn
- Pacific/Rarotonga
- Pacific/Tongatapu

除錯 Delegated Administrator

您可以透過檢查由 Delegated Administrator 元件、部署了 Delegated Administrator 的 Web 容器以及 Directory Server 和 Access Manager 所產生的記錄檔來取得 Delegated Administrator 的記錄資訊。

本附錄包含下列主題：

- [除錯指令行公用程式](#)
- [Delegated Administrator 主控台記錄](#)
- [Delegated Administrator 伺服器記錄](#)
- [Web 容器伺服器記錄](#)
- [Directory Server 和 Access Manager 記錄](#)

除錯指令行公用程式

若要除錯 Delegated Administrator 公用程式 (commadmin)，您可以使用 commadmin 指令與 -v 選項列印除錯訊息。

Delegated Administrator 主控台記錄

Delegated Administrator 主控台建立一個執行階段記錄檔：

預設記錄檔名稱：da.log

預設的位置：/opt/SUNWcomm/log

您可以透過編輯記錄特性檔案來指定您自己的記錄檔：

記錄特性檔案名稱：`logger.properties`

預設的位置：

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

您可以在 `logger.properties` 檔案中變更下列特性：

- `da.logging.enable=yes` 或 `no`

其中 `yes` 啟動記錄，而 `no` 停用記錄。

- `da.log.file=full pathname`

指定要在其中寫入記錄敘述的目錄和檔案。此特性將 `da.log` 變更成指定的檔案名稱和位置。

Delegated Administrator 伺服器記錄

您可以建立包含由安裝在 Web 容器上的 Delegated Administrator servlet 所產生之除錯敘述的 Delegated Administrator 伺服器記錄。

若要做此設定，您要啟動除錯 servlet 來記錄來自 Delegated Administrator servlet 執行的除錯訊息。您可以透過瀏覽器轉至下列 URL 路徑來開啓除錯 servlet：

`http://machine name:port/commcli/debug?op=set&state=all&package=all&filename=full path`

其中

`machine name` 是執行 Delegated Administrator 伺服器的機器名稱。

`full path` 是將寫入訊息的記錄的完整目錄路徑和名稱。

例如：

`http://abc.red.iplanet.com:8008/commcli/debug?op=set&state=all&package=all&filename=/tmp/debug.log`

前面的 URL 會將除錯 servlet 訊息記錄到下列路徑和檔案：

`/tmp/debug.log`

每當您重新啟動 Web 容器時，您必須開啓除錯 servlet。

Web 容器伺服器記錄

您可以由檢查 Web 容器所產生的伺服器記錄來進一步對 Delegated Administrator 除錯。

Web Server

Web Server 保持存取和錯誤記錄，這些記錄位於下列路徑中：

```
/web_server_base/https-machine name/logs
```

其中

web_server_base 是 Web Server 軟體安裝的路徑。

machine name 是執行 Web Server 的機器名稱。

Application Server 7.x

Application Server 7.x 保持存取和錯誤記錄，這些記錄位於下列路徑中：

```
/application_server7_base/domains/domain1/server1/logs
```

其中

application_server7_base 是 Application Server 7.x 軟體安裝的路徑。

Application Server 8.x

Application Server 8.x 保持存取和錯誤記錄，這些記錄位於下列路徑中：

伺服器記錄：

```
/application_server8_base/domains/domain1/logs
```

存取記錄：

```
/application_server8_base/domains/domain1/logs/access/server_access_log
```

其中

application_server8_base 是 Application Server 8.x 軟體安裝的路徑。

Directory Server 和 Access Manager 記錄

您可以由檢查 Directory Server 和 Access Manager 所產生的記錄來進一步對 Delegated Administrator 除錯。

Directory Server

Directory Server 保持存取和錯誤記錄，這些記錄位於下列路徑中：

```
/var/opt/mps/serverroot/slaped-hostname/logs
```

其中

hostname 是執行 Directory Server 的機器名稱。

Access Manager

Access Manager 維持下列路徑中的記錄檔。

```
/var/opt/SUNWam/debug
```

上述的路徑包含 amProfile 和 amAuth 記錄。

```
/var/opt/SUNWam/logs
```

上述的路徑包含 amAdmin.access 和 amAdmin.error 記錄。

ACI 合併計算

本附錄描述下列主題：

- [簡介](#)
- [合併計算和移除 ACI](#)
- [分析現有的 ACI](#)
- [分析如何合併計算 ACI](#)
- [捨棄之未使用的 ACI 清單](#)

簡介

當您同時安裝有 Messaging Server 和 Access Manager，並使用 LDAP Schema 2 目錄時，目錄中已初始安裝了數量龐大的存取控制指令 (ACI)。Messaging Server 不需要或者不使用許多的預設 ACI。

在執行階段檢查這些 ACI 的需要會影響 Directory Server 的效能，相對的，Directory Server 的效能又會影響 Messaging Server 查詢和其他目錄作業的效能。

您可以合併計算或減少目錄中預設 ACI 的數量，以增進 Directory Server 的效能。合併計算 ACI 也能夠使它們更容易管理。

減少 ACI 的方法如下：

- 合併、優化和簡化冗餘的 ACI
- 修改 ACI 以使用更簡單、更有效率的語法
- 將 ACI 和其他 ACI 合併計算 (在根尾碼上)
- 消除未使用的 ACI

- 對有許多社團組織的目錄，允許社團組織 ACI 自個別社團組織節點中移除。

本附錄首先描述如何使用 `ldif` 檔案 (`replacement.acis.ldif`) 來合併計算根尾碼上的 ACI 和從目錄移除未使用的 ACI。如需詳細資訊，請參閱下面的「[合併計算和移除 ACI](#)」。

接下來，此附錄分析每一個 ACI 並建議一個處理它的方法：移除、修訂以使其更有效率或重寫。

請注意這些建議中的下列限制：

- 目錄主控台沒有一般使用者存取
- Access Manager 主控台沒有一般使用者存取

有了這些限制，您必須自己決定（根據安裝需求）是否可以使用 `ldif` 檔案來合併計算和移除 ACI，或是否必需保留某些現在存在於目錄中的 ACI。

如需詳細資訊，請參閱此附錄後面的「[分析現有的 ACI](#)」。

接下來，此附錄描述由 `replacement.acis.ldif` 檔案合併計算的 ACI。它列出合併計算前現有的 ACI 和合併計算後已經修改的 ACI。如需詳細資訊，請參閱此附錄後面的「[分析如何合併計算 ACI](#)」。

最後，本附錄列出 `replacement.acis.ldif` 所捨棄的 ACI。如需詳細資訊，請參閱此附錄後面的「[捨棄之未使用的 ACI 清單](#)」。

合併計算和移除 ACI

本節中列出的 `ldif` 檔案 `replacement.acis.ldif` 會在根尾碼上安裝合併計算的 ACI，並從目錄刪除未使用的 ACI。此 `ldif` 檔案是由 Delegated Administrator 所提供，位於下列目錄中：

```
da_base/lib/config-templates
```

當您套用 `replacement.acis.ldif` 檔案到目錄上（用 `ldapmodify`），`ldapmodify` 指令會移除在根尾碼上 `aci` 屬性的全部實例，並以 `replacement.acis.ldif` 檔案中的 ACI 替代這些 ACI。

因此，初始此程式會從根尾碼移除全部 ACI，然後以下列一組 ACI 來替代它們。如果目錄包含另一個應用程式（如 Portal Server）所產生的 ACI，您應該將那些 ACI 儲存到一個檔案，然後在套用 `replacement.acis.ldif` 檔案後再將它們重新套用至目錄上。

如需使用此 ldif 檔案來清除您的 ACI 的說明，請參閱本節後面的「[替代 ACI 之步驟](#)」。

replacement.acis.ldif 檔案

```
dn: $rootSuffix
changetype: modify
replace: aci
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator";
    allow (all)
    userdn="ldap:///uid=admin,ou=Administrators,ou=TopologyManagement,
o=NetscapeRoot");)
aci: (target="ldap://$rootSuffix")
    (targetfilter=(!(objectclass=sunServiceComponent)))
    (targetattr != "userPassword|passwordHistory
    ||passwordExpirationTime||passwordExpWarned||passwordRetryCount
    ||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
    (version 3.0; acl "anonymous access rights";
    allow (read,search,compare)
    userdn = "ldap:///anyone"; )
aci: (targetattr != "nsroledn||aci||nsLookThroughLimit||nsSizeLimit
    ||nsTimeLimit||nsIdleTimeout||passwordPolicySubentry||passwordExpiration
Time
    ||passwordExpWarned||passwordRetryCount||retryCountResetTime
    ||accountUnlockTime||passwordHistory||passwordAllowChangeTime||uid||memb
erOf
    ||objectclass||inetuserstatus||ou||owner||mail||mailuserstatus
    ||memberOfManagedGroup||mailQuota||mailMsgQuota||mailhost
    ||mailAllowedServiceAccess||inetCOS||mailSMTPSubmitChannel")
    (version 3.0; acl "Allow self entry modification";
    allow (write)
    userdn ="ldap://self");)
aci: (targetattr != " aci || nsLookThroughLimit || nsSizeLimit
    || nsTimeLimit|| nsIdleTimeout")
    (version 3.0; acl "Allow self entry read search";
    allow(write)
    userdn ="ldap://self");)
|aci: (target="ldap://$rootSuffix")
    (targetattr="*")
    (version 3.0; acl "S1IS Proxy user rights";
    allow (proxy)
    userdn = "ldap:///cn=puser,ou=DSAME Users,
    $rootSuffix"; )
aci: (target="ldap://$rootSuffix")
    (targetattr="*")
```

```

(version 3.0; acl "S1IS special dsame user rights for all under the root
suffix";
allow (all)
userdn = "ldap:///cn=dsameuser,ou=DSAME Users,
$rootSuffix"; )
aci: (target="ldap:/// $rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS special ldap auth user rights";
allow (read,search)
userdn = "ldap:///cn=amldapuser,ou=DSAME Users,
$rootSuffix"; )
aci: (target="ldap:/// $rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all)
roledn = "ldap:///cn=Top-level Admin Role,
$rootSuffix"; )
aci: (targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read Only
Access";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group,ou=Groups,
$rootSuffix");)
aci: (targetattr="objectclass || mailalternateaddress || Mailautoreplymode
||
mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
|| mailforwardingaddress || mailAutoReplyTimeout ||
mailautoreplytextinternal
|| mailautoreplytext || vacationEndDate || vacationStartDate
|| mailautoreplysubject || maxPabEntries || mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
|| sunUCTimeFormat || mailuserstatus || maildomainstatus")
(version 3.0; acl "Messaging Server End User Administrator All Access";
allow (all)
groupdn = "ldap:///cn=Messaging End User Administrators Group,ou=Groups,
$rootSuffix");)
aci: (targetattr = "*" )
(version 3.0;acl "Allow Read-Only Access";
allow (read,search,compare)
groupdn = "ldap:///cn=Read-Only,ou=Groups,
$rootSuffix");)
aci: (target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)

```

```

    roledn = "ldap:///cn=Organization Admin Role, ($dn),
    $rootSuffix");
aci: (target="ldap:///($dn), $rootSuffix")
    (targetattr="*")
    (version 3.0; acl "Organization Admin Role access allow read";
    allow(read,search)
    roledn = "ldap:///cn=Organization Admin Role, [$dn],
    $rootSuffix" );
aci: (target="ldap:///($dn), $rootSuffix")
    (targetfilter=(!(|(nsroledn=cn=Top-level Admin Role, $rootSuffix)
    (entrydn=($dn), $rootSuffix))))
    ( targetattr = "*" )
    (version 3.0; acl "S1IS Organization Admin Role access allow";
    allow (all)
    roledn = "ldap:///cn=Organization Admin Role, [$dn],
    $rootSuffix");)

```

替代 ACI 之步驟

在您開始之前

在您開始此程式之前，我們建議您檢查在目錄中現有的 ACI。您應該決定您是否要保存此程式將刪除的任何 ACI。

初始此程式會從根尾碼移除全部 ACI，然後以下列一組 ACI 來替代它們。如果目錄包含 Messaging Server 以外的應用程式所產生的 ACI，您應該將那些 ACI 儲存到一個檔案，然後在套用 replacement.acis.ldif 檔案後再將它們重新套用至目錄上。

爲了幫助您分析 Access Manager 和 Messaging Server 所產生的現有 ACI，請參閱在此附錄後面部分的下列各節。

- [分析現有的 ACI](#)
- [分析如何合併計算 ACI](#)
- [捨棄之未使用的 ACI 清單](#)

替代 ACI

若要合併計算根尾碼上的 ACI 和移除未使用的 ACI，請採取下列步驟：

1. 儲存目前在根尾碼上現有的 ACI。您可以使用 `ldapsearch` 指令，如下列範例：

```
ldapsearch -D "cn=Directory Manager" -w <password>
-s base -b <$rootSuffix> aci=* aci ><filename>
```

其中

<password> 是 Directory Server 管理員的密碼。

<\$rootSuffix> 是您的根尾碼，如 `o=usergroup`。

<filename> 是會寫入儲存的 ACI 的檔案名稱。

2. 複製並重新命名 `replacement.acis.ldif` 檔案。

當您安裝 Delegated Administrator 時，`replacement.acis.ldif` 檔案安裝在下列目錄中：

```
da_base/lib/config-templates
```

3. 在您的 `replacement.acis.ldif` 檔案複本中編輯 `$rootSuffix` 項目。

變更根尾碼參數 `$rootSuffix` 成您的根尾碼 (如 `o=usergroup`)。 `$rootSuffix` 參數在 `ldif` 檔案中顯示多次；每一個實例都必需被替代。

4. 使用 LDAP 目錄工具 `ldapmodify` 來替代 ACI。

例如，您可以執行下列指令：

```
ldapmodify -D <directory manager> -w <password>
-f <replacement.acis.finished.ldif>
```

其中

<directory manager> 是 Directory Server 管理員的名稱。

<password> 是 Directory Server 管理員的密碼。

<replacement.acis.finished.ldif> 是合併計算及移除目錄中的 ACI 的已編輯過的 `ldif` 檔案名稱。

消除動態社團組織 ACI

當您使用 Delegated Administrator 主控台來建立社團組織時，社團組織節點上建立了一個 ACI 群組。

在上述程式中安裝的替代 ACI 會消除這些每個社團組織 ACI 的需要。您可以使用 Access Manager 主控台來防止建立每個社團組織的 ACI。採取下列步驟：

1. 以 amadmin 登入至 AM 主控台。AM 主控台位於下列 URL 中：
`http://<machine name>:<port>/amconsole`
其中
<machine name> 是執行 Access Manager 的機器名稱。
<port> 是連接埠
2. 選取 [服務配置] 標籤。
依預設，會顯示管理配置頁。
3. 在主控台的右邊，向下捲動至 [動態管理角色 ACI]。
4. 選取並刪除 [動態管理角色 ACI] 文字方塊中全部的 ACI。
5. 儲存編輯過的設定。

分析類型的 ACI

本節中的清單顯示當安裝 Access Manager 和 Messaging Server 時安裝到目錄中的 ACI。它也描述每個 ACI 的功能並建議某個 ACI 是否能夠保留、合併計算或捨棄。

ACI 分為下列種類：

- 根尾碼
- Access Manager
- 頂層服務台管理員角色
- 頂層策略管理員角色
- AM 自身
- 匿名 AM
- AM 拒絕寫入存取
- AM 容器管理員角色
- 社團組織服務台
- AM 社團組織管理員角色
- AM 其他
- Messaging Server

根尾碼

```
dn: $rootSuffix
#
# consolidate
#
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy state
attributes";
allow (write)
userdn ="ldap:///self";)
```

動作：合併計算。

沒有對此尾碼自身存取的需求。這是重複的 ACI；它可以與根尾碼上的自身 ACI 合併。

```
#
# retain
#
aci:
(targetattr = "*")
(version 3.0; acl "Configuration Administrator";
allow (all)
userdn = "ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement, o=NetscapeRoot";)
```

動作：保留。

這是透過「通過認證」認證 slapd-config 實例的「admin」使用者。如果全部的配置都是以 Directory Manager 執行，使用指令行公用程式，則不需要這個 ACI。若有人可能需要以此使用者認證主控台，則此 ACI 可以保留在這裡。相似的 ACI 可以移除。

```
-----
-----
#
# discard
#
aci:
(targetattr ="*")
(version 3.0;acl "Configuration Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot");)
```

動作：捨棄全部 DB 後端。

若使用主控台來委託伺服器管理權限，則這是將得到權限的「配置管理員」群組。

```
-----
-----
#
# discard
#
aci:
(targetattr ="*")
(version 3.0;acl "Directory Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Directory Administrators, $rootSuffix");)
```

動作：捨棄全部 DB 後端。

這是一般「目錄管理員」群組的權限定義。

```
#
# discard
#
aci:
(targetattr = "**")
(version 3.0; acl "SIE Group";
allow (all)
groupdn = "ldap:///cn=slapd-whater, cn=Sun ONE Directory Server, cn=Server
Group, cn=whater.red.iplanet.com, ou=red.iplanet.com, o=NetscapeRoot";)
```

動作：捨棄全部 DB 後端。

這是主控台 / 管理伺服器相關群組的權限定義。

Access Manager

```
# retain
#
aci:
(target="ldap://$rootSuffix")
(targetattr="**")
(version 3.0; acl "S1IS Proxy user rights";
allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"; )
```

動作：保留。

此 ACI 授予系統使用者存取 Access Manager 的權限。

```

#
# retain
#
aci:
(target="ldap:/// $rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root
suffix";
allow (all)
userdn = "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix"; )

```

動作：保留。

此 ACI 授予系統使用者存取 Access Manager 的權限。

```

#
# retain
#
aci:
(target="ldap:/// $rootSuffix") (targetattr="*") |
(version 3.0;acl "S1IS special ldap auth user rights";
allow (read,search)
userdn = "ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix"; )

```

動作：保留。

此 ACI 授予系統使用者存取 Access Manager 的權限。

```

#
# discard
#
aci:
(target="ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix")
(targetattr = "*" )
(version 3.0;

```

```
acl "S1IS special ldap auth user modify right";  
deny (write)  
roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 防止頂層管理員 (TLA) 修改 amldapuser 帳號。

```
#  
# retain  
#  
aci:  
(target="ldap:/// $rootSuffix")  
(targetattr="**")  
(version 3.0; acl "S1IS Top-level admin rights";  
allow (all)  
roledn = "ldap:///cn=Top-level Admin Role,$rootSuffix"; )
```

動作：保留。

此 ACI 授予頂層管理員角色存取權限。

```
#  
# discard  
#  
aci:  
(targetattr="iplanet-am-saml-user ||  
iplanet-am-saml-password") (targetfilter="(objectclass=iplanet-am-saml-service)")  
(version 3.0; acl "S1IS Right to modify saml user and password";  
deny (all)  
(roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix")  
AND (userdn != "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix")  
AND (userdn != "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"); )
```

動作：捨棄。

此 ACI 保護 SAML 相關屬性。

頂層服務台管理員角色

```
#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*" )
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

動作：捨棄。

```
#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

動作：捨棄。

頂層策略管理員角色

```
#
# discard
#
aci:
target="ldap:/// $rootSuffix"
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*" )
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 屬於頂層策略管理員角色。

```
#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*" )
(version 3.0; acl "S1IS Top-level Policy Admin Role access Auth Service
deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 屬於頂層策略管理員角色。

```

#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "")
(version 3.0; acl "SIIS Top-level Policy Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix");

```

動作：捨棄。

此 ACI 屬於頂層策略管理員角色。

```

#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter="(objectclass=sunismangedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "SIIS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix");

```

動作：捨棄。

此 ACI 屬於頂層策略管理員角色。

AM 自身

```

#
# consolidate
#
aci:

```

```
(targetattr = "*"
(version 3.0;
acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)
```

動作：合併計算成單一自我寫入 ACI。由於一般使用者沒有權限刪除任何項目（包括他們自己），因此不需要明確的拒絕。

這是多個設定自我權限的 ACI 其中之一。此明確的拒絕可防止任何項目刪除自己。

```
-----
-----
#
# consolidate
#
aci:
(targetattr = "objectclass || inetuserstatus ||
iplanet-am-user-login-status
|| iplanet-am-web-agent-access-allow-list ||
iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || iplanet-am-user-account-life
|| iplanet-am-session-max-session-time || iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions ||
iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions ||
iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)
```

動作：合併計算成單一自我寫入 ACI。

這是多個設定自我寫入權限的 ACI 其中之一。


```
#
# consolidate
#
aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci ||
nsLookThroughLimit
|| nsSizeLimit || nsTimeLimit || nsIdleTimeout || memberOf ||
iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except for nsroledn,
aci, and resource limit attributes";
allow (write)
userdn ="ldap:///self";)
```

動作：合併計算成單一自我寫入 ACI。

這是多個設定權限的 ACI 其中之一。

```
#
# consolidate
#
aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; acl "S1IS Allow self entry read search except for nsroledn,
aci, resource limit and
web agent policy attributes";
allow (read,search)
userdn ="ldap:///self";)
```

動作：合併計算成單一自我寫入 ACI。

這是多個設定自我寫入權限的 ACI 其中之一。

匿名 AM

```
-----  
#  
# consolidate  
#  
aci:  
(target="ldap:///ou=services,$rootSuffix")  
(targetfilter=(!(objectclass=sunServiceComponent)))  
(targetattr = "*")  
(version 3.0; acl "S1IS Services anonymous access";  
allow (read, search, compare)  
userdn = "ldap:///anyone";)
```

動作：合併計算成單一匿名 ACI。

這是多個授予匿名權限的 ACI 其中之一。

```
-----  
#  
# consolidate  
#  
aci:  
(target="ldap:///ou=iPlanetAMAdminConsoleService,*, $rootSuffix")  
(targetattr = "*")  
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";  
allow (read, search, compare)  
userdn = "ldap:///anyone";)
```

動作：合併計算成單一匿名 ACI。

這是多個授予匿名權限的 ACI 其中之一。

```
-----  
#  
# discard  
#  
aci:  
(target="ldap:/// $rootSuffix")  
(targetfilter=(entrydn=$rootSuffix))
```

```
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

動作：捨棄。

此 ACI 防止任何使用者 (除了 rootdn 之外) 刪除預設的社團組織。

```
-----
-----
#
# discard
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

動作：捨棄。

此 ACI 防止任何使用者 (除了 rootdn 之外) 刪除頂層管理員角色。

AM 拒絕登入存取

```
-----
#
# discard
#
aci:
(targetattr = "*")
```

```
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn = "ldap:///cn=Deny Write Access,$rootSuffix";)
```

動作：捨棄。

此 ACI 屬於拒絕寫入存取角色。

AM 容器管理員角色

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role, [$dn], $rootSuffix";)
```

動作：捨棄。

此 ACI 屬於容器管理員角色。

```
#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role, ($dn), $rootSuffix")
(targetattr="**")
```

```
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role, ($dn), $rootSuffix";)
```

動作：捨棄。

此 ACI 屬於容器管理員角色。

```
-----
-----
#
# discard
#
aci:
(target="ldap:///ou=People, $rootSuffix")
(targetfilter=(!(| (nsroledn=cn=Top-level Admin Role, $rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role, $rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role, $rootSuffix)
(nsroledn=cn=Organization Admin Role, $rootSuffix)
(nsroledn=cn=Container Admin Role, $rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com, $rootSuffix";)
```

動作：捨棄。

此 ACI 屬於群組和人物容器管理員角色。

社團組織服務台

```
-----
-----
#
# discard
#
aci: (extra verses dreambig)
```

```
(target="ldap:/// $rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix");)
```

動作：捨棄。

此 ACI 屬於社團組織服務台管理員角色。

```
#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix");)
```

動作：捨棄。

此 ACI 屬於社團組織服務台管理員角色。

AM 社團組織管理員角色

```

#
# consolidate
#
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn), $rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin Role, [$dn], $rootSuffix";)

```

動作：合併計算。

```

#
# consolidate
#
aci:
(target="ldap:///cn=Organization Admin Role, ($dn), $rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role, ($dn), $rootSuffix";)

```

動作：合併計算。

此 ACI 屬於社團組織管理員角色。

```

#
# consolidate
#
aci: (missing)
(target="ldap:///($dn), $rootSuffix")
(targetattr="*")

```

```
(version 3.0; aci "Organization Admin Role access allow read to org node";  
allow (read,search)  
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

動作：合併計算。

此 ACI 屬於社團組織管理員角色。

```
#  
# consolidate  
#  
aci:  
(target="ldap:///($dn),$rootSuffix")  
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)  
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))  
(targetattr != "nsroledn")  
(version 3.0; aci "Organization Admin Role access allow";  
allow (all)  
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

動作：合併計算。

此 ACI 屬於社團組織管理員角色。

```
#  
# consolidate  
#  
aci:  
(target="ldap:///($dn),$rootSuffix")  
(targetattr!="businessCategory || description || facsimileTelephoneNumber  
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox ||  
postalCode  
|| registeredaddress || street || 1 || st || telephonenumber  
|| maildomainreportaddress  
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
```



```
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

動作：合併計算。

此 ACI 屬於社團組織管理員角色。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

動作：合併計算。

AM 其他

```
#
#
# discard
#
aci:
(target="ldap://$rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

動作：捨棄。

捨棄此 ACI 會停用 `iplanet-am-modifiable-by` 屬性相關權限。

Messaging Server

```
#
# consolidate
#
aci:
(target="ldap:/// $rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read Access
Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

動作：合併計算。

此 ACI 授予傳訊一般使用者管理員群組權限。

```
#
# consolidate
#
aci:
(target="ldap:/// $rootSuffix")
(targetattr="objectclass|mailalternateaddress|mailautoreplymode
|mailprogramdeliveryinfo|nswmextendeduserprefs|preferredlanguage
|maildeliveryoption|mailforwardingaddress
|mailAutoReplyTimeout|mailautoreplytextinternal|mailautoreplytext
|vacationEndDate|vacationStartDate|mailautoreplysubject|pabURI
```

```

| |maxPabEntries| |mailMessageStore| |mailSieveRuleSource| |sunUCDateFormat
| |sunUCDateDeLimiter| |sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Administrator Write Access
Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix");)

```

動作：合併計算。

此 ACI 授予傳訊一般使用者管理員群組權限。

```

-----
-----
#
# consolidate
#
aci:
(targetattr="uid| |ou| |owner| |mail| |mailAlternateAddress
| |mailEquivalentAddress| |memberOf
| |inetuserstatus| |mailuserstatus| |memberOfManagedGroup| |mailQuota
| |mailMsgQuota| |inetSubscriberAccountId| |dataSource| |mailhost
| |mailAllowedServiceAcces| |pabURI| |inetCOS| |mailSMTPSubmitChannel
| |aci")
(targetfilter= (&(objectClass=inetMailUser) (! (nsroledn=cn=Organization Admin
Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self");)

```

動作：合併計算。

這是多個設定自我權限的 ACI 其中之一。

分析如何合併計算 ACI

本節中的清單顯示在替代 `ldif` 檔案 (`replacement.acis.ldif`) 中合併計算的 ACI，您可以使用此檔案合併計算目錄中的 ACI。如需如何替代 ACI 的說明，請參閱「[替代 ACI 之步驟](#)」。

ACI 分為幾組。每一個類別中，先列出原始 ACI，然後是合併計算後的 ACI：

- [原始匿名存取權限](#)
- [合併計算的匿名存取權限](#)
- [原始自身 ACI](#)
- [合併計算自身 ACI](#)
- [原始 Messaging Server ACI](#)
- [合併計算 Messaging Server ACI](#)
- [原始社團組織管理員 ACI](#)
- [合併計算社團組織管理員 ACI](#)

原始匿名存取權限

```
aci:
(targetattr != "userPassword || passwordHistory ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordAllowChangeTime ")
(version 3.0; acl "Anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

```
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

```
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
```

```
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

```
aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*" )
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

```
aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*, $rootSuffix")
(targetattr = "*" )
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous
access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

合併計算的匿名存取權限

```
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr != "userPassword|passwordHistory
||passwordExpirationTime||passwordExpWarned||passwordRetryCount
||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
(version 3.0; acl "anonymous access rights";
allow (read,search,compare)
userdn = "ldap:///anyone"; )
```

分析：可匿名存取根，此根允許相同項並排除 aci 屬性。Access Manager 的這個替代會消除目標中昂貴的 (*)，因為它允許尾碼的匿名存取。

原始自身 ACI

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit
||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordHistory || passwordAllowChangeTime")
```

```
(version 3.0; aci "Allow self entry modification except for
nsroledn, aci, resource
limit attributes, passwordPolicySubentry and password policy state
attributes";
allow (write)
userdn ="ldap:///self";)
```

```
aci:
(targetattr = "*" )
(version 3.0; aci "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)
```

```
aci:
(targetattr = "objectclass || inetuserstatus ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list
|| iplanet-am-user-account-life ||
iplanet-am-session-max-session-time
|| iplanet-am-session-max-idle-time ||
iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions ||
iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn ||
iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-levelAdmin Role,$rootSuffix)))
(version 3.0; aci "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)
```

```
aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
||
sLookThroughLimit
|| nsSizeLimit || nsTimeLimit || nsIdleTimeout || memberOf ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
planet-am-web-agent-access-deny-list")
(version 3.0; aci "S1IS Allow self entry modification except for
nsroledn, aci,
and resource limit attributes";
allow (write)
userdn ="ldap:///self";)
```

```

aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; aci "S1IS Allow self entry read search except for
nsroledn, aci, resource
limit and web agent policy attributes";
allow (read,search)
userdn = "ldap:///self";)

aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress||mailEquiva
lent
address||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedService
Access
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=( &(objectClass=inetMailUser) (!(nsroledn=cn=Organizati
on Admin
ole,*))))
(version 3.0; aci "Deny write access to users over Messaging Server
protected
attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)

```

合併計算自身 ACI

```

aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
asswordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime
||
id || memberOf
|| objectclass || inetuserstatus || ou || owner || mail ||
mailuserstatus
|| memberOfManagedGroup ||mailQuota || mailMsgQuota || mailhost
|| mailAllowedServiceAccess || inetCOS || mailSMTPSubmitChannel")

```

```
(version 3.0; aci "Allow self entry modification";
allow (write)
userdn = "ldap:///self";)

aci:
(targetattr != " aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit || nsIdleTimeout")
(version 3.0; aci "Allow self entry read search";
allow (read,search)
userdn = "ldap:///self";)
```

分析：缺少全部的 `iplanet-am-*` 屬性。既然 `deny` 是沒有 ACI 時的預設值，那麼全部 `deny` ACI 都會移除。允許 `write` 的 ACI 都被合併計算成一個 ACI。

原始 Messaging Server ACI

```
aci:
(target="ldap:/// $rootSuffix")
(targetattr="*")
(version 3.0; aci "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group,
ou=Groups,
rootSuffix";)

aci:
(target="ldap:/// $rootSuffix")
(targetattr="objectclass || mailalternateaddress || mailautoreplymode ||
mailprogramdeliveryinfo
|| nswmextendeduserprefs || preferredlanguage || maildeliveryoption ||
mailforwardingaddress
|| mailAutoReplyTimeout || mailautoreplytextinternal || mailautoreplytex
t ||
vacationEndDate
|| vacationStartDate || mailautoreplysubject || pabURI || maxPabEntries ||
mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter ||
sunUCTimeFormat")
(version 3.0; aci "Messaging Server End User Administrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
```



```

allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group,
ou=Groups,
rootSuffix");

aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress||
mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota||
mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedService
Access
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization
Admin
Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected
attributes - product=SOMS,schema 2
support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self");

```

合併計算 Messaging Server ACI

在自身 ACI 中處理自身 ACI。

```

aci:
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read Only
Access";
allow (read,search)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix"; )

```

```

aci:
(targetattr="objectclass || mailalternateaddress ||
Mailautoreplymode ||
mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
|| mailforwardingaddress || mailAutoReplyTimeout ||

```

```

mailautoreplytextinternal
|| mailautoreplytext || vacationEndDate || vacationStartDate
|| mailautoreplysubject || maxPabEntries || mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
|| sunUCTimeFormat || mailuserstatus || maildomainstatus")
(version 3.0; acl "Messaging Server End User Administrator All
Access";
allow (all)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix");

```

分析：與原始 ACI 相同。

原始社團組織管理員 ACI

```

aci:(different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix");

```

```

aci:(missing)
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org
node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" );

```

```

aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix");

```

```

aci:
(target="ldap:///($dn), $rootSuffix")
(targetattr!="businessCategory || description ||
facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide ||
postOfficeBox ||
postalCode
|| registeredaddress || street || 1 || st || telephonenumber ||
maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role, ($dn), $rootSuffix" );

aci:(duplicate of per organization aci)
(target="ldap:///cn=Organization Admin Role, ($dn), $rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role, ($dn), $rootSuffix");

aci:
(target="ldap:///cn=Organization Admin
Role, ($dn), dc=red, dc=iplanet, dc=com")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role, ($dn), $rootSuffix");

aci:
(target="ldap:///o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin
Role,dc=red,dc=iplanet,dc=com))))
(targetattr = "nsroledn")
(targetattrfilters="add=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe
.com,
o=SharedDomainsRoot,o=Business,$rootSuffix),
del=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomai
nsRoot,
o=Business,$rootSuffix)")
(version 3.0;
acl "S1IS Organization Admin Role access allow";
allow (all)

```

```

roledn = "ldap:///cn=Organization Admin
Role,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,o=Business,
$rootSuffix";)

aci:
(target="ldap://($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,[$dn],dc=red,dc=iplanet,dc=com";)

```

合併計算社團組織管理員 ACI

```

aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)

aci:
(target="ldap://($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read";
allow(read,search)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix" ;)

aci:
(target="ldap://($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(entrydn=($dn),$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)

```

捨棄之未使用的 ACI 清單

本節中的清單顯示當您套用 `replacement.acis.ldif` 檔案至目錄上時，自此目錄捨棄而未使用的預設 ACI。

捨棄的 ACI 分為下列種類：

- 尾碼
- 頂層服務台管理員角色
- 頂層策略管理員角色
- Access Manager 匿名
- Access Manager 拒絕寫入存取
- Access Manager 容器管理員角色
- 社團組織服務台
- Access Manager 其他

尾碼

```
# discard
#
aci:
(targetattr = "*" )
(version 3.0;acl "Configuration Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot");)

#
# discard
#
aci:
(targetattr = "*" )
(version 3.0;acl "Directory Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Directory Administrators, $rootSuffix");)

#
# discard
#
aci:
(targetattr = "*" )
```

```
(version 3.0;
acl "SIE Group";
allow (all)
groupdn = "ldap:///cn=slapd-whater, cn=Sun ONE Directory Server,
cn=Server
Group, cn=whater.red.iplanet.com, ou=red.iplanet.com,
o=NetscapeRoot";)
```

```
#
# discard - prevents TLA from modifying the amldapuser account.
#
```

```
aci:
(target="ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix")
(targetattr = "*" )
(version 3.0;
acl "S1IS special ldap auth user modify right";
deny (write)
roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix";)
```

```
#
# discard - protects SAML related attributes
#
```

```
aci:
(targetattr="iplanet-am-saml-user || iplanet-am-saml-password")
(targetfilter="(objectclass=iplanet-am-saml-service)")
(version 3.0; acl "S1IS Right to modify saml user and password";
deny (all)
(roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix")
AND (userdn != "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix")
AND (userdn != "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"); )
```

頂層服務台管理員角色

```
#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*" )
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access
allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

```

#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access
allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)

```

頂層策略管理員角色

```

#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*" )
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)

```

```

#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*" )
(version 3.0; acl "S1IS Top-level Policy Admin Role access Auth
Service deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)

```

```

#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*" )

```

```
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix");

#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter="(objectclass=sunismangedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix");
```

Access Manager 匿名

```
#
# discard - prevents anyone other than rootdn from deleting default
organization.
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )

#
# discard - prevents any user other than rootdn from deleting the TLA
admin role.
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```


Access Manager 拒絕登入存取

```
#
# discard
#
aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn = "ldap:///cn=Deny Write Access,$rootSuffix";)
```

Access Manager 容器管理員角色

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)
```

```
#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)
```

```
#
# discard
#
aci:
(target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
```

```
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn =
"ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix");
```

社務組織服務台

```
#
# discard
#
aci:(extra verses dreambig)
(target="ldap:/// $rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*" )
(version 3.0; acl "S1IS Organization Help Desk Admin Role access
allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin
Role,$rootSuffix");

#
# discard
#
aci:
(target="ldap:/// $rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access
allow";
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin
Role,$rootSuffix");
```

Access Manager 其他

```
#
# discard - Removal disables the associated privileges to the
attribute
iplanetam-modifiable-by
#
aci:
(target="ldap:/// $rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he
creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

捨棄之未使用的 ACI 清單

字彙表

請參閱 Java Enterprise System 字彙表 (<http://docs.sun.com/doc/819-1936>)，以取得本文件集所使用字詞的完整清單。

A

- Access Manager 38
 - 記錄 150
- Application Server 7.x
 - 為 Delegated Administrator 進行配置 48
 - 重新啓動 55
 - 記錄 149
 - 配置選項 36
- Application Server 8.x
 - 為 Delegated Administrator 進行配置 50
 - 重新啓動 55
 - 記錄 149
 - 配置選項 37

B

- Bronze 服務等級範本 31

C

- Calendar Server
 - 配置 40
- cli-usrprefs.properties 檔案 55
- comm_dssetup.pl 39
- commadmin
 - 執行 57

- commadmin admin add 74
- commadmin admin remove 76
- commadmin admin search 77
- commadmin domain create 78
- commadmin domain delete 81
- commadmin domain modify 83
- commadmin domain purge 85
- commadmin domain search 87
- commadmin group create 89
- commadmin group delete 91
- commadmin group modify 93
- commadmin group search 96
- commadmin resource create 98
- commadmin resource delete 101
- commadmin resource modify 102
- commadmin resource search 104
- commadmin user create 106
- commadmin user delete 108
- commadmin user modify 110
- commadmin user search 114
- Communications Services
 - 文件 12
- config-commda 43
- CoS 套裝軟體的預設範本 28
- CoS 範本範例 28
 - 郵件服務的提供方式 31
- CoS 範本範例中的郵件服務 31
- cos.default.ldif 28
- cos.sample.ldif 28
- cscal 101

csresource 100

D

da.cos.skeleton.ldif 檔案 59

da.log 檔案 56, 147

da.provider.skeleton.ldif 131

da.sample.data.ldif 檔案
描述 138
提供的社團組織 136

da_base 38

daconfig.properties 檔案
位置 56

DC 樹的根尾碼
新增相容性模式的 ACI 62

defaultmail 範本 28

Delegated Administrator
LDAP 物件類別 17
LDAP 屬性 17
元件 33
安裝目錄 38
配置程式 43

Delegated Administrator 公用程式
cli-usrprefs.properties 55
配置 45
配置檔 55
執行 57
描述 16

Delegated Administrator 主控台
daconfig.properties 56
配置 46
配置檔 56
啓動 57
描述 16
登入 57

Delegated Administrator 伺服器
resource.properties 檔案 55
記錄檔 148
配置 51
配置檔 55

Diamond 服務等級範本 32

Directory Server
記錄 150

Directory Server 設定程序檔 39

E

Emerald 服務等級範本 32

G

Gold 服務等級範本 31

I

inetCOS 屬性 30

inetdomain 物件類別 64

iPlanet Delegated Administrator
管理員角色 25
與目前的 Delegated Administrator 比較 25

J

Java Enterprise System 安裝程式 37

jdapi-mailhoststoreplugin 68

jdapi-volinternalloginplugin 69

L

LDAP 物件類別和屬性 17

ldapmodify
用來建立服務套裝軟體 61
使用來建立提供者社團組織 131

Linux, 預設基底目錄用於 10
 logger.properties 檔案 148
 loginAuth-idAttr 特性 69

M

mailAllowedServiceAccess 26
 MailDomainReportAddressPlugin 67
 MailHostStorePlugin 67
 mailMsgMaxBlocks 26
 mailMsgQuota 26
 mailQuota 26
 Messaging Server
 文件 11
 配置 40

O

ObjectclassPlugin 67

P

Platinum 服務等級範本 31

R

resource.properties 檔案
 位置 55
 新增外掛程式 67
 新增使用者登入值 69
 rootSuffix 參數 60
 Ruby 服務等級範本 32

S

saveState 檔案 56
 Schema 2 相容性模式
 新增 ACI 61
 Security.properties 檔案
 位置 65
 移除喜好的郵件主機 65
 Silver 服務等級範本 31
 Solaris
 支援 13
 修補程式 13
 Sun Java System Calendar Server
 配置 40
 Sun Java System Messaging Server
 配置 40

U

UidPlugin 67

V

VollInternalLoginPlugin 67

W

Web Server
 為 Delegated Administrator 進行配置 47
 重新啓動 55
 記錄 149
 Web Servre
 配置選項 35

三書

- 三層次階層
 - 目錄資訊樹 124, 138
 - 簡介 19
 - 邏輯檢視 118

七書

- 支援
 - Solaris 13
- 文件
 - Communications Services 文件所在位置 12
 - Messaging Server 文件所在位置 11

工書

- 外掛程式
 - MailDomainReportAddressPlugin 67
 - MailHostStorePlugin 67
 - ObjectclassPlugin 67
 - UidPlugin 67
 - VollInternalLoginPlugin 67
- 新增 66
- 目錄資訊樹
 - 三層次階層 137
 - 自訂服務提供者範本 123
 - 單層次階層 21, 22
 - 雙層次階層 23

六書

- 共用社團組織
 - 描述 122
- 安裝 Access Manager 38
- 安裝 Java Enterprise System 37
- 自訂
 - 使用者登入 69

- 自訂服務提供者範本
 - ldif 檔案 131
 - 定義 131
 - 建立 SPA 122
 - 建立的社團組織 123
 - 建立提供者社團組織 130
- 行事曆服務
 - 新增到預設網域 58

一書

- 完整社團組織
 - 描述 122

八書

- 使用者登入
 - 自訂 69
- 服務套裝軟體
 - 可用的郵件服務 26
 - 定義 25
 - 建立您自己的 59
- 服務提供者管理員
 - 所管理的社團組織 121
 - 建立 122
 - 指定給一個使用者 120
 - 描述 119
 - 簡介 117
- 服務等級套裝軟體
 - Bronze 31
 - Diamond 32
 - DIT 中的位置 30
 - Emerald 32
 - Gold 31
 - Platinum 31
 - Ruby 32
 - Silver 31
 - 建立 58
 - 建立服務套裝軟體的範本 59
 - 預設範本 28

- 範本 27
- 範本範例 28
- 社團組織管理員
 - 執行作業的方式 24
 - 描述 24

I 書

- 建立資源 100
- 指令行公用程式
 - commadmin admin add 74
 - commadmin admin remove 76
 - commadmin admin search 77
 - commadmin domain create 78
 - commadmin domain delete 81
 - commadmin domain modify 83
 - commadmin domain purge 85
 - commadmin domain search 87
 - commadmin group create 89
 - commadmin group delete 91
 - commadmin group modify 93
 - commadmin group search 96
 - commadmin resource create 98
 - commadmin resource delete 101
 - commadmin resource modify 102
 - commadmin resource search 104
 - commadmin user create 106
 - commadmin user delete 108
 - commadmin user modify 110
 - commadmin user search 114
 - 執行 57

十書

- 時區 143
- 特性名稱 141, 147
- 記錄檔
 - da.log 56, 147
 - logger.properties 檔案 147
- 配置 Calendar Server 40

- 配置 Messaging Server 40
- 配置後作業 58
- 配置程式 43
- 配置資訊
 - Application Server 7.x 36
 - Application Server 8.x 37
 - Web Server 35
 - 必要的選項 35
- 除錯 servlet 148

十一書

- 頂層管理員
 - 執行作業的方式 23
 - 描述 23

十二書

- 喜好的郵件主機
 - 配置 65
 - 從主控台移除 65
- 單層次階層 17
- 提供者社團組織
 - 建立 122
 - 建立之步驟 130
 - 描述 121
- 無訊息安裝 56
- 登入 Delegated Administrator 57
- 郵件服務
 - 新增到預設網域 58

十三書

- 資源
 - 建立 100

十三 部分

十三 畫

範例服務提供者社團組織

描述 [136](#)

範本所提供的社團組織 [136](#)

十八 畫

雙層次階層 [18](#)