Sun Java System Access Manager 7 2005Q4 管理指南

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

文件號碼：819–3483

060420@14774

目錄

前言

「Sun Java System Access Manager 7 2005Q4 管理指南」描述如何使用 Sun Java™ System Access Manager 主控台，以及如何透過指令行介面管理使用者和服務。

Access Manager 是 Sun Java Enterprise System (Java ES) 的元件，它是一組軟體元件，提供支援分散於整個網路或網際網路環境之企業應用程式所需的服務。

本書的適用對象

本書的適用對象爲使用 Sun Java System 伺服器與軟體實作網路存取平台的 IT 管理員與軟體開發人員。

閱讀本書之前

讀者應熟悉下列元件與概念：

- 如「Sun Java System Access Manager 7 2005Q4 Technical Overview」中描述之 Access Manager 技術方面的概念。
- 部署平台：Solaris™ 或 Linux 作業系統
- 可執行 Access Manager 的 Web 容器：Sun Java System Application Server、Sun Java System Web Server、BEA WebLogic 或 IBM WebSphere Application Server
- 技術方面的概念：Lightweight Directory Access Protocol (LDAP)、Java 技術、JavaServer Pages (JSP) 技術、HyperText Transfer Protocol (HTTP)、HyperText Markup Language (HTML) 及 eXtensible Markup Language (XML)

相關書籍

可用相關文件如下：

- 第 14 頁的 「Access Manager 核心文件」
- 第 14 頁的 「Sun Java Enterprise System 產品文件」

Access Manager 核心文件

「Access Manager 核心文件集」包含下列標題：

- 產品上市後，可於線上取得「Sun Java System Access Manager 7 2005Q4 版本說明」。其匯集了各類最新資訊，包括目前版本中新功能的描述、已知問題和限制、安裝注意事項及如何報告軟體或文件的問題。
- 「Sun Java System Access Manager 7 2005Q4 Technical Overview」提供 Access Manager 元件如何一同運作以整合存取控制功能，及保護企業資產和於網路環境中使用的應用程式之簡介。它同時會說明 Access Manager 的基本概念與詞彙。
- 「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」以解決方案生命週期爲根據，提供規劃和部署 Sun Java System Access Manager 的解決方案。
- 「Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide」提供有關如何調校 Access Manager 及其相關元件以取得最佳效能的資訊。
- 「Sun Java System Access Manager 7 2005Q4 管理指南」描述如何使用 Access Manager 主控台，及如何透過指令行介面管理使用者和服務資料。
- 「Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide」提供以 Liberty Alliance Project 規格爲基準的聯合模組之相關資訊。它包含以這些規格爲基準的整合性服務之相關資訊、啓用基於 Liberty 的環境之說明指示及用於延伸架構的應用程式設計介面 (API) 之摘要。
- 「Sun Java System Access Manager 7 2005Q4 Developer's Guide」提供如何自訂 Access Manager 和整合其功能與組織的現行技術基礎架構之相關資訊。它還包含有關此產品及其 API 之程式方面的詳細資訊。
- 「Sun Java System Access Manager 7 2005Q4 C API Reference」提供組成公用 Access Manager C API 的資料類型、結構及功能之摘要。
- 「Java API Reference」(文件號碼 819-2141) 提供於 Access Manager 中實作 Java 套裝軟體的相關資訊。
- 「Sun Java System Access Manager Policy Agent 2.2 User's Guide」簡介 Access Manager 可用的策略功能和策略代理程式。

「版本說明」的更新內容與和核心文件修正之連結，可在 Sun Java Enterprise System 文件網站的 Access Manager 頁面中找到。已更新的說明文件標示有修訂日期。

Sun Java Enterprise System 產品文件

可在下列產品的文件中找到有用的資訊：

- Directory Server
- Web Server
- Application Server
- Web Proxy Server

相關的協力廠商網站參考

本文件提供了協力廠商的 URL 及其他相關資訊做爲參考。

備註 – 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。

文件、支援與訓練

Sun 功能	URL	說明
文件	http://www.sun.com/documentation/	下載 PDF 與 HTML 文件，以及訂購書面列印的文件
支援與訓練	http://www.sun.com/supportraining/	取得技術支援、下載修補程式與 Sun 培訓課程的資訊

印刷排版慣例

下表描述本書在印刷排版上所作的變更。

表 P–1 印刷排版慣例

字體或符號	意義	範例
`AaBbCc123`	指令、檔案及目錄的名稱；螢幕畫面輸出	請編輯您的 `.login` 檔案。 請使用 `ls -a` 列出所有檔案。 `machine_name% you have mail.`
`AaBbCc123`	您所鍵入的內容 (與螢幕畫面輸出相區別)	`machine_name%` **`su`** `Password:`
aabbcc123	預留位置：用實際的名稱或數值取代	移除檔案的指令是 `rm` *filename*。

表 P–1 印刷排版慣例 *(續)*

字體或符號	意義	範例
AaBbCc123	書名、新的術語以及要強調的術語	請參閱「使用者指南」中的第 6 章。 請執行 *patch analysis*。 請不要儲存此檔案。 [請注意某些重點項目在線上以粗體顯示。]

指令範例中的 Shell 提示符號

下表顯示用於 C shell、Bourne shell 和 Korn shell 的預設系統提示符號以及超級使用者提示符號。

表 P–2 提示

Shell	提示符號
C shell 提示符號	`machine_name%`
C shell 超級使用者提示符號	`machine_name#`
Bourne shell 和 Korn shell 提示符號	`$`
Bourne shell 和 Korn shell 超級使用者提示符號	`#`

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。

請至下列網址提出您對本文件的意見：`http://docs.sun.com`，並按一下 [Send Comments (傳送您的意見)]。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，本書的書名爲「Sun Java System Access Manager 7 2005Q4 管理指南」，其文件號碼爲 819-3483。提出意見時您還需要在表格中輸入此文件的英文標題和文件號碼。例如，本文件的英文文件號碼爲 819-2137，完整標題爲「Sun Java System Access Manager 7 2005Q4 Administration Guide」。

第 I 部分

Access Manager 配置

這是「Sun Java System Access Manager™ 7 2005Q4 管理指南」的第一部分。討論安裝 Access Manager 後您可以執行的配置選項。本部分包含以下章節：

◆ ◆ ◆ 第 1 章

Access Manager 7 2005Q4 配置程序檔

本章描述如何使用 amconfig 程序檔以及範例無訊息模式輸入檔案 (amsamplesilent) 來配置及部署 Sun Java™ System Access Manager。主題包括：

Access Manager 7 2005Q4 安裝簡介

對於新安裝，始終透過執行 Sun Java Enterprise System (Java ES) 安裝程式安裝 Access Manager 7 2005Q4 的第一個實例。執行安裝程式時，可以選擇下列的配置選項之一：

- [立即配置] 選項可藉由在 Access Manager 安裝面板上所做的選擇 (或預設值)，讓您於安裝期間安裝與配置第一個實例。
- [以後配置] 選項會安裝 Access Manager 7 2005Q4 元件，在安裝之後，您必須對其進行手動配置，或如同第 33 頁的 「配置與重新配置 Access Manager 實例」中的描述來執行 Access Manager 程序檔。如果選擇此選項，將不會配置您目前安裝的任何產品。例如，如果選擇要安裝 Access Manager 和 Application Server，並選取 [以後配置] 選項，那麼這兩個應用程式都不會配置。

備註 – 如果您將 BEA WebLogic 或 IBM WebSphere Application Server 安裝爲 Access Manager Web 容器，則安裝 Access Manager 時必須選擇 [以後配置] 選項。請參閱第 2 章以取得更多資訊。

如需有關此安裝程式的資訊，請參閱「Sun Java Enterprise System 2005Q4 Installation Guide for UNIX」。

Java Enterprise System 安裝程式會將 Access Manager 7 2005Q4 amconfig 程序檔和範例無訊息模式輸入檔案 (amsamplesilent) 安裝在 *AccessManager-base*/SUNWam/bin 目錄 (Solaris 系統) 或 *AccessManager-base*/identity/bin 目錄 (Linux 系統)。

AccessManager-base 代表 Access Manager 基底安裝目錄。在 Solaris 系統上，預設基底安裝目錄是 /opt，在 Linux 系統上，則是 /opt/sun。不過，執行安裝程式時您可以決定指定另一個目錄。

amconfig 程序檔爲最高層程序檔，可視需要呼叫其他程序檔，以執行請求的作業。如需更多資訊，請參閱第 30 頁的 「Access Manager amconfig 程序檔」。

範例配置程序檔輸入檔案 (amsamplesilent) 是一個可用來建立輸入檔案的範本，當您以無訊息模式執行 amconfig 程序檔時必須指定此輸入檔案。

這個範例配置程序檔輸入檔案是 ASCII 文字檔案，其中包含 Access Manager 配置變數。執行 amconfig 程序檔之前，請複製 (並重新命名，如果需要的話) amsamplesilent 檔案，然後根據系統環境來編輯檔案中的變數。配置變數格式如下：

```
variable-name=value
```

例如：

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
 SERVER_HOST=ishost.example.com
```

如需可在配置程序檔輸入檔案中設定的變數清單，請參閱第 21 頁的 「Access Manager 範例配置程序檔輸入檔案」。

注意 – 當您以無訊息模式執行 amconfig 程序檔時，所使用範例配置程序檔輸入檔案的格式並未遵循相同的格式，或必須使用相同的變數名稱做爲 Java Enterprise System 無訊息安裝狀態檔案。這個檔案中包含機密資料，例如管理員密碼。視需要確實保護或刪除這個檔案。

Access Manager amconfig 程序檔作業

以 Sun Java Enterprise System 安裝程式安裝 Access Manager 的第一個實例後，可執行 amconfig 程序檔，依無訊息模式輸入檔案中的變數值執行以下作業：

- 部署和配置 Access Manager 的第一個實例或在相同主機系統上部署和配置 Access Manager 的附加實例。例如，當您配置 Web 容器的附加實例後，您可以爲該 Web 容器實例部署並配置新的 Access Manager 實例。
- 重新配置 Access Manager 第一個實例和任何附加實例。
- 部署並配置 Access Manager 完整伺服器服務，或僅部署並配置可啓用下列產品支援的 SDK 服務：
  - BEA WebLogic

- IBM WebSphere Application Server

部署並配置特定 Access Manager 元件，例如主控台或聯合管理模組。

- 解除安裝您以 `amconfig` 程序檔部署的 Access Manager 實例和元件。

Access Manager 範例配置程序檔輸入檔案

當您執行 Java Enterprise System 安裝程式後，可以在 Solaris 系統中的 *AccessManager-base*`/SUNWam/bin` 目錄，或 Linux 系統中的 *AccessManager-base*`/identity/bin` 目錄找到 Access Manager 範例配置程序檔輸入檔案 (`amsamplesilent`)。

若要設定配置變數，先複製並重新命名 `amsamplesilent` 檔案。然後爲您要執行的作業在副本中設定變數。如需此檔案的範例，請參閱第 35 頁的 「範例配置程序檔輸入檔案」。

此範例無訊息模式輸入檔案包含以下配置變數：

- 第 21 頁的 「配置模式變數」
- 第 22 頁的 「Access Manager 配置變數」
- 第 25 頁的 「Web 容器配置變數」
- 第 29 頁的 「Directory Server 配置變數」

配置模式變數

本節說明必要 DEPLOY_LEVEL 變數的值。此變數決定您要 `amconfig` 程序檔執行的作業。

表 1–1 變數

作業	DEPLOY_LEVEL 變數值和說明
安裝	1 = 新實例的完整 Access Manager 安裝 (預設) 2 = 僅安裝 Access Manager 主控台 3 = 僅安裝 Access Manager SDK 4 = 僅安裝 SDK 並配置容器 5 = 僅安裝聯合管理模組 6 = 限安裝伺服器 7=安裝 Access Manager 並配置容器，以與 Portal Server 一起部署。 警告 DEPLOY_MODE=7 僅用於與 Portal Server 一起部署的 Access Manager。 在部份部署中，您可能想使用不同的 Web 容器在單一主機上只安裝主控台和伺服器。首先，執行 Java ES 安裝程式，使用 [以後配置] 選項安裝所有的 Access Manager 子元件。然而，執行 `amconfig` 程序檔配置主控台和伺服器。
解除安裝 (取消配置)	11 = 完全解除安裝 12 = 完全解除安裝主控台 13 = 僅解除安裝 SDK 14 = 僅解除安裝 SDK 並取消配置容器 15 = 解除安裝聯合管理模組 16 = 僅解除安裝伺服器 與 Portal Server 一起部署時，解除安裝 Access Manager 並取消配置容器。 警告 DEPLOY_MODE=7 僅用於與 Portal Server 一起部署 Access Manager 時。
重新安裝 (也稱爲重新部署或重新配置)	21 = 重新部署所有主控台、密碼、服務和共用 Web 應用程式。 26 = 取消部署所有主控台、密碼、服務和共用 Web 應用程式。

Access Manager 配置變數

本節說明 Access Manager 配置變數。

表 1–2 Access Manager 配置變數

變數	說明
AM_REALM	指定 Access Manager 模式： ■ enabled：Access Manager 使用 Access Manager 7 2005Q4 功能與主控台，在「範圍模式」中作業。 ■ disabled：Access Manager 使用 Access Manager 6 2005Q1 功能與主控台，在「舊有模式」中作業。 預設：enabled **注意 –** 依預設會啓用 Access Manager 範圍模式。若您與 Portal Server、Messaging Server、Calendar Server、Delegated Administrator 或 Instant Messaging 一起部署 Access Manager，則在執行 `amconfig` 程序檔前必須先選取「舊有模式」(AM_REALM=disabled)。
BASEDIR	Access Manager 套裝軟體的基底安裝目錄。 預設：PLATFORM_DEFAULT Solaris 系統中，PLATFORM_DEFAULT 爲 `/opt` Linux 系統中，PLATFORM_DEFAULT 爲 `/opt/sun`
SERVER_HOST	完全合格的系統主機名稱，此系統會執行或安裝 Access Manager。 對於遠端 SDK 安裝，請將此變數設爲安裝或即將安裝 Access Manager 的主機，而非遠端用戶端主機。 此變數應符合 Web 容器配置中的對等變數。例如，對於 Application Server 8，此變數應符合 AS81_HOST。
SERVER_PORT	Access Manager 連接埠號。預設：58080 對於遠端 SDK 安裝，請將此變數設爲安裝或即將安裝 Access Manager 的主機上的連接埠，而非遠端用戶端主機。 此變數應符合 Web 容器配置中的對等變數。例如，對於 Application Server 8，此變數應符合 AS81_PORT。
SERVER_PROTOCOL	伺服器通訊協定：http 或 https。預設：http 對於遠端 SDK 安裝，請將此變數設爲安裝或即將安裝 Access Manager 的主機上的通訊協定，而非遠端用戶端主機。 此變數應符合 Web 容器配置中的對等變數。例如，對於 Application Server 8，此變數應符合 AS81_PROTOCOL。
CONSOLE_HOST	安裝現有主控台的伺服器之完全合格的主機名稱。 預設：提供給 Access Manager 主機的值
CONSOLE_PORT	安裝主控台並偵聽連結的 Web 容器連接埠。 預設：提供給 Access Manager 連接埠的值

表 1–2 Access Manager 配置變數 *(續)*

變數	說明
CONSOLE_PROTOCOL	安裝主控台的 Web 容器之通訊協定。 預設：伺服器通訊協定
CONSOLE_REMOTE	如果主控台對 Access Manager 服務而言是遠端的，設爲 true。否則，設爲 false。預設：false
DS_HOST	Directory Server 完全合格的主機名稱。
DS_PORT	Directory Server 連接埠。預設：389。
DS_DIRMGRDN	目錄管理員 DN：對 Directory Server 擁有無限存取權的使用者。 預設：「`cn=Directory Manager`」
DS_DIRMGRPASSWD	目錄管理員密碼 請參閱第 22 頁的 「Access Manager 配置變數」描述中關於特殊字元的備註。
ROOT_SUFFIX	目錄的初始或根字尾。您必須確定此值存在於您所使用的 Directory Server 中。 請參閱第 22 頁的 「Access Manager 配置變數」描述中關於特殊字元的備註。
ADMINPASSWD	管理員 (`amadmin`) 的密碼。必須與 `amldapuser` 密碼不同。 備註：如果密碼包含特殊字元如斜線 (/) 或反斜線 (\\)，特殊字元必須加上單括號 (”)。例如： `ADMINPASSWD='\\\\\\\\\\\####///'` 然而，密碼不能將單括號做爲實際密碼字元之一。
AMLDAPUSERPASSWD	`amldapuser` 的密碼。必須與 `amadmin` 密碼不同。 請參閱第 22 頁的 「Access Manager 配置變數」描述中關於特殊字元的備註。
CONSOLE_DEPLOY_URI	用於存取與 Access Manager 管理主控台子元件相關聯的 HTML 頁面、類別以及 JAR 檔案的 URI 前綴。 預設：`/amconsole`
SERVER_DEPLOY_URI	用於存取和識別管理與策略服務核心子元件相關聯的 HTML 頁面、類別以及 JAR 檔案的 URI 前綴。 預設：`/amserver`
PASSWORD_DEPLOY_URI	該 URI 用於決定將由執行 Access Manager 的 Web 容器用在您指定的字串與相應已部署應用程式之間的對映。 預設：`/ampassword`

表 1–2 Access Manager 配置變數 (續)

變數	說明
COMMON_DEPLOY_URI	用於在 Web 容器上存取共用網域服務的 URI 前綴。 預設：/amcommon
COOKIE_DOMAIN	當 Access Manager 授予使用者階段作業 ID 時，傳回到瀏覽器的可信任 DNS 網域之名稱。至少要提供一個值。一般而言，此格式爲以點號開頭的伺服器網域名稱。 範例：.example.com
JAVA_HOME	JDK 安裝目錄的路徑。預設：/usr/jdk/entsys-j2se。此變數提供指令行介面 (如 amadmin) 之可執行檔使用的 JDK。此版本必須是 1.4.2 或更高版本。
AM_ENC_PWD	密碼加密金鑰：Access Manager 用來加密使用者密碼的字串。預設：無。將值設爲 none 時，amconfig 會爲使用者產生密碼加密金鑰，因此密碼加密將會存在於使用者指定或經由 amconfig 建立的安裝中。 重要：如果部署多個 Access Manager 或遠端 SDK 實例，所有實例將使用相同的密碼加密金鑰。當您部署附加實例時，從第一個實例之 AMConfig.properties 檔案中的 am.encryption.pwd 特性複製值。
PLATFORM_LOCALE	平台的語言環境。預設：en_US (美國英語)
NEW_OWNER	安裝後 Access Manager 檔案的新所有者。預設：root
NEW_GROUP	安裝後 Access Manager 檔案的新群組。預設：other 對於 Linux 安裝，將 NEW_GROUP 設爲 root。
PAM_SERVICE_NAME	來自 PAM 配置或作業系統隨附之堆疊的 PAM 服務名稱，用於 Unix 認證模組 (一般而言，對於 Solaris 是 other，對於 Linux 是 password)。預設：other。
XML_ENCODING	XML 編碼。預設：ISO-8859-1
NEW_INSTANCE	指定配置程序檔是否應部署 Access Manager 到一個使用者建立的新 Web 容器實例： ■ true = 將 Access Manager 部署到現存實例以外的使用者新建 Web 容器實例。 ■ false = 配置第一個實例或重新配置實例。 預設：false
SSL_PASSWORD	不是用於此版本中。

Web 容器配置變數

若要指定 Access Manager 的 Web 容器，請在無訊息模式輸入檔案中設定 WEB_CONTAINER 變數。如需 Access Manager 7 2005Q4 支援的 Web 容器版本資訊，請參閱「Sun Java System Access Manager 7 2005Q4 版本說明」。

表 1–3 Access Manager WEB_CONTAINER 變數

值	Web 容器
WS6 (預設)	第 26 頁的 「Sun Java System Web Server 6.1 SP5」
AS8	第 27 頁的 「Sun Java System Application Server 8.1」
WL8	第 28 頁的 「BEA WebLogic Server 8.1」
WAS5	第 29 頁的 「IBM WebSphere 5.1」

Sun Java System Web Server 6.1 SP5

本節說明 Web Server 6.1 2005Q4 SP5 無訊息模式輸入檔案中的配置變數。

表 1–4 Web Server 6.1 配置變數

變數	說明
WS61_INSTANCE	將部署或取消部署 Access Manager 的 Web Server 實例名稱。 預設：https-*web-server-instance-name* 其中 *web-server-instance-name* 是 Access Manager 主機 (第 22 頁的 「Access Manager 配置變數」變數)
WS61_HOME	Web Server 基底安裝目錄。 預設：`/opt/SUNWwbsvr`
WS61_PROTOCOL	將部署 Access Manager 的 Web Server 實例使用之通訊協定，由第 26 頁的 「Sun Java System Web Server 6.1 SP5」變數設定：http 或 https。 預設：Access Manager 通訊協定 (第 22 頁的 「Access Manager 配置變數」變數)
WS61_HOST	Web Server 實例之完全合格的主機名稱 (第 26 頁的 「Sun Java System Web Server 6.1 SP5」變數)。 預設：Access Manager 主機實例 (第 22 頁的 「Access Manager 配置變數」變數)
WS61_PORT	Web Server 偵聽連線時所在的連接埠。 預設：Access Manager 連接埠號 (第 22 頁的 「Access Manager 配置變數」變數)
WS61_ADMINPORT	Web Server Administration Server 偵聽連線時所在的連接埠。 預設：8888
WS61_ADMIN	Web Server 管理員的使用者 ID。 預設：「`admin`」

Sun Java System Application Server 8.1

本節說明 Application Server 8.1 無訊息模式輸入檔案中的配置變數。

表 1–5 Application Server 8.1 配置變數

變數	說明
AS81_HOME	Application Server 8.1 安裝目錄的路徑。 預設：`/opt/SUNWappserver/appserver`
AS81_PROTOCOL	Application Server 實例使用的通訊協定：http 或 https。 預設：Access Manager 通訊協定 (第 22 頁的 「Access Manager 配置變數」變數)
AS81_HOST	Application Server 實例偵聽連線時所在之完全合格的網域名稱。 預設：Access Manager 主機 (第 22 頁的 「Access Manager 配置變數」變數)
AS81_PORT	Application Server 實例偵聽連線時所在的連接埠。 預設：Access Manager 連接埠號 (第 22 頁的 「Access Manager 配置變數」變數)
AS81_ADMINPORT	Application Server 的管理伺服器偵聽連線時所在的連接埠。 預設：4849
AS81_ADMIN	爲 Application Server 所顯示網域管理 Application Server 管理伺服器的使用者名稱。 預設：`admin`
AS81_ADMINPASSWD	Application Server 所顯示網域的 Application Server 管理員密碼。 請參閱第 22 頁的 「Access Manager 配置變數」描述中關於特殊字元的備註。
AS81_INSTANCE	要執行 Access Manager 的 Application Server 實例的名稱。 預設：`server`
AS81_DOMAIN	您要將此 Access Manager 實例部署至的網域之 Application Server 目錄路徑。 預設：`domain1`
AS81_INSTANCE_DIR	Application Server 儲存實例檔案的目錄路徑。 預設：`/var/opt/SUNWappserver/domains/domain1`
AS81_DOCS_DIR	Application Server 儲存內容文件的目錄。 預設：`/var/opt/SUNWappserver/domains/domain1/docroot`

表 1–5 Application Server 8.1 配置變數 *(續)*

變數	說明
AS81_ADMIN_IS_SECURE	指定 Application Server 管理實例是否正在使用 SSL： ■ true：已經啓用安全連接埠協定 (HTTPS 通訊協定)。 ■ false：未啓用安全連接埠協定 (HTTP 通訊協定)。 預設：true (已啓用) 在 `ampsamplesilent` 中，另有一個設定可指定 Application Server 管理連接埠是否安全： ■ true：Application Server 管理連接埠安全 (HTTPS 通訊協定)。 ■ false：Application Server 管理連接埠不安全 (HTTP 通訊協定)。 預設：true (已啓用)。

BEA WebLogic Server 8.1

本節說明 BEA WebLogic Server 8.1 於無訊息模式輸入檔案中的配置變數。

表 1–6 BEA WebLogic Server 8.1 配置變數

變數	說明
WL8_HOME	WebLogic 主目錄。預設：`/usr/local/bea`
WL8_PROJECT_DIR	WebLogic 專案目錄。預設：`user_projects`
WL8_DOMAIN	WebLogic 網域名稱。預設：`mydomain`
WL8_SERVER	WebLogic 伺服器名稱。預設：`myserver`
WL8_INSTANCE	WebLogic 實例名稱。預設：`/usr/local/bea/weblogic81 ($WL8_HOME/weblogic81)`
WL8_PROTOCOL	WebLogic 通訊協定。預設：http
WL8_HOST	WebLogic 主機名稱。預設：伺服器主機名稱
WL8_PORT	WebLogic 連接埠。預設：7001
WL8_SSLPORT	WebLogic SSL 連接埠。預設：7002
WL8_ADMIN	WebLogic 管理員。預設：「`weblogic`」
WL8_PASSWORD	WebLogic 管理員密碼。 請參閱第 22 頁的 「Access Manager 配置變數」描述中關於特殊字元的備註。
WL8_JDK_HOME	WebLogic JDK 主目錄。預設：第 28 頁的 「BEA WebLogic Server 8.1」 `/jdk142_04`
WL8_CONFIG_LOCATION	應設爲 WebLogic 啓動程序檔之位置的父系目錄。

IBM WebSphere 5.1

本節說明 IBM WebSphere Server 5.1 無訊息模式輸入檔案中的配置變數。

表 1–7 IBM WebSphere 5.1 配置變數

變數	說明
WAS51_HOME	WebSphere 主目錄。預設：`/opt/WebSphere/AppServer`
WAS51_JDK_HOME	WebSphere JDK 主目錄。預設：`/opt/WebSphere/AppServer/java`
WAS51_CELL	WebSphere 儲存格。預設：主機名稱值
WAS51_NODE	WebSphere 節點名稱。預設：安裝 WebSphere 的伺服器之主機名稱。預設：主機名稱值
WAS51_INSTANCE	WebSphere 實例名稱。預設：`server1`
WAS51_PROTOCOL	WebSphere 通訊協定。預設：http
WAS51_HOST	WebSphere 主機名稱。預設：伺服器主機名稱
WAS51_PORT	WebSphere 連接埠。預設：9080
WAS51_SSLPORT	WebSphere SSL 連接埠。預設：9081
WAS51_ADMIN	WebSphere 管理員。預設：「`admin`」
WAS51_ADMINPORT	WebSphere 管理員連接埠。預設：9090

Directory Server 配置變數

如需 Access Manager 7 2005Q4 支援的 Directory Server 版本資訊，請參閱「Sun Java System Access Manager 7 2005Q4 版本說明」。本節說明無訊息模式輸入檔案中的 Directory Server 配置變數。

表 1–8 Directory Server 配置變數

變數	說明
DIRECTORY_MODE	Directory Server 模式： 1 = 用於目錄資訊樹 (DIT) 的新安裝。 2 = 用於現有 DIT。命名屬性和物件類別相同，因此配置程序檔載入 `installExisting.ldif` 以及 `umsExisting.ldif` 檔案。 配置程序檔也以配置時實際輸入的值 (例如，BASE_DIR、BASE_DIR 及 ROOT_SUFFIX) 更新 LDIF 以及特性檔案。 此更新亦稱爲「標記交換」，因爲配置程序檔以實際配置值取代檔案中的定位字元標記。 3 = 當您希望以手動載入時用於現有 DIT。命名屬性和物件類別不同，因此配置程序檔不會載入 `installExisting.ldif` 以及 `umsExisting.ldif` 檔案。程序檔進行標記交換 (如模式 2 所述)。 您必須檢查並修改 (視需要) LDIF 檔案後手動載入 LDIF 檔案和服務。 4 = 用於現有多重伺服器安裝。配置程序檔不會載入 LDIF 檔案和服務，因爲該作業是根據現有 Access Manager 安裝。程序檔僅進行標記交換 (如模式 2 所述)，並新增平台清單中的一個伺服器項目。 5 = 用於現有升級。程序檔僅進行標記交換 (如模式 2 所述)。 預設：1
USER_NAMING_ATTR	使用者命名屬性：使用者或資源於其相關明稱空間中的專屬辨識符號。預設：`uid`
ORG_NAMING_ATTR	使用者之公司或組織的命名屬性。預設：`o`
ORG_OBJECT_CLASS	組織物件類別。預設：`sunismanagedorganization`
USER_OBJECT_CLASS	使用者物件類別。預設：`inetorgperson`
DEFAULT_ORGANIZATION	預設的組織名稱。預設：無

Access Manager amconfig 程序檔

執行 Java Enterprise System 安裝程式後，`amconfig` 程序檔位於 *AccessManager-base*`/SUNWam/bin` 目錄中 (Solaris 系統) 或 *AccessManager-base*`/identity/bin` 目錄中 (Linux 系統)。

`amconfig` 程序檔讀取無訊息配置輸入檔案，然後視需要以無訊息模式呼叫其他程序檔，以執行請求的作業。

若要執行 `amconfig` 程序檔，請使用此語法：

```
amconfig -s
          input-file
```

其中：

-s 於無訊息模式中執行 `amconfig`。

`input-file` 是無訊息配置輸入檔案，包含您要執行作業的配置變數。如需更多資訊，請參閱第 21 頁的 「Access Manager 範例配置程序檔輸入檔案」。

執行 `amconfig` 程序檔有幾個注意事項：

- 您必須以超級使用者 (`root`) 執行。
- 指定 `amsamplesilent` 檔 (或檔案副本) 的完整路徑。例如：

```
# cd /opt/SUNWam/bin
# ./amconfig -s ./amsamplesilent
```

或

```
# ./amconfig -s /opt/SUNWam/bin/amsamplesilent
```

備註 – 在 Access Manager 7 2005Q4 發行版本中，不支援以下程序檔：

- 具有建立引數的 `amserver`
- `amserver.`*instance*

同時，依預設 `amserver start` 僅啓動認證 `amsecuridd` 與 `amunixd` 輔助程式。`amsecuridd` 輔助程式只能在 Solaris OS SPARC 平台上使用。

Access Manager 部署方案

在您使用 Java Enterprise System 安裝程式安裝 Access Manager 的第一個實例後，可部署和配置附加 Access Manager 實例，做法是先編輯無訊息配置輸入檔案中的配置變數，再執行 `amconfig` 程序檔。

本節描述以下方案：

- 第 32 頁的 「部署 Access Manager 附加實例」
- 第 33 頁的 「配置與重新配置 Access Manager 實例」
- 第 34 頁的 「解除安裝 Access Manager」
- 第 35 頁的 「解除安裝所有 Access Manager 實例」

部署 Access Manager 附加實例

您必須使用 Web 容器的管理工具建立並啓動新的 Web 容器實例，才能部署新的 Access Manager 實例。相關資訊請參考特定 Web 容器說明文件：

- 針對 Web Server，請參閱 http://docs.sun.com/coll/1308.1 與 http://docs.sun.com/coll/1425.1
- 針對 Application Server，請參閱 http://docs.sun.com/coll/1310.1 與 http://docs.sun.com/coll/1416.1

本節中說明的各項步驟，僅適用於已使用 [立即配置] 選項安裝的 Access Manager 實例。如果您計劃使用 WebLogic 或 WebSphere 來做爲 Web 容器，在安裝 Access Manager 時必須使用 [以後配置] 選項。請參閱第 2 章以取得更多資訊。

部署 Access Manager 附加實例

本節說明如何在其他主機伺服器上部署 Access Manager 附加實例，以及如何更新 [平台伺服器清單]。

▼ 要部署 Access Manager 附加實例

1 **以管理員身份登入，視實例的 Web 容器而異。例如，如果 Web Server 6.1 為新實例的 Web 容器，以超級使用者 (root) 或 Web Server Administration Server 的使用者帳號登入。**

2 **複製 amsamplesilent 檔案到可寫入目錄，並將該目錄設為目前使用的目錄。例如，您可以建立一個稱為 /newinstances 的目錄。**

提示：重新命名 amsamplesilent 檔案的副本，以說明您要部署的新實例。例如，下列步驟使用一個稱爲 amnewws6instance 的輸入檔案，以安裝 Web Server 6.1 的新實例。

3 **在新的 amnewws6instance 檔案中設定下列變數：**

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
```

在 amnewws6instance 檔案中，視需要爲您要建立的新實例設定其他變數。關於這些變數的描述，請參閱下列章節中的表格：

- 第 22 頁的 「Access Manager 配置變數」
  - 第 25 頁的 「Web 容器配置變數」
  - 第 29 頁的 「Directory Server 配置變數」

    重要：所有 Access Manager 實例都必須使用相同的密碼加密金鑰值。若要設定此實例的 AM_ENC_PWD 變數，請從第一個實例的 AMConfig.properties 檔案中，複製 am.encryption.pwd 特性的值。

    假如稍後您需要解除安裝這個實例，請儲存 amnewws6instance 檔案。

4 **執行 amconfig，指定新的 amnewws6instance 檔案。例如，在 Solaris 系統上：**

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./newinstances/amnewws6instance
```

`-s` 選項於無訊息模式中執行 `amconfig`。

`amconfig` 程序檔視需要呼叫其他配置程序檔，使用 `amnewws6instance` 檔案中的變數部署新實例。

▼ 若要更新 [平台伺服器清單]

當您建立附加容器實例時，必須更新 Access Manager 的 [平台伺服器清單]，使其反映附加的容器。

1 **請以頂層管理員的身份登入 Access Manager 主控台。**

2 **按一下 [服務配置] 標籤。**

3 **按一下 [平台] 服務。**

4 **請在 [伺服器清單] 中為新實例輸入下列資訊：**

protocol://*fqdn*:*port*|*instance-number*

實例編號應爲下一個未使用的可用號碼。

5 **按一下 [加入]。**

6 **按一下 [儲存]。**

配置與重新配置 Access Manager 實例

您可以配置以 [以後配置] 選項安裝的 Access Manager 實例，或執行 `amconfig` 程序檔在 Java Enterprise System 安裝程式中重新配置以 [立即配置] 選項安裝的第一個實例。

例如，您可能想要重新配置實例，以變更 Access Manager 所有者和群組。

▼ 若要配置或重新配置 Access Manager 實例

1 **以管理員身份登入，視實例的 Web 容器而異。例如，如果 Web Server 6.1 為新實例的 Web 容器，以超級使用者 (root) 或 Web Server Administration Server 的使用者帳號登入。**

2 **將用來部署實例的無訊息配置輸入檔案複製到可寫入的目錄，並使該目錄成為您的目前目錄。例如，若要重新配置 Web Server 6.1 的實例，在下列步驟中是使用 `/reconfig` 目錄中名為 `amnewinstanceforWS61` 的輸入檔案。**

3 在 amnewinstanceforWS61 檔案中，將 DEPLOY_LEVEL 變數設定為第 21 頁的 「配置模式變數」作業描述的變數之一。例如，設定 DEPLOY_LEVEL=21 以重新配置一個完全安裝。

4 在 amnewinstanceforWS61 檔案中，將 NEW_INSTANCE 變數設為 false：

```
NEW_INSTANCE=false
```

5 設定其他在 amnewinstanceforWS61 檔案中的變數以重新配置實例。例如，要變更實例的所有者和群組，將 NEW_OWNER 和 NEW_GROUP 變數設成新值。

關於其他變數的描述，請參閱下列章節中的表格：

- 第 22 頁的 「Access Manager 配置變數」
  - 第 25 頁的 「Web 容器配置變數」
  - 第 29 頁的 「Directory Server 配置變數」

6 執行 amconfig 程序檔，指定新的已編輯輸入檔案。例如，在 Solaris 系統上：

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./reconfig/amnewinstanceforWS61
```

-s 選項於無訊息模式中執行程序檔。 amconfig 程序檔視需要呼叫其他配置程序檔，使用 amnewinstanceforWS61 檔案中的變數以重新配置實例。

解除安裝 Access Manager

您可以解除安裝由執行 amconfig 程序檔所安裝的 Access Manager 實例。您也可以暫時取消配置 Access Manager 實例，除非您移除 Web 容器實例，否則仍可於稍後重新部署另一個 Access Manager 實例。

▼ 要解除安裝 Access Manager 實例

1 以管理員身份登入，視實例的 Web 容器而異。例如，如果 Web Server 6.1 為新實例的 Web 容器，以超級使用者 (root) 或 Web Server Administration Server 的使用者帳號登入。

2 將用來部署實例的無訊息配置輸入檔案複製到可寫入的目錄，並使該目錄成為您的目前目錄。例如，若要取消配置 Web Server 6.1 的實例，在下列步驟中是使用 /unconfigure 目錄中名為 amnewinstanceforWS61 的輸入檔案。

3 在 amnewinstanceforWS61 檔案中，將 DEPLOY_LEVEL 變數設定為第 21 頁的 「配置模式變數」作業描述的變數之一。例如，設定 DEPLOY_LEVEL=11 以解除安裝 (或取消配置) 一個完全安裝。

4 執行 amconfig 程序檔，指定新的已編輯輸入檔案。例如，在 Solaris 系統上：

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./unconfigure/aminstanceforWS61
```

-s 選項於無訊息模式中執行程序檔。 amconfig 程序檔讀取 amnewinstanceforWS61 檔案然後解除安裝實例。

如果您稍後要重新部署另一個 Access Manager 實例，仍可以使用 Web 容器實例。

解除安裝所有 Access Manager 實例

此方案會從系統中完整地移除所有 Access Manager 7 2005Q4 實例與套裝軟體。

▼ 若要完全從系統中移除 Access Manager 7 2005Q4

1. **請以超級使用者的身份登入或成為超級使用者 (root)。**
2. **在用來部署實例的輸入檔案中，將 DEPLOY_LEVEL 變數設定為第 21 頁的 「配置模式變數」作業描述的變數之一。例如，設定 DEPLOY_LEVEL=11 以解除安裝 (或取消配置) 一個完全安裝。**
3. **使用您在第 35 頁的 「解除安裝所有 Access Manager 實例」中編輯的檔案來執行 amconfig 程序檔。例如，在 Solaris 系統上：**

   ```
   # cd opt/SUNWam/bin/
   # ./amconfig -s ./newinstances/amnewws6instance
   ```

   amconfig 程序檔於無訊息模式中執行以解除安裝實例。

   爲所有您要解除安裝的其他 Access Manager 實例重複這個步驟，但您使用 Java Enterprise System 安裝程式安裝的實例 (第一個實例) 除外。

4. **若要解除安裝第一個實例，並移除系統中所有 Access Manager 套裝軟體，請執行 Java Enterprise System 解除安裝程式。如需有關解除安裝程式的更多資訊，請參閱「Sun Java Enterprise System 2005Q4 Installation Guide for UNIX」 。**

範例配置程序檔輸入檔案

下節包含 Access Manager 配置程序檔輸入檔案的範例，用於與 WebLogic 8.1 共同部署。

```
DEPLOY_LEVEL=1
BASEDIR=/opt
SERVER_HOST=ide-56.example.company.com
SERVER_PORT=7001
SERVER_PROTOCOL=http
CONSOLE_HOST=$SERVER_HOST
CONSOLE_PORT=$SERVER_PORT
CONSOLE_PROTOCOL=$SERVER_PROTOCOL
CONSOLE_REMOTE=false
```

```
DS_HOST=ide-56.example.company.com
DS_PORT=389
DS_DIRMGRDN=”cn=Directory Manager”
DS_DIRMGRPASSWD=11111111
ROOT_SUFFIX=”dc=company,dc=com”
ADMINPASSWD=11111111
AMLDAPUSERPASSWD=00000000
CONSOLE_DEPLOY_URI=/amconsole
SERVER_DEPLOY_URI=/amserver
PASSWORD_DEPLOY_URI=/ampassword
COMMON_DEPLOY_URI=/amcommon
COOKIE_DOMAIN=.iplanet.com
JAVA_HOME=/usr/jdk/entsys-j2se
AM_ENC_PWD=””
PLATFORM_LOCALE=en_US
NEW_OWNER=root
NEW_GROUP=other
XML_ENCODING=ISO-8859-1
NEW_INSTANCE=false
WEB_CONTAINER=WL8
WL8_HOME=/export/bea8
WL8_PROJECT_DIR=user_projects
WL8_DOMAIN=mydomain
WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
WL8_SERVER=myserver
WL8_INSTANCE=/export/bea8/weblogic81
WL8_PROTOCOL=http
WL8_HOST=ide-56.example.company.com
WL8_PORT=7001
WL8_SSLPORT=7002
WL8_ADMIN=”weblogic”
WL8_PASSWORD=”11111111”
WL8_JDK_HOME=$WL8_HOME/jdk142_04
DIRECTORY_MODE=1
USER_NAMING_ATTR=uid
ORG_NAMING_ATTR=o
ORG_OBJECT_CLASS=examplemanagedorganization
USER_OBJECT_CLASS=inetorgperson
DEFAULT_ORGANIZATION=
Sample Configuration Script Input File for WebLogic 8.1.x
```

◆ ◆ ◆ 第 2 章

2 安裝並配置協力廠商 Web 容器

本章說明安裝並配置與 Sun Java™ System Access Manager 一起部署之協力廠商 Web 容器的程序。針對此版本，Access Manager 支援 BEA WebLogic 8.1 (及其目前修補程式) 與 IBM WebSphere 5.1 (及其目前修補程式)。

WebLogic 和 WebSphere 並不是 Java Enterprise System 的一部份，所以您必須分別以 Java ES 安裝程式來安裝並配置它們。一般而言，程序如下：

- 安裝、配置與啓動 Web 容器實例。
- 從 Java ES 安裝程式來安裝 Directory Server。
- 從 Java ES 安裝程式以「以後配置」模式安裝 Access Manager，這會使 Access Manager 仍保留未配置的狀態。
- 執行 Access Manager 配置程序檔，以在 Web 容器內部署 Access Manager。
- 重新啓動 Web 容器。

安裝並配置 BEA WebLogic 8.1

當您安裝 WebLogic 之前，請確認已在 DNS 中註冊主機網域。同時，驗證您安裝的 WebLogic 軟體版本正確。如需更多資訊，請移至 BEA 產品網站，網址爲 http://commerce.bea.com/index.jsp。

▼ 若要安裝並配置 WebLogic 8.1

1 **將下載的軟體影像 (`.zip` 或 `.gz` 格式) 解壓縮。確定 zip/gzip 公用程式適用於正確的平台，否則您在解壓縮時會收到總和檢查錯誤的訊息。**

2 **從目標系統的 shell 視窗執行安裝程式。**

遵循 WebLogic 安裝公用程式所提供的程序 (可以在以下網址找到詳細的安裝指示：http://e-docs.bea.com/wls/docs81/)。

在安裝程序期間，請確定記錄以下資訊，稍後在 Access Manager 配置時會用到這些資訊：

- FQDN (用於 WL8_HOST 參數中)
  - 安裝位置
  - 連接埠號

3 **完成安裝之後，請從下列位置執行 WebLogic 配置工具來配置網域和伺服器實例：**

WebLogic-base/WebLogic-instance/common/bin/quickstart.sh

依預設，WebLogic 會將伺服器實例定義成 myserver，網域定義成 mydomain。您可能不會選擇使用這些預設。如果您建立新的網域和實例，請確認記錄此資訊，以供 Access Manager 配置與部署使用。請參閱 WebLogic 8.1 文件以取得指示。

4 **如果您在管理實例上進行安裝，請從以下位置使用 startWebLogic.sh 公用程式來啓動 WebLogic：**

WebLogic-base/WebLogic-Userhome /domains/ *WebLogic-domain*/startWebLogic.sh

如果是在管理式實例上進行安裝，請使用以下指令啓動 WebLogic：

WebLogic-base /WebLogic-Userhome/domains/ WebLogic-domain /startManagedWebLogic WebLogic-managed-instancename admin-url

安裝並配置 IBM WebSphere 5.1

安裝 WebSphere 之前，請確認已在 DNS 中註冊您的主機網域，並驗證您安裝的 WebSphere 軟體是適用於平台的正確版本。如需更多資訊，請移至 IBM 產品支援網站，網址爲 http://www-306.ibm.com/software/websphere/support/。

▼ 若要安裝並配置 WebSphere 5.1

1 **將下載的軟體影像 (.zip 或 .gz 格式) 解壓縮。確定 zip/gzip 公用程式適用於正確的平台，否則您在解壓縮時會收到總和檢查錯誤的訊息。**

2 **從目標系統的 shell 視窗執行安裝程式。如果您計劃要安裝修補程式，請先安裝 5.1 版，然後再套用修補程式。您可在以下網址找到詳細的安裝指示：http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp。**

在安裝程序期間，請確定記錄以下資訊，稍後在 Access Manager 配置時會用到這些資訊：

- 主機名稱
  - 網域名稱
  - 儲存格名稱
  - 節點名稱
  - 連接埠號

- 安裝目錄
- WebSphere 實例名稱
- 管理連接埠

  依預設，WebSphere 會將伺服器實例定義成 `server1`，不過您可能不會使用此預設。如果您建立新的實例，請確認記錄此資訊，以供 Access Manager 配置與部署使用。請參閱 WebSphere 5.1 文件以取得指示。

3 驗證伺服器已成功安裝。

a. 請確認以下目錄中存在 `server.xml` 檔案：

`/opt/WebSphere/AppServer/config/cells/cell-name/noes/`

`node-name/servers/server1`

b. 使用 `startServer.sh` 指令來啓動伺服器，例如：

`/opt/WebSphere/AppServer/bin/startServer.sh server1`

c. 在 Web 瀏覽器中，以下列格式輸入對應的 URL 來檢視範例 Web 應用程式：

`http://` *fqdn:portnumber/snoop*

4 驗證安裝順利完成之後，使用 `stopServer.sh` 公用程式來停止伺服器。例如：

`opt/WebSphere/AppServer/bin/stopServer.sh server1`

5 若您要安裝 WebSphere 5.1 修補程式，請使用 `updateWizard.sh` 指令行公用程式在原始 5.1 實例上安裝修補程式。

6 重新啓動 WebSphere 並驗證安裝已順利完成。

使用 Java ES 來安裝 Directory Server 和 Access Manager

Access Manager 安裝牽涉到兩個獨立的 Java Enterprise System (Java ES) 安裝程式呼叫。

▼ 若要安裝 Directory Server

1 執行第一個 Java ES 呼叫，以 [立即配置] 選項來安裝 Directory Server (本機或遠端)。[立即配置] 選項可讓您在安裝期間，依選取的選項 (或預設值) 來配置第一個實例。

2 **執行第二個 Java ES 呼叫，以 [以後配置] 選項來安裝 Access Manager。這個選項會安裝 Access Manager 2005Q4 元件。在安裝之後，您必須配置 Access Manager。**

WebLogic 與 WebSphere 的安裝獨立於 Java ES 安裝，所以安裝程式中並沒有包含自動部署容器所需的配置資料。因此，安裝 Access Manager 時您必須選取 [以後配置] 選項。此選項會將 Access Manager 部署保留在以下狀態：

- 使用中的 Directory Server (本機或遠端) 沒有載入 Access Manager DIT 資料。
  - 不會自動載入 Access Manager 配置檔案。
  - 不會產生 Access Manager Web 應用程式 `.war` 檔案。
  - 不會自動啓動與執行 Access Manager 部署以及後安裝配置程序。

    如需詳細的安裝指示，請參照「Sun Java Enterprise System 安裝指南」，網址爲 http://docs.sun.com/doc/819-0811。

配置 Access Manager

在目標系統的本機磁碟上完成 Access Manager 安裝之後，您需要以 WebLogic 8.1 或 WebSphere 5.1 手動配置 Access Manager。這個程序有以下三個步驟：

▼ 若要配置 Access Manager

1 **編輯配置程序檔輸入檔案**

2 **執行配置程序檔**

3 **重新啓動 Web 容器**

建立配置程序檔輸入檔案

Access Manager 配置程序檔輸入檔案中包含所有的部署層級、Access Manager、Web 容器以及 Directory Server 變數定義。Access Manager 包含範例配置程序檔輸入檔案範本 (`amsamplesilent`)，位於 *AccessManager-base*`/SUNWam/bin` 目錄 (Solaris 系統) 或 *AccessManager-base*`/identity/bin` 目錄 (Linux 系統) 中。

您可以使用 `amsamplesilent` 範本來建構配置程序檔輸入檔案。第 21 頁的 「Access Manager 範例配置程序檔輸入檔案」中說明編輯此檔案的指示以及變數定義。

編輯檔案之前，請確認已從 Web 容器安裝取得以下資訊：

BEA WebLogic 和 IBM WebSphere

- 安裝位置
- 實例名稱和位置
- 主機名稱
- FQDN
- 其偵聽的連接埠號
- 管理 ID
- 使用的通訊協定

僅限 BEA WebLogic

- 管理密碼
- 共用程式庫位置
- 網域名稱和位置
- 專案目錄名稱
- JDK 位置

僅限 IBM WebSphere

- 儲存格名稱
- 節點名稱
- JDK 位置

執行配置程序檔

當您儲存了配置程序檔輸入檔案之後，請執行 `amconfig` 程序檔以完成配置程序。例如：

```
AccessManager-base/SUMWam/bin/amconfig -s silentfile
```

silentfile 應該是配置輸入檔案的絕對路徑。

執行此程序檔會執行以下功能：

1. 將 Access Manager 模式載入到使用中的 Directory Server 實例。
2. 將 Access Manager 服務資料載入到 Directory Server 實例。
3. 產生使用中的 Access Manager 實例所使用的 Access Manager 配置檔案。
4. 將 Access Manager Web 應用程式資料部署到 Web 容器。
5. 自訂 Web 容器配置以符合 Access Manager 的需求。

重新啓動 Web 容器

在您完成配置程序之後，必須重新啓動 Web 容器。請參照產品的文件以取得指示。

針對 BEA WebLogic 8.1，請參閱 http://e-docs.bea.com/wls/docs81。

針對 IBM WebSphere 5.1，請參閱
http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp。

◆ ◆ ◆ 第 3 章

3 在 SSL 模式中配置 Access Manager

使用具有簡單認證的安全套接層 (SSL) 可以保證機密性和資料完整性。若要在 SSL 模式中啓用 Access Manager，通常要：

- 以安全 Web 容器配置 Access Manager
- 將 Access Manager 配置到安全的 Directory Server

使用安全 Sun Java Enterprise System Web Server 配置 Access Manager

若要使用 Web Server 在 SSL 模式中配置 Access Manager，請參閱以下步驟：

▼ 若要配置安全的 Web Server

1 **在 Access Manager 主控台中，移至服務配置模組並選取 [平台] 服務。在 [伺服器清單] 屬性中，移除 `http://` 協定，然後加入 `https://` 協定。按一下 [儲存]。**

備註 – 請務必按一下 [儲存]。否則，雖然您仍可以繼續執行下面的步驟，但您所做的所有配置變更均會遺失，並且無法以管理員身份登入以修正此問題。

步驟 2 至 24 描述 Web Server。

2 **登入 Web Server 主控台。預設連接埠為 8888。**

3 **選取 Access Manager 於其上執行的 Web Server 實例，然後按一下 [管理]。**
系統會顯示快顯式視窗，說明配置已變更。按一下 [確定]。

4 **按一下畫面右上角的 [套用] 按鈕。**

5 **按一下 [套用變更]**。
Web Server 會自動重新啓動。按一下 [確定] 以繼續。

6 **停止選取的 Web Server 實例**。

7 **按一下 [安全] 標籤**。

8 **按一下 [建立資料庫]**。

9 **輸入新的資料庫密碼並按一下 [確定]**。
請確保記下資料庫密碼，以備稍後使用。

10 **建立憑證資料庫後，按一下 [請求憑證]**。

11 **在畫面提供的欄位中輸入資料**。
[鍵值對欄位密碼] 欄位和您在步驟 9 中輸入的內容相同。在位置欄位中，您必須完整拼出位置。縮寫詞 (如 CA) 無效。必須定義所有欄位。在[共用名稱] 欄位中，提供您 Web Server 的主機名稱。

12 **提交表格後，您將看到與以下訊息類似的訊息：**

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

13 **複製這些文字並提交，以請求憑證**。
請確保您取得了 Root CA 憑證。

14 **您將接收到包含憑證的憑證回應，如：**

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

15 **將這些文字複製到剪貼簿，或儲存在檔案中**。

16 移至 Web Server 主控台並按一下 [安裝憑證]。

17 按一下該 Server 的憑證。

18 在 [鍵值對檔案密碼] 欄位中輸入憑證資料庫密碼。

19 在提供的文字欄位中貼上憑證，或核取單選按鈕並在文字方塊中輸入檔案名稱。按一下 [提交]。
瀏覽器將顯示該憑證，並提供加入憑證的按鈕。

20 按一下 [安裝憑證]。

21 按一下 [可信任的憑證授權機構的憑證]。

22 以步驟 16 至 21 中所述的相同方式安裝 Root CA 憑證。

23 兩個憑證安裝完成後，按一下 Web Server 主控台中的 [喜好設定] 標籤。

24 如果要在不同的連接埠上啓用 SSL，請選取 [加入偵聽套接字]。然後選取 [編輯偵聽套接字]。

25 從 [停用至啓用] 變更安全性狀態，然後按一下 [確定] 提交變更，再按一下 [套用] 和 [套用變更]。
步驟 26–29 適用於 Access Manager。

26 開啓 `AMConfig.properties` 檔案。依預設，此檔案位於 `etc/opt/SUNWam/config`。

27 用 `https://` 取代所有出現的 `http://` 協定，Web Server 實例目錄中的除外。`AMConfig.properties` 中也指定了這一點，但必須保持一致。

28 儲存 `AMConfig.properties` 檔案。

29 在 Web Server 主控台中，按一下託管 Web 伺服器實例之 Access Manager 的 [開啓/關閉] 按鈕。
Web Server 會在 [啓動/停止] 頁面中顯示一個文字方塊。

30 在文字欄位中輸入憑證資料庫密碼並選取 [啓動]。

以安全 Sun Java System Application Server 配置 Access Manager

將 Access Manager 設定爲在已啓用 SSL 的 Application Server 上執行，過程分兩步驟。首先，將 Application Server 實例與安裝的 Access Manager 安全結合在一起，然後配置 Access Manager 本身。

使用 SSL 設定 Application Server 6.2

本節說明於 SSL 模式下設定 Application Server 6.2 的步驟。

▼ 安全結合 Application Server 實例

1. **在您的瀏覽器中輸入以下位址，以管理員身份登入 Sun Java System Application Server 主控台：**

   ```
   http://fullservername:port
   ```

   預設連接埠爲 4848。

2. **輸入您在安裝時輸入的使用者名稱和密碼。**
3. **選取您在其上安裝 (或將要安裝) 的 Application Server 實例。右框架會顯示配置已變更。**
4. **按一下 [套用變更]。**
5. **按一下 [重新啓動]。Application Server 會自動重新啓動。**
6. **在左框架中，按一下 [安全]。**
7. **按一下 [管理資料庫] 標籤。**
8. **按一下 [建立資料庫] (如果未選取)。**
9. **輸入新的資料庫密碼並確認，然後按一下 [確定] 按鈕。請確保記下資料庫密碼，以備稍後使用。**
10. **建立憑證資料庫後，按一下 [憑證管理] 標籤。**
11. **按一下 [請求] 連結 (如果未選取)。**

12 為憑證輸入以下請求資料

a. 如果該憑證為新憑證或更新的憑證，則選取它。許多憑證會在一段特定時間後過期，某些憑證授權機構 (CA) 會自動給您傳送換新通知。

b. 指定您要提交憑證請求的方式。

如果希望 CA 接收電子郵件訊息形式的請求，請核取 [CA 電子郵件] 並輸入 CA 的電子郵件位址。如需 CA 清單，請按一下 [可用憑證授權機構清單]。

如果您從使用憑證伺服器的內部 CA 請求憑證，則請按一下 [CA URL] 並輸入憑證伺服器的 URL。此 URL 應指向用於處理憑證申請的憑證伺服器程式。

c. 輸入您鍵值對檔案的密碼 (您在步驟 9 中指定的密碼)。

d. 輸入以下識別資訊：

共用名稱。伺服器的完整名稱，包含連接埠號。

請求者名稱。請求者的名稱。

電話號碼。請求者的電話號碼。

共用名稱 。Sun Java System Application Server 的完全合格名稱，將會安裝數位憑證。

電子郵件位址。管理員的電子郵件位址。

組織名稱。您的組織名稱。憑證授權機構可能會要求在此屬性中輸入的所有主機名稱均屬於註冊到該組織的領域。

組織單元名稱。組織的分支、部門或其他運作部門的名稱。

地區名稱 (城市)。您所在城市或城鎮的名稱。

州的名稱。如果您的組織分別在美國或加拿大，此項指組織所在州或省的名稱。請勿縮寫。

國家/地區代碼。代表您國家/地區的兩個字母的 ISO 代碼。例如，美國的代碼是 US。

13 按一下 [確定] 按鈕。畫面上將會顯示訊息，例如：

```
--BEGIN NEW CERTIFICATE REQUEST---
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl
--END NEW CERTIFICATE REQUEST--
```

14 將所有這些文字複製到一個檔案並按一下 [確定]。請確定您取得了 Root CA 憑證。

15 選取一個 CA，然後依循該授權單位網站的指示，取得數位憑證。您可以從 CMS、Verisign 或 Entrust.net 取得憑證

16 從憑證授權機構接收到數位憑證後，您可以將文字複製到剪貼簿，或將其儲存到檔案中。

17 移至 Application Server 主控台並按一下 [安裝] 連結。

18 選取 [此伺服器的憑證]。

19 在 [鍵值對檔案密碼] 欄位中輸入憑證資料庫密碼。

20 在提供的文字欄位、訊息文字 (帶有標頭) 中貼上憑證，或在此檔案文字方塊的訊息中輸入檔案名稱。選取相應的單選按鈕。

21 按一下 [確定] 按鈕。瀏覽器會顯示憑證，並提供加入憑證的按鈕。

22 按一下 [新增伺服器憑證]。

23 以上述方式安裝 Root CA 憑證。但是，請選取 [可信任的憑證授權機構的憑證]。

24 安裝完兩個憑證後，展開左框架中的 HTTP 伺服器節點。

25 選取 HTTP 伺服器下的 HTTP 偵聽程式。

26 選取 `http-listener-1`。瀏覽器會顯示套接字資訊。

27 將 `http-listener-1` 使用之連接埠的值從安裝應用程式伺服器時所輸入的值變更為更適當的值，如：443。

28 選取 [啓用 SSL/TLS]。

29 選取 [憑證別名]。

30 指定回傳伺服器。該伺服器應該與步驟 12 中指定的共用名稱相符。

31 按一下 [儲存]。

32 選取您要在其上安裝 Access Manager 軟體的 Application Server 實例。右框架會顯示配置已變更。

33 按一下 [套用變更]。

34 按一下 [重新啓動]。Application Server 會自動重新啓動。

使用 SSL 配置 Application Server 8.1

使用 SSL 配置 Application Server 8.1 的基本步驟如下。請參閱 Application Server 8.1 文件以取得詳細的指示。

1. 透過 Application Server 管理主控台在 Application Server 上建立一個安全的連接埠。如需更多資訊，請參閱位於下列位置之「Sun Java System Application Server Enterprise Edition 8.1 管理指南」中的「配置安全性」。

   http://docs.sun.com/app/docs/coll/1310.1 與
   http://docs.sun.com/app/docs/coll/1416.1

2. 驗證信任伺服器憑證的憑證授權機構 (CA) 是否存在於 web 容器的信任資料庫中。之後，獲取並安裝 web 容器的伺服器憑證。如需更多資訊，請參閱位於下列位置之「Sun Java System Application Server Enterprise Edition 8.1 管理指南」中的「使用證書和SSL」。

   http://docs.sun.com/app/docs/coll/1310.1 與
   http://docs.sun.com/app/docs/coll/1416.1

3. 重新啓動 Web 容器。

在 SSL 模式中配置 Access Manager

本節說明在 SSL 模式中配置 Access Manager 的步驟。設定 Access Manager 的 SSL 之前，請確定您已爲您的部署配置 Web 容器。

▼ 若要在 SSL 模式中配置 Access Manager

1 在 Access Manager 主控台中，移至服務配置模組並選取 [平台] 服務。在伺服器清單屬性中，加入使用 HTTPS 協定的相同的 URL 和一個已啓用 SSL 的連接埠號。按一下 [儲存]。

備註 – 如果 Access Manager 單一實例正在偵聽兩個連接埠 (一個 HTTP，一個 HTTPS)，且您試圖以停止的 Cookie 存取 Access Manager，Access Manager 將沒有回應。這並非支援的配置。

---

2 從下列預設位置開啓 `AMConfig.properties` 檔案：

`/etc/opt/SUNWam/config`。

3 用 `https://` 取代所有出現的 `http://` 協定，並將連接埠埠號變更為已啓用 SSL 的連接埠埠號。

4 儲存 `AMConfig.properties` 檔案。

5 重新啓動 Application Server。

使用安全 BEA WebLogic Server 配置 AMSDK

在 SSL 中使用 AMSDK 進行配置之前，必須先安裝 BEA WebLogic Server 並配置成 Web 容器。如需安裝說明，請參閱 BEA WebLogic 伺服器文件。若要針對 Access Manager 將 WebLogic 配置爲 Web 容器，請參閱第 1 章。

▼ 若要配置安全的 WebLogic 實例

1. **使用快速開始功能表來建立網域**
2. **移至 BEA WebLogic 安裝目錄並產生憑證請求。**
3. **使用 CSR 文字檔將伺服器憑證套用至 CA。**
4. **將核准的憑證儲存到文字檔中。例如，**`approvedcert.txt`。
5. **使用下列指令，載入** `cacerts` **中的根 CA：**

   ```
   cd jdk141_03/jre/lib/security/
   ```

   ```
   jdk141_03/jre/bin/keytool -keystore cacerts -keyalg RSA -import -trustcacerts -alias
   "<alias name>" -storepass changeit -file /opt/bea81/cacert.txt
   ```

6. **使用以下指令來載入伺服器憑證：**

   ```
   jdk141_03/jre/bin/keytool -import -keystore <keystorename> -keyalg RSA -import
   -trustcacerts -file approvedcert.txt -alias "mykey"
   ```

7. **使用您的使用者名稱和密碼登入 BEA WebLogic 主控台。**
8. **瀏覽至以下位置：**
   您的網域 > 伺服器 > myserver > 配置金鑰庫
9. **選取自訂身份和 Java Standard Trust**
10. **輸入鍵值儲存區位置。例如，**`/opt/bea81/keystore`。
11. **輸入鍵值儲存區密碼和鍵值儲存區通行密語。例如：**
    鍵值儲存區密碼：`JKS/Java Standard Trust` (對 WL 8.1，則僅爲 JKS)

    鍵值儲存區通行密語：`changeit`
12. **檢閱 SSL 私密金鑰設定的私密金鑰別名與密碼。**

備註 – 您必須使用完整強度 SSL 授權，否則 SSL 啓動將會失敗

13 **在 Access Manager 中，下列 `AmConfig.properties` 中的參數會於安裝期間自動配置。如果未自動配置，您可以編輯它們：**

```
com.sun.identity.jss.donotInstallAtHighestPriority=true [ this is not
 required for AM 6.3 and above]
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.JSSESocketFactory
com.iplanet.security.encryptor=com.iplanet.services.util.JCEEncryption
```

如果您的 JDK 路徑如下所示：

```
com.iplanet.am.jdk.path=/usr/jdk/entsys-j2se
```

那麼請使用鍵工具公用程式，在憑證資料庫中匯入根 CA。例如：

```
/usr/jdk/entsys-j2se/jre/lib/security
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore cacerts
-keyalg RSA -import -trustcacerts -alias "machinename" -storepass changeit -file
/opt/bea81/cacert.txt
```

鍵工具公用程式位於以下目錄中：

```
/usr/jdk/entsys-j2se/jre/bin/keytool
```

14 **從 Access Manager `amadmin` 指令行公用程式移除 `-D"java.protocol.handler.pkgs=com.iplanet.services.comm"`。**

15 **在 SSL 模式中配置 Access Manager。如需更多資訊，請參閱****第 49 頁的 「在 SSL 模式中配置 Access Manager」****。**

使用安全 IBM WebSphere Application Server 配置 AMSDK

在 SSL 中使用 AMSDK 進行配置之前，必須先安裝 IBM WebSphere Server 並配置成 Web 容器。如需安裝說明，請參閱 WebSphere 伺服器的文件。若要針對 Access Manager 將 WebLogic 配置爲 Web 容器，請參閱第 1 章。

▼ 若要配置安全的 WebSphere 實例

1 **啓動 `ikeyman.sh` (位於 Websphere `/bin` 目錄下)。**

2 **從 [簽署人] 功能表匯入憑證授權機構 (CA) 的憑證。**

3. **從 [個人憑證] 功能表產生 CSR。**
4. **擷取在上個步驟中建立的憑證。**
5. **選取 [個人憑證] 並匯入伺服器憑證。**
6. **從 WebSphere 主控台，變更預設 SSL 設定並選取密碼。**
7. **設定預設 IBM JSSE SSL 提供者。**
8. **輸入以下指令，從您剛才建立的檔案，將 Root CA 憑證匯入到 Application Server JVM 鍵值儲存區：**

   ```
   $ appserver_root-dir/java/bin/ keytool -import -trustcacerts -alias cmscacert
   -keystore ../jre/lib/security/cacerts -file
   /full_path_cacert_filename.txt
   ```

   app-server-root-dir 是應用程式伺服器的根目錄，而 *full_path_cacert_filename.txt* 是包含憑證的檔案之完整路徑。

9. **在 Access Manager 中，更新下列 `AmConfig.properties` 中的參數以使用 JSSE：**

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.
   am.util.SecureRandomFactoryImpl
   com.iplanet.security.SSLSocketFactorImpl=netscape.ldap.factory.
   JSSESocketFactory
   com.iplanet.security.encyptor=com.iplanet.services.unil.JCEEncryption
   ```

10. **在 SSL 模式中配置 Access Manager。如需更多資訊，請參閱第 49 頁的 「在 SSL 模式中配置 Access Manager」。**

在 SSL 模式中配置 Access Manager 到 Directory Server

爲了在網路上提供安全通訊，Access Manager 包含 LDAPS 通訊協定。LDAPS 是標準的 LDAP 通訊協定，但於 Secure Sockets Layer (SSL) 頂層執行。爲啓用 SSL 通訊，您必須先在 SSL 模式中配置 Directory Server，然後連接 Access Manager 到 Directory Server。基本步驟如下：

1. 取得並安裝 Directory Server 的憑證，並將 Directory Server 配置爲信任憑證授權機構 (CA) 的憑證。
2. 開啓目錄中的 SSL。
3. 配置認證、策略和平台服務以連接到啓用 SSL 的 Directory Server。
4. 配置 Access Manager 以安全地連接到 Directory Server 後端。

在 SSL 模式中配置 Directory Server

爲了能在 SSL 模式下配置 Directory Server，您必須取得與安裝伺服器憑證、將 Directory Server 配置爲信任 CA 的憑證，然後啓用 SSL。有關如何完成這些工作的詳細指示，請參閱「*Directory Server* 管理指南」中的第十一章「管理認證和加密」。此文件位於以下位置：

http://docs.sun.com/coll/DirectoryServer_04q2
(http://docs.sun.com/coll/DirectoryServer_04q2) 與
http://docs.sun.com/coll/DirectoryServer_04q2_zh_TW
(http://docs.sun.com/coll/DirectoryServer_04q2_zh_TW)

如果您的 Directory Server 已經啓用 SSL，前往下一節以參考有關連接 Access Manager 到 Directory Server 的詳細資料。

連接 Access Manager 到啓用 SSL 的 Directory Server

將 Directory Server 配置爲 SSL 模式後，您必須安全地將 Access Manager 連接到 Directory Server 後端。

▼ 將 Access Manager 連接至 Directory Server

1. **在 Access Manager 主控台中，前往服務配置模組的 LDAP 認證服務。**
   a. **變更 Directory Server 連接埠為 SSL 連接埠。**
   b. **選擇啓用對 LDAP 伺服器屬性的 SSL 存取。**
2. **前往服務配置模組中的成員關係認證服務。**
   a. **變更 Directory Server 連接埠為 SSL 連接埠。**
   b. **選擇啓用對 LDAP 伺服器屬性的 SSL 存取。**
3. **前往位於服務配置中的策略配置服務。**
   a. **變更 Directory Server 連接埠為 SSL 連接埠。**
   b. **選擇 LDAP SSL 屬性。**

4. **在文字編輯器中開啓** `serverconfig.xml`。**此檔案位於以下位置：**
   `/etc/opt/SUNWam/config`

   a. **在** `<Server>` **元素中，變更下列值：**
      `port` - 輸入 Access Manager 偵聽的安全連接埠之埠號 (預設值爲 636)。
      `type`- 將 SIMPLE 變更爲 SSL。

   b. **儲存並關閉** `serverconfig.xml`。

5. **從下列預設位置開啓** `AMConfig.properties` **檔案：**
   /etc/opt/ `SUNWam/config`。
   變更下列特性：

   a. `com.iplanet.am.directory.port = 636` **(若使用預設值)**

   b. `ssl.enabed = true`

   c. **儲存** `AMConfig.properties`。

6. **重新啓動伺服器**。

第 II 部分

存取控制

這是「Sun Java System Access Manager™ 7 2005Q4 管理指南」的第二部分。「存取控制」介面提供建立與管理認證與授權服務的方法，以保護並規範範圍型的資源。當企業使用者請求資訊時，Access Manager 將驗證使用者的身份並授權使用者存取使用者所請求的特定資源。本部分包含以下章節：

◆ ◆ ◆ 第 4 章

4 Access Manager 主控台

Access Manager 主控台爲 Web 介面，允許具不同層級存取權限的管理員執行作業。比如建立範圍和組織、在範圍中建立使用者或從範圍刪除使用者以及建立用以保護和限制對範圍資源之存取的強制策略。此外，管理員可檢視和終止目前的使用者階段作業，管理其聯合配置 (建立、刪除和修改認證網域與提供者)。另一方面，不具管理權限的使用者可以管理個人資訊 (名稱、電子郵件位址、電話號碼等)、變更密碼、訂閱和取消訂閱群組以及檢視其角色。Access Manager 主控台有兩個主要檢視：

管理檢視

當具有管理角色的使用者通過 Access Manager 認證後，預設檢視爲 [管理] 檢視。在此檢視中，管理員可執行大部份與 Access Manager 相關的管理工作。Access Manager 可用兩種不同的模式安裝；「範圍」模式和「舊有」模式。每個模式都有自己的主控台。如需有關「範圍」和「舊有」模式的更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Technical Overview」。

範圍模式主控台

管理員可使用「範圍」模式主控台來管理基於範圍的存取控制、預設服務配置、Web 服務和聯合。若要存取管理員登入畫面，請在您的瀏覽器中使用以下位址語法：

protocol://*servername* /amserver/UI/Login

protocol 可爲 http 或 https，依您的部署而定。

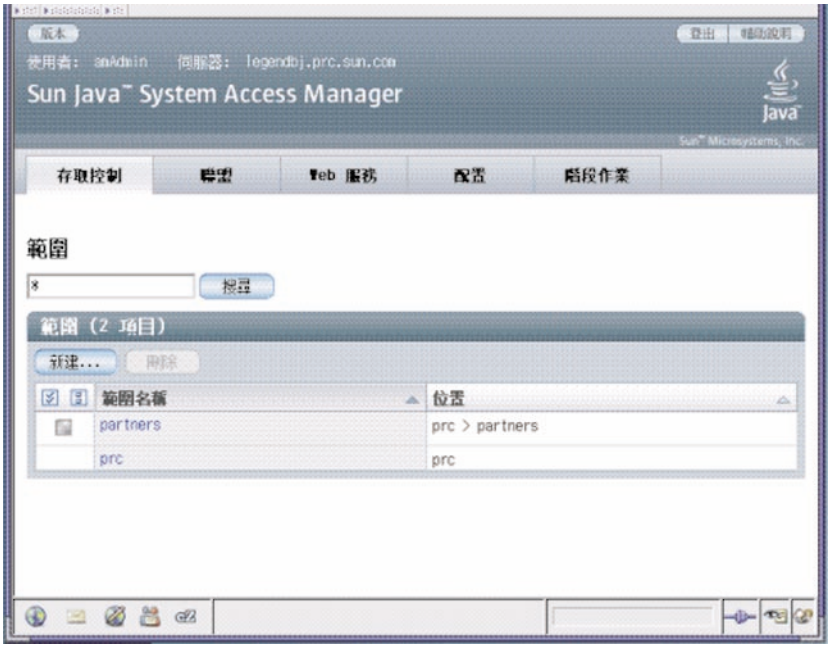

圖 4–1 範圍模式管理檢視

舊有模式主控台

「舊有模式」主控台是以 Access Manager 6.3 的架構爲基礎。此舊有 Access Manager 架構使用 Sun Java System Directory Server 內的 LDAP 目錄資訊樹狀結構 (DIT) 。在「舊有」模式中，使用者資訊和存取控制資訊都是儲存在 LDAP 組織中。選擇「舊有」模式時，LDAP 組織相當於存取控制範圍。範圍資訊會整合在 LDAP 組織中。在「舊有」模式中，[目錄管理] 標籤可用於基於 Access Manager 的識別管理。

若要存取管理員登入畫面，請在您的瀏覽器中使用以下位址語法：

protocol`://`*servername* `/amserver/console`

`protocol` 可爲 http 或 https，依您的部署而定。

圖 4–2 舊有模式管理檢視

舊有模式 6.3 主控台

Access Manager 6.3 的部份功能不能在 Access Manager 7.0 主控台中使用。因此，管理員可透過 7.0 舊有部署登入 6.3 主控台。若 Access Manager 是建立在 Sun Java System Portal Server 或其他需使用 Sun Java System Directory Server 做爲中央識別儲存庫的 Sun Java System 通訊產品上時，通常是使用此主控台。其他功能，如「委託管理」和「服務類別」，只能透過此主控台存取。

備註 – 請勿互換使用 6.3 和 7.0 舊有模式主控台。

若要存取 6.3 主控台，請在您的瀏覽器中使用以下位址語法：

protocol://*servername* /amconsole

`protocol` 可爲 http 或 https，依您的部署而定。

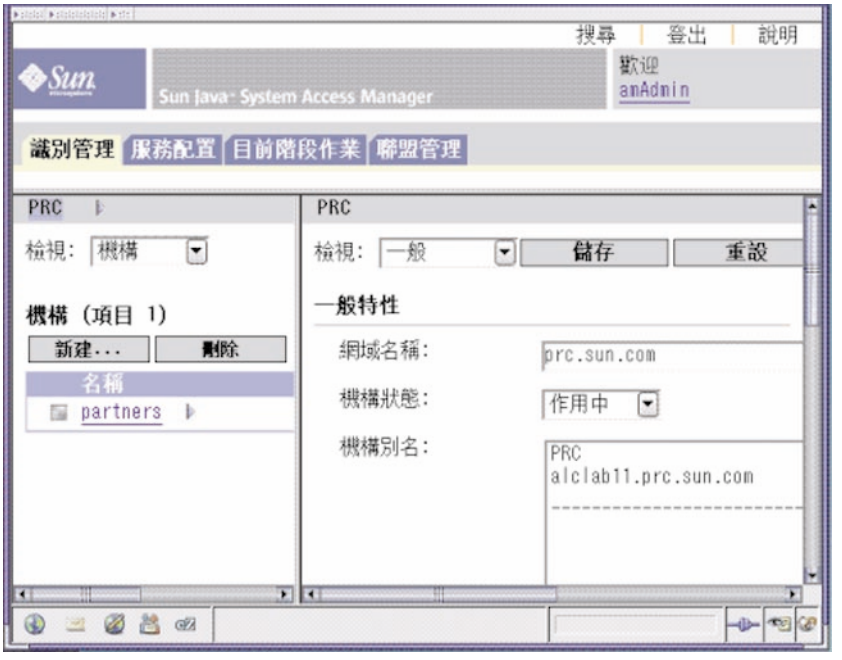

圖 4–3 舊有 6.3 主控台

使用者設定檔檢視

沒有指定管理角色的使用者認證 Access Manager 時，預設的檢視爲使用者本身的使用者設定檔。[使用者設定檔] 檢視可從「範圍」或「舊有」模式存取。使用者必須在 [登入] 頁面輸入使用者自己的使用者名稱和密碼才可存取此檢視。

在此檢視中，使用者可以修改其個人設定檔的特定屬性值。這包括但不僅限於名稱、家庭住址和密碼。[使用者設定檔] 檢視中顯示的屬性可以延伸。

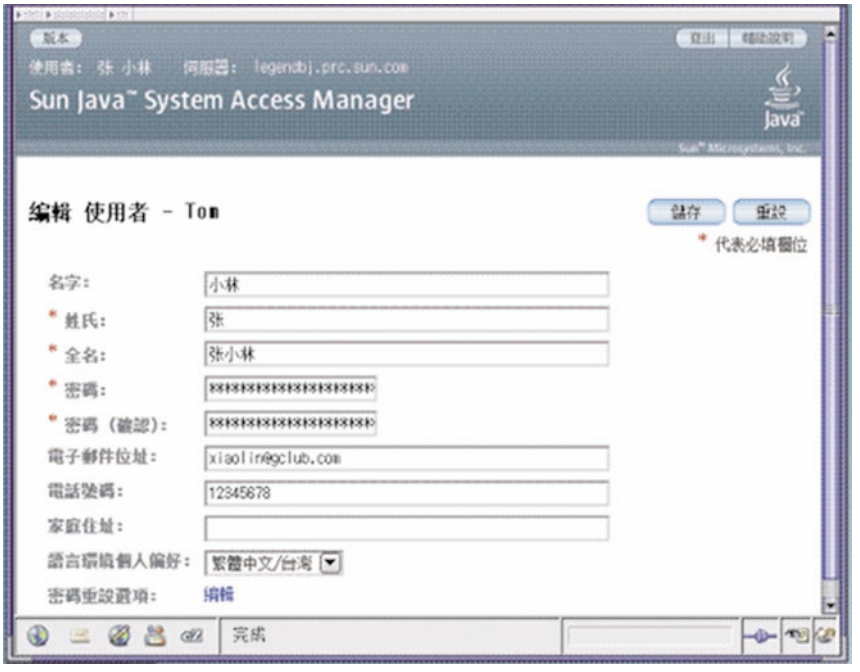

圖 4–4 使用者設定檔檢視

◆ ◆ ◆ 第 5 章

管理範圍

存取控制範圍是一組您可與使用者或使用者群組關聯的認證特性與授權策略。範圍資料儲存於一個專有權資訊樹狀結構中，其爲 Access Manager 於您指定的資料存放區中所建立。Access Manager 框架於 Access Manager 資訊樹狀結構中聚集包含於每一個範圍中的策略與特性。依預設，除使用者資料外，Access Manager 7 會自動地將 Access Manager 資訊樹狀結構做爲特殊的分支插入 Sun Java Enterprise System Directory Server 中。當使用任何 LDAPv3 資料庫時，您可以使用存取控制範圍。

如需有關範圍的詳細資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Technical Overview」。

於 [範圍] 標籤中，您可爲存取控制配置下列特性：

- 第 64 頁的「認證」
- 第 64 頁的「服務」
- 第 65 頁的「權限」

建立及管理範圍

本節描述如何建立及管理範圍。

▼ 建立新的範圍

1 **從 [存取控制] 標籤下的 [範圍] 清單中選取 [新建]。**

2 **定義下列一般屬性：**

名稱　輸入範圍的名稱。

父系　定義您正在建立的範圍位置。選取新範圍將存在處的父系範圍。

3 **定義下列範圍屬性：**

範圍狀態	選擇作用中或非作用中狀態。預設值爲 [作用中]。在範圍存在期間，可以透過選取 [特性] 圖示隨時變更該狀態。登入時，選擇 [非作用中] 以停用使用者存取。
範圍/DNS 別名	允許加入範圍 DNS 名稱的別名。此屬性僅接受「實際的」網域別名 (不允許使用隨機字串)。

4 按一下 [確定] 以儲存，或按一下 [取消] 以返回前一個頁面。

一般特性

[一般特性] 頁面顯示範圍的基本屬性。若要修改這些特性，於 [存取控制] 標籤之下按一下 [範圍名稱] 的範圍。然後，編輯下列特性：

範圍狀態	選擇作用中或非作用中狀態。預設值爲 [作用中]。在範圍存在期間，可以透過選取 [特性] 圖示隨時變更該狀態。登入時，選擇 [非作用中] 以停用使用者存取。
範圍/DNS 別名	允許加入範圍 DNS 名稱的別名。此屬性僅接受「實際的」網域別名 (不允許使用隨機字串)。

一旦您編輯了特性，請按一下 [儲存]。

認證

一般認證服務必須先註冊爲某個範圍的服務，使用者才能使用其他認證模組登入。Access Manager 7 管理員使用核心認證服務可以定義範圍認證參數的預設值。若未於特定認證模組中定義置換值，稍後則可以使用這些值。核心認證服務的預設值定義於 `amAuth.xml` 檔案中，並於安裝後儲存於 Directory Server 之中。

如需詳細資料，請參閱第 7 章

服務

在 Access Manager 中，服務是由 Access Manager 主控台一起管理的屬性群組。屬性可以只是一些相關資訊，如員工名稱、職稱與電子郵件位址。但屬性通常做爲軟體模組的配置參數，如電子郵件應用程式或發薪服務。

經由 [服務] 標籤，您可對範圍新增並配置大量 Access Manager 預設服務。您可以新增下列服務：

- 管理
- 探索服務
- 全域化設定

- 密碼重設
- 階段作業
- 使用者

備註 – Access Manager 強制服務 .xml 檔案中必需的屬性皆具有某些預設值。若您具有無值之必需屬性的服務，您需要新增預設值並重新載入服務。

▼ 將服務新增至範圍

1. **按一下您要新增服務的範圍名稱。**
2. **選取 [服務] 標籤。**
3. **按一下 [服務] 清單中的 [新增]。**
4. **選取您要為範圍新增的服務。**
5. **按 [下一步]。**
6. **定義範圍屬性以配置服務。請參閱線上說明中的「配置」以取得服務屬性的說明。**
7. **按一下 [完成]。**
8. **若要編輯服務的特性，請按一下服務清單中的名稱。**

權限

權限定義對某個範圍內之角色或群組的存取權限。角色或群組被用於 [Access Manager 識別主旨] 類型的策略主旨定義。若要指定或修改權限，按一下您要編輯的角色或群組名稱。您可以指定的權限包括：

- 僅針對策略特性的讀取與寫入存取權
- 所有範圍與策略特性的讀取與寫入存取權
- 所有特性與服務的唯讀存取權

◆ ◆ ◆ 第 6 章

6 資料存放區

資料存放區是一個資料庫，您可在其中儲存使用者屬性與使用者配置資料。

Access Manager 提供一個連接至識別儲存庫架構的識別儲存庫外掛程式。這個新的模型可讓您檢視並擷取 Access Manager 使用者資訊，而不需變更現有的使用者資料庫。Access Manager 架構整合識別儲存庫外掛程式的資料與其他 Access Manager 外掛程式的資料以形成每位使用者的虛擬識別。Access Manager 稍後可在多個識別儲存庫間的認證與授權程序中使用通用識別。當使用者階段作業結束時，將銷毀虛擬使用者識別。

LDAPv3 資料存放區

當以「範圍」與「舊有」兩種模式安裝 Access Manager 時，您可爲任何 LDAPv3 儲存庫建立一個新的資料存放區實例。於下列狀況之下您應選擇 LDAPv3 儲存庫類型：

- 當不需要角色、服務類別 (CoS) 及與前一版的 Access Manager 相容時。
- 當您要使用一個存在的目錄時。
- 當您要對識別儲存庫使用一個非 Sun Java System Directory Server 的目錄伺服器時。
- 當您不需 Access Manager 對識別儲存庫進行寫入時。
- 當您要使用一個平面的「目錄資訊樹狀結構 (DIT)」時。

▼ 建立新的 LDAPv3 資料存放區

下節將描述連接一個通用 LDAPv3 資料存放區的步驟。

1. **選取要新增資料存放區的範圍**。
2. **按一下 [資料存放區] 標籤**。
3. **按一下 [資料存放區] 清單中的 [新建]**。
4. **輸入資料存放區的名稱**。

5 定義 LDAPv3 儲存庫外掛程式的屬性。

6 按一下 [完成]。

LDAPv3 儲存庫外掛程式屬性

下列屬性用於配置 LDAPv3 儲存庫外掛程式：

- 第 73 頁的 「重試之間的延遲時間」
- 第 73 頁的 「需要重試的 LDAPException 錯誤碼」

主 LDAP 伺服器

輸入您要連接的 LDAP 伺服器名稱。格式應爲 `hostname.domainname:portnumber`。

若輸入了多個 `host:portnumber` 項目，則會嘗試連接清單中的第一個主機。僅當連接至目前主機失敗時，才會嘗試清單中的下一個項目。

LDAP 連結 DN

指定 Access Manager 將用來認證您目前所連接之 LDAP 伺服器的 DN 名稱。具有連結所用之 DN 名稱的使用者應具有您配置於 LDAPv3 支援的類型和作業屬性中的正確的新增/修改/刪除特權。

LDAP 連結密碼

指定 Access Manager 將用來認證您目前所連接之 LDAP 伺服器的 DN 密碼。

LDAP 連結密碼 (確認)

確認密碼。

LDAP 組織 DN

此資料儲存庫將對映的 DN 。此將爲於此資料存放區中執行之所有作業的基底 DN。

啓用 LDAP SSL

當啓用時，Access Manger 將使用 HTTPS 通訊協定連線至主伺服器。

LDAP 連接儲存區最小大小

指定連接儲存區中的初始連線數目。使用連接儲存區可避免每次都建立新的連線。

LDAP 連接儲存區最大大小

指定允許的最大連線數目。

從搜尋傳回的最多結果

指定搜尋作業傳回項目的最大數目。若已達到上限，Directory Server 會傳回任何符合搜尋請求的項目。

搜尋逾時

指定搜尋請求所分配的最大秒數。若已達到上限，Directory Server 會傳回任何符合搜尋請求的搜尋項目。

LDAP 依照參照

若啓用，此選項指定自動依照其他 LDAP 伺服器的參照。

LDAPv3 儲存庫外掛程式類別名稱

指定實作 Access Manager 儲存庫外掛程式的類別檔案位置。

屬性名稱對映

啓用將對映至原生資料存放區的框架所知的通用屬性。例如，若框架使用 `inetUserStatus` 來決定使用者狀態，原生資料存放區可以實際使用 `userStatus`。屬性定義區分大小寫。

LDAPv3 外掛程式支援的類型和作業

指定此 LDAP 伺服器允許的或可執行的作業。預設作業是僅限於此 LDAPv3 儲存庫外掛程式支援的作業。以下是 LDAPv3 儲存庫外掛程式支援的作業：

- 群組 — 讀取、建立、編輯、刪除
- 範圍 — 讀取、建立、編輯、刪除、服務
- 使用者 — 讀取、建立、編輯、刪除、服務
- 代理程式 — 讀取、建立、編輯、刪除

您可以根據 LDAP 伺服器的設定與作業

從上述作業移除權限，但您不可以新增更多的權限。

LDAP 使用者搜尋屬性

此欄位定義對使用者進行搜尋的屬性類型。例如，若使用者的 dn 爲 `uid=k user5,ou=people,dc=iplanet,dc=com`，則命名屬性爲 uid。`(uid=*)` 將附加至使用者的搜尋篩選器。

LDAP 使用者搜尋篩選器

指定用於尋找使用者項目的搜尋篩選器。例如，若 LDAP 使用者搜尋屬性爲 uid 而 LDAP 使用者搜尋篩選器爲 `(objectClass=inetorgperson)`，則實際使用者搜尋篩選器將爲：`(&(uid=*)(objectClass=inetorgperson))`。

LDAP 使用者物件類別

指定使用者的物件類別。當建立了一個使用者時，本使用者物件類別清單將新增至使用者的屬性清單。

LDAP 使用者屬性

定義與使用者相關聯的屬性清單。任何不在本清單上的讀取/寫入使用者屬性嘗試皆不被允許。這些屬性區分大小寫。於此處定義物件類別與屬性模式之前，必須在 Directory Server 中定義物件類型與屬性模式。

LDAP 群組搜尋屬性

此欄位定義對群組進行搜尋的屬性類型。例如，若群組 dn 爲 `cn=group1,ou=groups,dc=iplanet,dc=com`，群組的命名屬性爲 cn 而 `(cn=*)` 將附加至群組搜尋篩器。

LDAP 群組搜尋篩選器

指定用於尋找群組項目的搜尋篩選器。例如，如果 LDAP 群組搜尋屬性是 `cn`，而 LDAP 群組搜尋篩選器是 `(objectclass=groupOfUniqueNames)`，則實際的群組搜尋篩選器將爲 `(&(cn=*)(objectclass=groupOfUniqueNames))`。

LDAP 群組容器命名屬性

若群組存在於容器中，請指定群組容器的命名屬性。否則，此屬性將爲空白。例如，如果 `cn=group1,ou=groups,dc=iplanet,dc=com` 的群組 DN 存在於 `ou=groups` 中，則群組容器命名屬性爲 `ou`。

LDAP 群組容器值

指定群組容器值。例如，`cn=group1,ou=groups,dc=iplanet,dc=com` 的群組 DN 存在於容器名稱 `ou=groups` 中，則群組容器值將爲 `groups`。

LDAP 群組物件類別

指定群組的物件類別。當建立了一個群組時，本群組物件類別清單將新增至群組的屬性清單。

LDAP 群組屬性

定義與群組相關聯的屬性清單。任何不在本清單上的讀取/寫入群組屬性嘗試皆不被允許。這些屬性區分大小寫。於此處定義物件類別與屬性模式之前，必須在 Directory Server 中定義物件類型與屬性模式。

群組成員身份的屬性名稱

指定屬性名稱，其值爲 DN 所屬之所有群組的名稱。預設值爲 `memberOf`。

群組成員的屬性名稱

指定屬性名稱，其值爲屬於此群組的 DN。預設值爲 `uniqueMember`。

群組成員 URL 的屬性名稱

指定屬性名稱，其值爲解析爲此群組所屬成員的一個 LDAP URL。預設值爲 `memberUrl`。

LDAP 使用者容器命名屬性

若使用者存在於容器中，請指定使用者容器的命名屬性。若使用者並未位於使用者容器中，此欄位應爲空白。例如，假設使用者 dn `uid=kuser5,ou=people,dc=iplanet,dc=com`，若 `ou=people` 爲使用者容器名稱，則命名屬性爲 `ou`。

LDAP 使用者容器值

指定使用者容器值。預設值爲 `people`。例如，給定使用者 DN `uid=kuser5,ou=people,dc=iplanet,dc=com`，如果 `ou=people` 是使用者容器的名稱，則命名屬性爲 `ou` 且「LDAP 使用者容器值」是 `people`。

代理程式搜尋屬性

此欄位定義對代理程式進行搜尋的屬性類型。預設值爲 `uid`。例如，如果代理程式的 DN 是 `uid=kagent1,ou=agents,dc=iplanet,dc=com`，則其命名屬性爲 uid。`(uid=*)` 將會附加到代理程式的搜尋篩選器。

LDAP 代理程式容器命名屬性

若代理程式位於一個代理程式容器中，則爲代理程式容器的命名屬性。若代理程式並未位於代理程式容器中，此欄位應爲空白。例如，給定使用者 DN `uid=kagent1,ou=agents,dc=iplanet,dc=com`，則代理程式命名屬性爲 `ou`。

LDAP 代理程式容器值

指定代理程式容器值。若代理程式並未位於代理程式容器中，則其爲空白。於前一個範例中，代理程式容器值應爲 `agents`。

LDAP 代理程式搜尋篩選器

定義用來搜尋代理程式的篩選器。[LDAP 代理程式搜尋] 屬性置於此欄位之前以形成實際代理程式搜尋篩選器。

例如，若 [LDAP 代理程式搜尋屬性] 爲 `uid` 而 [LDAP 使用者搜尋篩選器] 爲 `(objectClass=sunIdentityServerDevice)`，則實際使用者搜尋篩選器將爲：`(&(uid=*)(objectClass=sunIdentityServ erDevice))`

LDAP 代理程式物件類別

定義代理程式的物件類別。當建立了一個代理程式時，本使用者物件類別清單將新增至代理程式的屬性清單

LDAP 代理程式屬性

定義與代理程式相關聯的屬性清單。任何不在本清單上的讀取/寫入代理程式屬性嘗試皆不被允許。這些屬性區分大小寫。於此處定義物件類別與屬性模式之前，必須在 Directory Server 中定義物件類型與屬性模式。

永久性搜尋基底 DN

定義用於永久性搜尋的基 DN。某些 LDAPv3 伺服器僅在根字尾層次上支援永久性搜尋。

重新啓動前永久性搜尋最長閒置時間

重新啓動永久性搜尋前，請定義最大閒置時間。此值必須大於 1。若值小於或等於 1，則無論連線的閒置時間爲何，皆將重新啓動搜尋。

若 Access Manager 與載入平衡器同時部署，則某些載入平衡器將在閒置一段特定時間後逾時。於此條件中，您應該將 [重新啓動前永久性搜尋最長閒置時間] 設定爲一個小於載入平衡器之指定時間的值。

出現錯誤碼後的最大重試次數

若遇到 [需要重試的 LDAPException 錯誤碼] 中指定的錯誤碼，請定義永久性搜尋作業的最大重試次數。

重試之間的延遲時間

指定每次重試前的等待時間。僅適用於永久性搜尋連線。

需要重試的 LDAPException 錯誤碼

指定錯誤碼以初始永久性搜尋作業重試。此屬性僅適用於永久性搜尋，並不適用於所有 LDAP 作業。

AMSDK 儲存庫外掛程式

當 Access Manager 以「舊有」模式安裝時，AMSDK 識別儲存庫將自動地與 Access Manager 資訊樹狀結構融合。於「範圍」模式中，您可選擇安裝 AMSDK 儲存庫，但識別儲存庫並未與 Access Manager 資訊樹狀結構融合。於下列狀況之下您應選擇 AMSDK 儲存庫類型：

- 若要利用 Sun Java System Directory Server 的特定功能，如角色和服務類別 (CoS)。
- 若要取得與 Access Manager 先前版本的相容性。

▼ 若要建立一個新的 AMSDK 儲存庫外掛程式

1. **請選取範圍，以便在其中配置 Access Manager 儲存庫外掛程式。**
2. **按一下 [資料存放區] 標籤。**
3. **按一下 [資料存放區] 清單中的 [新建]。**
4. **輸入儲存庫外掛程式的名稱。**

5. **選取 [Access Manager 儲存庫外掛程式]**。
6. **按 [下一步]**。
7. **定義下列欄位：**

Access Manager 外掛程式類別名稱	指定實作 Access Manager 儲存庫外掛程式的類別檔案位置。
Access Manager 組織	指向 Access Manager 所管理 Directory Server 之組織的 DN。此將爲於此資料存放區中執行之所有作業的基底 DN。

8. **按一下 [完成]**。

◆ ◆ ◆ 第 7 章

7 管理認證

認證服務提供一項基於 Web 的使用者介面給所有安裝於 Access Manager 部署中的預設認證模組。該介面提供動態和可自訂的工具，在使用者請求存取時顯示登入需求畫面 (基於呼叫的認證模組) 以匯集認證憑證。該介面使用 Sun Java System™ Application Framework (有時稱爲 *JATO*，它是一種 Java 2 Enterprise Edition (J2EE) 簡報框架，用於協助開發者建立實用的網路應用程式) 建立。

配置認證

本節描述如何配置您部署的認證。第一部分略述預設認證模組類型並提供任何所需的預先配置的指令。您可對範圍、使用者、角色等等配置相同認證模組類型的多重配置實例。此外，您可新增認證鏈接，如此於順利認證之前，認證必須通過多重實例的準則。本節包含：

認證模組類型

認證模組是一個收集使用者資訊 (如使用者 ID 和密碼) 並檢查資料庫中之項目資訊的外掛程式。若使用者提供符合認證準則的資訊，則將對使用者授予所請求資源的存取權。若使用者提供不符合認證準則的資訊，則將拒絕使用者所請求資源的存取權。Access Manager 安裝時附有 15 種認證模組類型。

備註 – 用作認證實例之前，某些認證模組類型需要進行預先配置。如需要，配置步驟將列於模組類型描述之中。

核心

依預設，Access Manager 提供十五種不同的認證模組，以及核心認證模組。核心認證模組爲認證模組提供總體配置。加入及啓用 Active Directory、匿名、基於憑證的認證、HTTP Basic、JDBC、LDAP、任何認證模組之前，必須先加入和啓用核心認證。對預設範圍自動啓用核心和 LDAP 認證兩種模組。

按一下 [進階特性] 按鈕顯示可爲範圍定義的核心認證屬性。全域屬性不適用於範圍，因此將不顯示。

Active Directory

Active Directory 認證模組執行認證的方式與 LDAP 模組相似，但使用的是 Microsoft 的 Active Directory™ 伺服器 (相對於 LDAP 認證模組使用的 Directory Server)。雖然可對 Active Directory 伺服器配置 LDAP 認證模組，但此模組可讓您在相同範圍下同時擁有 LDAP 和 Active Directory 兩種認證模組。

備註 – 在此版本中，Active Directory 認證模組僅支援使用者認證。只有 LDAP 認證模組會支援密碼策略。

匿名

依預設，啓用此模組時，使用者能以 *anonymous* 使用者的身份登入 Access Manager。藉由配置 [有效匿名使用者清單] 屬性，亦可對此模組定義一份匿名使用者清單。授與匿名存取權意味著無需提供密碼即可進行存取。可以將匿名存取權限制爲特定類型的存取權 (例如，讀取存取權或搜尋存取權)，或限制在目錄內的子樹或個別項目中。

憑證

基於憑證的認證需要使用個人數位憑證 (PDC) 來識別和認證使用者。可以將 PDC 配置爲需要與儲存在 Directory Server 中的 PDC 相符，並要根據憑證廢止清單進行驗證。

在對範圍加入基於憑證的認證模組之前，需要完成許多工作。首先，需要確保與 Access Manager 一同安裝之 Web 容器的安全，並對其進行配置，以用於基於憑證的認證。於啓用基於憑證的模組之前，請參閱「*Sun ONE Web Server 6.1* 管理員指南」中的第 6 章「使用證書和金鑰」，以取得這些 Web Server 的初始配置步驟。此文件位於以下位置：

```
http://docs.sun.com/db/prod/s1websrv#hic
```

或者，參閱位於下列位置的「*Sun ONE Application Server Administrator's Guide to Security*」：

http://docs.sun.com/db/prod/s1appsrv#hic (`http://docs.sun.com/db/prod/s1appsrv#hic`)

備註 – 每一位要使用基於憑證的模組進行認證的使用者，必須請求用於使用者瀏覽器的 PDC。根據所使用的瀏覽器不同，會有不同的說明。請參閱您瀏覽器的說明文件，以取得更多資訊。

爲了加入此模組，您必須以範圍管理員的身份登入 Access Manager，並配置 Access Manager 和 Web 容器，以使用 SSL 並啓用用戶端認證。如需更多資訊，請參閱第 3 章。

HTTP Basic

此模組使用基本認證，它是 HTTP 通訊協定內建的認證支援。Web 伺服器發出要求提供使用者名稱和密碼的用戶端請求，並將這些資訊作爲授權請求的一部分傳回伺服器。會擷取該使用者名稱和密碼，從內部將使用者認證至 LDAP 認證模組。爲使 HTTP Basic 正常工作，必須加入 LDAP 認證模組 (僅加入 HTTP Basic 模組將不起作用)。一旦使用者認證成功，其無需提供使用者名稱和密碼即可重新進行認證。

JDBC

Java Database Connectivity (JDBC) 認證模組提供一種機制，可讓 Access Manager 經由提供 JDBC 技術啓用驅動程式的 SQL 資料庫來認證使用者。與 SQL 資料庫的連線可以直接經由 JDBC 驅動程式或 JNDI 連線池。

備註 – 此模組已在 MySQL4.0 和 Oracle 8i 上通過測試。

LDAP

如果使用 LDAP 認證模組，當使用者登入時，他或她必須以特定的使用者 DN 和密碼連結至 LDAP Directory Server。此爲所有基於範圍的認證之預設認證模組。若使用者提供 Directory Server 中的使用者 ID 和密碼，系統將允許此使用者存取有效的 Access Manager 階段作業，並使用該階段作業進行設定。對預設範圍自動啓用核心和 LDAP 認證兩種模組。

成員身份

成員身份認證的實施類似於個人網站，例如：my.site.com 或 mysun.sun.com。啓用此模組時，使用者無需借助管理員，即可建立帳號並將其作爲個人帳號。對於這個新帳號，使用者能以已加入使用者的身份來存取它。還可以存取檢視器介面，此介面作爲授權資料和使用者偏好設定儲存在使用者設定檔資料庫中。

MSISDN

Mobile Station Integrated Services Digital Network (MSISDN) 認證模組會使用如行動電話等裝置相關的行動用戶 ISDN 來啓用認證。這是非互動式模組。此模組擷取用戶 ISDN 並利用 Directory Server 進行驗證，以找到符合該號碼的使用者。

RADIUS

Access Manager 可以配置爲搭配已安裝的 RADIUS 伺服器使用。如果您的企業使用老舊的 RADIUS 伺服器進行認證，這會很有用。啓用 RADIUS 認證模組需要執行兩個步驟：

1. 配置 RADIUS 伺服器。

   如需詳細指示，請參閱 RADIUS 伺服器的文件。

2. 註冊和啓用 RADIUS 認證模組。

與 Sun Java System Application Server 一起配置 RADIUS

當 RADUIS 用戶端與其伺服器形成通訊端連線時，依預設，Application Server 的 server.policy 檔案中僅可有 SocketPermission 的連線權限。爲了使 RADUIS 認證正常工作，需要爲以下動作授與權限：

- 接受
- 連接
- 偵聽
- 解析

若要授予通訊端連線的權限，您必須在應用程式伺服器的 server.policy 檔案中加入一個項目。SocketPermission 由主機規格和一組指定與該主機連線方式的動作組成。主機依如下指令指定：

```
host = hostname | IPaddress:portrange:portrange = portnumber

| -portnumberportnumber-portnumber
```

主機表示爲 DNS 名稱、數字 IP 位址或本端主機 (針對本端機器)。DNS 名稱主機規格中可使用一次萬用字元「*」。如果包含萬用字元，它必須位於最左側，如：*.example.com。

連接埠 (或連接埠範圍) 爲選擇性的。形式爲 N- 的連接埠規格 (其中 N 爲連接埠埠號)，表示號碼爲 N 及大於 N 的所有連接埠。形式爲 -N 的連接埠規格則表示號碼爲 N 及小於 N 的所有連接埠。

偵聽動作僅在與本端主機搭配使用時才有意義。如果存在任何其他動作，則暗含**解析** (解析主機/IP 名稱服務查找) 動作。

例如，建立 SocketPermission 時請注意，如果將以下權限授與某程式碼，則該權限可讓程式碼與 `machine1.example.com` 上的 `port 1645` 連線，並接受該連接埠上的連線：

```
permission java.net.SocketPermission machine1.example.com:1645, "connect,accept";
```

同樣，如果將以下權限授與某程式碼，則該權限可讓程式碼接受本端主機上 1024 至 65535 之間任一連接埠上的連線、與這些連接埠連線或偵聽這些連接埠：

```
permission java.net.SocketPermission "machine1.example.com:1645", "connect,accept";

permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

備註 – 因爲有害的程式碼可以更容易在不擁有資料的存取權的多方中傳輸和共用這些資料，所以將接受或建立與遠端主機連線的權限授與程式碼可能會引發問題。請確保透過指定精確的連接埠號 (而不是指定連接埠號範圍) 僅授與適當的權限。

SafeWord

可配置 Access Manager 以處理對安全運算的 SafeWord™ 或 SafeWord PremierAccess™ 認證伺服器的 SafeWord 認證請求。Access Manager 會提供 SafeWord 認證的用戶端。SafeWord 伺服器可以存在於安裝有 Access Manager 的系統，或是單獨的系統上。

與 Sun Java System Application Server 一起配置 SafeWord

SafeWord 用戶端與其伺服器形成通訊端連線時，依預設，應用程式伺服器的 `server.policy` 檔案中，只允許有 SocketPermission 的**連線**權限。爲了使 SafeWord 認證正常工作，需要爲以下動作授與權限：

- 接受
- 連接
- 偵聽
- 解析

若要授予通訊端連線的權限，您必須在應用程式伺服器的 `server.policy` 檔案中加入一個項目。SocketPermission 由主機規格和一組指定與該主機連線方式的動作組成。主機依如下指令指定：

```
host = (hostname | IPaddress)[:portrange] portrange =

portnumber | -portnumberportnumber-[portnumber]
```

主機表示爲 DNS 名稱、數字 IP 位址或本端主機 (針對本端機器)。DNS 名稱主機規格中可使用一次萬用字元「`*`」。如果包含萬用字元，它必須位於最左側，如：`*.example.com`。

連接埠 (或 portrange) 爲選擇性的。形式爲 N- 的連接埠規格 (其中 N 爲連接埠埠號)，表示號碼爲 N 及大於 N 的所有連接埠。形式爲 -N 的連接埠規格則表示號碼爲 N 及小於 N 的所有連接埠。

偵聽動作僅在與本端主機搭配使用時才有意義。如果存在任何其他動作，則暗含**解析** (解析主機/IP 名稱服務查找) 動作。

例如，建立 SocketPermission 時請注意，如果將以下權限授與某程式碼，則該權限可讓程式碼與 machine1.example.com 上的 port 1645 連線，並接受該連接埠上的連線：

```
permission java.net.SocketPermission machine1.example.com:5030, "connect,accept";
```

同樣，如果將以下權限授與某程式碼，則該權限可讓程式碼接受本端主機上 1024 至 65535 之間任一連接埠上的連線、與這些連接埠連線或偵聽這些連接埠：

```
permission java.net.SocketPermission "machine1.example.com:5030", "connect,accept";

permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

備註 – 因爲有害的程式碼可以更容易在不擁有資料的存取權的多方中傳輸和共用這些資料，所以將接受或建立與遠端主機連線的權限授與程式碼可能會引發問題。請確保透過指定精確的連接埠號 (而不是指定連接埠號範圍) 僅授與適當的權限。

SAML

安全指定標記語言 (SAML) 認證模組擷取並驗證目標伺服器上的 SAML 指定。只有在此模組是配置於目標機器上時 (包括升級後，例如：Access Manager 2005Q1 升級至 Access Manager 2005Q4)，SAML SSO 才有作用。

SecurID

Access Manager 可以配置爲能處理對 RSA 的 ACE/Server 認證伺服器提出之「SecurID 認證」請求。Access Manager 會提供 SecurID 認證的用戶端。ACE/Server 可以存在於安裝有 Access Manager 的系統，或是單獨的系統上。若要對在本機管理的使用者 ID 進行認證 (請參閱 admintool (1M))，需要超級使用者存取權限。

「SecurID 認證」使用認證輔助程式 amsecuridd，它是 Access Manager 主程序以外的單獨程序。此輔助程式會在啓動時偵聽某連接埠，以取得配置資訊。如果安裝了 Access Manager 並以 nobody 身份或非超級使用者的使用者 ID 執行，必須仍以超級使用者身份執行 *AccessManager-base*/SUNWam/share/bin/amsecuridd 程序。如需 amsecuridd 輔助程式的詳細資訊，請參閱第 20 章。

備註 – 在此版本的 Access Manager 中，「SecurID 認證」模組不適用於 Linux 或 Solaris x86 平台，且不應在這兩個平台上註冊、配置或啓用。它僅適用於 SPARC 系統。

UNIX

Access Manager 可以配置爲根據安裝有 Access Manager 的 Solaris 或 Linux 系統上已知的 Unix 使用者 ID 和密碼，處理認證請求。雖然僅有一個範圍屬性和幾個用於 Unix 認證的全域屬性，但仍有一些針對系統的考量。若要對本機管理的使用者 ID 進行認證 (請參閱 `admintool` (1M))，則需要超級使用者存取權限。

「Unix 認證」使用認證 輔助程式 `amunixd`，它是 Access Manager 主程序以外的單獨程序。此輔助程式會在啓動時偵聽某連接埠，以取得配置資訊。每個 Access Manager 只有一個 Unix 輔助程式以供其所有範圍使用。

如果安裝了 Access Manager 並以 `nobody` 身份或非超級使用者的使用者 ID 執行，必須仍以超級使用者身份執行 *AccessManager-base*`/SUNWam/share/bin/amunixd` 程序。Unix 認證模組透過開啓 `localhost:58946` 的通訊端來呼叫 `amunixd` 常駐程式，以偵聽 Unix 認證請求。若要在預設連接埠上執行 `amunixd` 輔助程式程序，請輸入以下指令：

```
./amunixd
```

若要在非預設連接埠上執行 `amunixd`，請輸入下列指令：

```
./amunixd [-c portnm] [ipaddress]
```

IP 位址與連接埠埠號位於 `AMConfig.properties` 的 `UnixHelper.ipadrs` 屬性 (IPV4 格式) 和 `UnixHelper.port` 屬性中。您可透過 `amserver` 指令行公用程式執行 `amunixd` (`amserver` 會自動執行此程序，並從 `AMConfig.properties` 擷取連接埠號和 IP 位址)。

`/etc/nsswitch.conf` 檔案中的 `passwd` 項目會決定是參考 `/etc/passwd` 和 `/etc/shadow` 檔案，還是參考 NIS 來進行認證。

Windows Desktop SSO

「Windows Desktop SSO 認證」模組是基於 Kerberos 的認證外掛程式模組，用於 Windows 2000™。它可讓通過 Kerberos 配送中心 (Kerberos Distribution Center；KDC) 認證的使用者，毋需再次提交登入條件便可通過 Access Manager 的認證 (單次登入)。

使用者透過 SPNEGO (Simple and Protected GSS-API Negotiation Mechanism) 通訊協定向 Access Manager 提出 Kerberos。爲了經由此認證模組來執行基於 Kerberos 的單次登入 Access Manager，在用戶端的使用者必須支援 SPNEGO 通訊協定，才能自我認證。通常，任何支援此通訊協定的使用者應該都能使用這個模組對 Access Manager 進行認證。視用戶端記號的可用性而定，此模組會提供 SPENGO 記號或 Kerberos 記號 (不論那一個，通訊協定都相同)。於 Windows 2000 (或更新版本) 上執行的 Microsoft Internet Explorer (5.01 或更新版本) 目前支援此通訊協定。此外，Solaris (9 和 10) 上的 Mozilla 1.4 具有 SPNEGO 支援，但只會傳回 KERBEROS 記號，因爲 Solaris 不支援 SPNEGO。

備註 – 您必須使用 JDK 1.4 或更新版本，才能利用 Kerberos V5 認證模組的新功能和 Java GSS API，在此 SPNEGO 模組中執行基於 Kerberos 的 SSO。

使用的已知限制

若在 WindowsDesktopSSO 認證時使用的是 Microsoft Internet Explorer 6.x，且瀏覽器不具使用者的 Kerberos/SPNEGO 記號 (符合 WindowsDesktopSSO 模組中配置的 (KDC) 範圍) 之存取權，則在瀏覽器對 WindowsDesktopSSO 模組的認證失敗後，瀏覽器對其他模組的運作也會不正確。導致此問題的直接原因在於當 Internet Explorer 無法執行 WindowsDesktopSSO 模組時，即使出現回呼的提示，瀏覽器也無法將回呼 (屬於其他模組) 傳遞至 Access Manager，除非瀏覽器重新啓動。由於 Null 使用者憑證，因此 WindowsDesktopSSO 之後的所有模組都將失敗。

請參閱下列文件以取得相關資訊：

http://support.microsoft.com/default.aspx?scid=kb;en-us;308074
(`http://support.microsoft.com/default.aspx?scid=kb;en-us;308074`)

http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM
(`http://support.microsoft.com/default.aspx?scid=kb;en-us;308074`)

配置 Windows Desktop SSO

啓用 Windows Desktop SSO 認證是一個具有兩個步驟的程序：

1. 在 Windows 2000 網域控制器中建立一個使用者
2. 設定 Internet Explorer。

▼ 要在 Windows 2000 網域控制器中建立一個使用者

1 在網域控制器中，建立針對 [Access Manager 認證] 模組的使用者帳號。

a. 從 [開始] 功能表移至 [程式集] > [管理工具]。

b. 選取 [使用者與電腦]。

c. 建立含 Access Manager 主機名稱的新使用者，以作為使用者 ID (登入名稱)。Access Manager 主機名稱不應包含網域名稱。

2 將使用者帳號與服務提供者名稱產生關聯，並將 keytab 檔案匯出至安裝了 Access Manager 的系統。若要進行上述動作，請執行下列指令：

`ktpass -princ host/`*`hostname.domainname`*`@DCDOMAIN -pass password -mapuser userName-out`

`hostname``.host.keytab`

`ktpass -princ HTTP/`*`hostname.domainname`*`@DCDOMAIN -pass`

`password` `-mapuser` *`userName`*`-out` *`hostname`*

`.HTTP.keytab`

`ktpass` 指令接受下列參數：

hostname。執行 Access Manager 的主機名稱 (不含網域名稱)。

domainname。Access Manager 網域名稱。

DCDOMAIN。網域控制器的網域名稱。此名稱可能與 Access Manager 的網域名稱不同。

password。使用者帳號的密碼。請確定密碼正確，因爲 `ktpass` 不會驗證密碼。

userName。使用者帳號 ID。它應該與 hostname 相同。

備註 – 請確保兩個 keytab 檔案均已做好安全措施。

服務範本值應類似於以下範例：

服務主體： `HTTP/machine1.EXAMPLE.COM@ISQA.EXAMPLE.COM`

Keytab 檔案名稱：`/tmp/machine1.HTTP.keytab`

Kerberos 範圍： `ISQA.EXAMPLE.COM`

Kerberos 伺服器名稱：`machine2.EXAMPLE.com`

使用網域名稱傳回主體：`false`

認證層級： `22`

3 **重新啓動伺服器**。

▼ 設定 Internet Explorer

上述步驟適用於 Microsoft Internet Explorer™ 6 及更高版本。若您是使用較早的版本，請確定 Access Manager 在瀏覽器的網際網路區域內，並啓用 Windows 原有的認證 (Native Windows Authentication)。

1 **在 [工具] 功能表中，移至 [網際網路選項] > [進階/安全性] > [安全性]**。

2 **選取 [整合 Windows 認證] 選項**。

3 **移至 [安全性] > [本機網際網路]**。

   a. **選取 [自訂層級]。在 [使用者認證/登入] 面板中，選取 [僅於內部網路域內自動登入] 選項**。

   b. **前往 [網站] 並選取所有選項**。

   c. **按一下 [進階] ，並將 Access Manager 加入至本機區域 (若尚未加入的話)**。

Windows NT

Access Manager 可以配置爲搭配已安裝的 Windows NT /Windows 2000 伺服器使用。Access Manager 會提供 NT 認證的用戶端。

1. 配置 NT 伺服器。如需詳細說明，請參閱 Windows NT 伺服器的文件。
2. 加入和啓用 Windows NT 認證模組之前，您必須先取得和安裝 Samba 用戶端，以便與 Solaris 系統上的 Access Manager 進行通訊。

安裝 Samba Client

爲啓用 Windows NT 認證模組，Samba Client2.2.2 必須下載並安裝於下列目錄中：

```
AccessManager-base/SUNWam/bin
```

Samba Client 是一種檔案與列印伺服器，用於不需要單獨的 Windows NT/2000 Server 而將 Windows 和 UNIX 機器結合在一起。如需更多資訊及下載，請於以下位置存取：http://wwws.sun.com/software/download/products/3e3af224.html。

Red Hat Linux 隨附 Samba 用戶端，其所在目錄如下：

```
/usr/bin
```

若要使用 Linux 的 Windows NT 認證模組，請將用戶端二進位複製到下列 Access Manager 目錄中：

AccessManager-base`/sun/identity/bin`

備註 – 如果您有多個介面，則需要額外的配置。多重介面可以透過 `smb.conf` 檔案中的配置設定，以傳遞到 `mbclient`。

認證模組實例

根據預設認證模組，可爲範圍建立多重認證模組實例。您可個別地新增相同認證模組之已配置的多重實例。

▼ 建立新的認證模組實例

1 按一下您要新增認證模組實例的範圍名稱。

2 選取 [認證] 標籤。

備註 – [管理員認證配置] 按鈕僅定義管理員的認證服務。若管理員的認證模組必須與一般使用者的認證模組不同，則可以使用此屬性。配置於此屬性中的模組將在存取 Access Manager 主控台時被挑選出來。

3 **按一下 [模組實例] 清單中的 [新建]。**

4 **輸入認證模組實例的名稱。該名稱必須是唯一的。**

5 **選取範圍之認證模組類型的 [類型]。**

6 **按一下 [建立]。**

7 **按一下剛建立的模組實例名稱並編輯該模組的特性。請參閱線上說明中的「認證」一節，以取得每個模組類型特性的定義。**

8 **重複這些步驟以新增多重模組實例。**

認證鏈接

可以配置一個以上的認證模組，因此使用者必需傳送認證憑證給其全體。這稱爲認證鏈接。Access Manager 中的認證鏈接可使用整合於認證服務中的 JAAS 框架來達成。模組鏈結配置於認證配置服務底下。

▼ 建立新的認證鏈接

1 **按一下您要新增認證鏈接的範圍名稱。**

2 **選取 [認證] 標籤。**

3 **按一下 [認證鏈接] 清單中的 [新建]。**

4 **輸入此認證鏈接的名稱。**

5 **按一下 [建立]。**

6 **按一下 [新增] 以定義您要包括於鏈接中的認證模組實例。若要這麼做，請由實例清單中選取模組實例名稱。顯示於此清單中的模組實例名稱是在模組實例屬性中所建立的。**

7 **選取鏈接的條件。這些旗標為定義這些旗標的認證模組建立實施準則。此實施具有階層結構。[必要的] 為最高階層而 [可選的] 為最低階層：**

必要條件	模組實例必須成功。若成功，認證將繼續進行至 [認證鏈接] 清單中的下一個選項。如果失敗，控制立即返回應用程式 (認證將不會繼續 [認證鏈接] 清單中的下一個選項)。
必要的	此模組的認證過程必須成功。若鏈接中任何一個必要模組失敗了，則整個認證鏈接將完全失敗。然而，無論必要模組成功與否，控制將繼續進行至鏈接中的下一個模組。
充足的	模組實例不必要成功。若其確實成功，控制將立即返回應用程式 (認證將不進行至模組實例清單的下一個選項)。若失敗，認證將繼續進行至 [認證鏈接] 清單中的下一個選項。
可選的	模組實例不必要成功。無論成功或失敗，認證都將繼續進行至 [認證鏈接] 清單中的下一個選項。

8 **輸入鏈接的選項。允許此模組使用的其他選項，格式為鍵=值對。多重選項由空格分隔。**

9 **定義下列屬性：**

成功登入 URL	指定使用者認證成功後將重新導向至的 URL。
登入失敗 URL	指定使用者認證失敗後將重新導向至的 URL。
認證後處理類別	定義於登入成功或失敗後用來自訂認證後處理的 Java 類別名稱。

10 **按一下 [儲存]。**

認證類型

認證服務提供不同的方式讓認證套用。這些不同的認證方法可藉由指定登入 URL 參數或透過認證 API 來獲取 (請參閱使用者指南中「Sun Java System Access Manager 7 2005Q4 Developer's Guide」中的第 5 章「Using Authentication APIs and SPIs」以取得更多資訊) 。配置認證模組之前，必須先修改 [核心認證] 服務屬性 [範圍認證模組]，使之包括特定的認證模組名稱。

認證配置服務用於爲以下任一認證類型定義認證模組：

- 第 88 頁的 「基於範圍的認證」
- 第 90 頁的 「基於組織的認證」
- 第 92 頁的 「基於角色的認證」
- 第 95 頁的 「基於服務的認證」
- 第 97 頁的 「基於使用者的認證」
- 第 99 頁的 「基於認證層級的認證」
- 第 101 頁的 「基於模組的認證」

爲這些認證類型之一定義認證模組後，便可以將此模組配置爲根據認證程序成敗提供重新導向 URL 以及處理後的 Java 類別規格。

認證類型決定存取的方式

這些方法的每一種，使用者都可以核准或是拒絕認證。一旦做出決定，每種方法都會依照此程序。步驟 1 至步驟 3 依照成功的認證；步驟 4 依照成功與失敗兩者的認證。

1. Access Manager 確認認證的使用者是否定義於 Directory Server 資料存放區中，且設定檔是否於使用中。

   核心認證模組中的使用者設定檔屬性可以定義爲**必需**、**動態**、**隨使用者別名動態變化**或**忽略**。認證成功之後，Access Manager 會確認 Directory Server 資料庫中是否定義了要認證的使用者，並且如果使用者設定檔值爲**必需**，再確認設定檔是否在使用中。這是預設情形。如果使用者設定檔爲**動態配置**，認證服務將會在 Directory Server 資料庫中建立使用者設定檔。若使用者設定檔設定爲**忽略**，將不會完成使用者驗證。

2. 認證處理後 SPI 的執行完成。

   核心認證模組包含認證處理後類別屬性，其中可能納入認證處理後類別名稱爲其值。`AMPostAuthProcessInterface` 是處理後介面。它可以執行於成功或失敗認證上或是在登出後。

3. 下列特性會加入階段作業記號，或在階段作業記號中更新，而使用者的階段作業會啓動。

   realm。這是使用者歸屬的範圍 DN。

   Principal。這是使用者的 DN。

   Principals。這是使用者已認證過的名稱清單。此屬性可能有一項以上的值定義爲以管道分隔的清單。

   UserId。這是使用者的 DN (與模組傳回的相同)，或在非 LDAP 或 Membership 模組的情況下，爲使用者名稱。(所有主體都必需對映到相同的使用者。UserID 爲它們所對映之使用者 DN。)

   備註 – 此特性可爲非 DN 值。

   UserToken。這是使用者名稱。(所有主體都必需對映到相同的使用者。UserToken 爲它們所對映之使用者名稱。)

   Host。這是用戶端的主機名稱或是 IP 位址。

   authLevel。這是使用者已認證過的最高層級。

   AuthType。這是已認證其使用者的認證模組之以直線符號分隔的清單 (例如，`module1|module2|module3`)。

   clientType。這是用戶端瀏覽器的裝置類型。

   Locale。這是用戶端的語言環境。

   CharSet。這是決定用於用戶端的字元集。

Role。僅適用於基於角色的認證，此爲使用者歸屬的角色。

Service。僅適用於基於服務的認證，此爲使用者歸屬的服務。

4. 在成功或失敗認證後，Access Manager 會尋找重新導向使用者的位置之相關資訊。

   URL 重新導向目的位置可以是 Access Manager 頁面或 URL。重新導向會依據優先順序進行，Access Manager 則根據認證方法及認證是否已成功或已失敗，依此優先順序尋找重新導向。此順序詳述於下列認證方法章節的重新導向部分。

URL 重新導向

於認證配置服務中，您可爲成功或失敗的認證指定 URL 重新導向。URL 本身在此服務的 [登入成功 URL] 和 [登入失敗 URL] 屬性中定義。爲了啓用 URL 重新導向，您必須將認證配置服務加入您的範圍，使之可用於角色、範圍或使用者的配置。在加入認證配置服務時，請確定您加入的是認證模組，例如 LDAP - REQUIRED。

基於範圍的認證

此認證方法可讓使用者對一個範圍或子範圍進行認證。此爲 Access Manager 的預設認證方法。範圍的認證方法是透過對範圍註冊核心認證模組，並定義範圍認證配置屬性來設定的。

基於範圍的認證登入 URL

藉由定義 `realm` 參數或 `domain` 參數，可於使用者介面登入 URL 中指定認證的範圍。由下列項目決定認證的請求範圍，其優先順序爲：

1. `domain` 參數。
2. `realm` 參數。
3. 管理服務中的 `DNS` **別名**屬性值。

   於呼叫正確的範圍後，將從核心認證服務的範圍認證配置屬性擷取使用者將認證的認證模組。用來指定並初始基於範圍的認證的登入 URL 爲：

   ```
   http://server_name.domain_name:port/amserver/UI/Login

   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name

   http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name
   ```

   若無定義的參數，則將從指定於登入 URL 中的伺服器主機和網域決定範圍。

基於範圍的認證重新導向 URL

於基於組織的認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於範圍的認證重新導向 URL

成功的基於範圍的認證重新導向 URL 是依優先順序檢查下列位置來決定：

1. 認證模組設定的 URL。
2. `goto` 登入 URL 參數設定的 URL。
3. 使用者設定檔 (`amUser.xml`) 的 `iplanet-am-user-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
4. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
5. 使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
6. 於 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
7. 設定於使用者設定檔 (`amUser.xml`) 之 `iplanet-am-user-success-url` 屬性中的 URL。
8. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性中設定的 URL。
9. 設定於使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性中的 URL。
10. `iplanet-am-auth-login-success-url` 屬性中設定的 URL，作爲全域預設值。

失敗的基於範圍的認證重新導向 URL

失敗的基於範圍的認證重新導向 URL 是以下列順序檢查下列位置來決定：

1. 認證模組設定的 URL。
2. `gotoOnFail` 登入 URL 參數設定的 URL。
3. 對使用者項目 (`amUser.xml`) 的 `iplanet-am-user-failure-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。
4. 使用者角色項目的 `iplanet-am-auth-login-failure-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
5. 對使用者範圍項目的 `iplanet-am-auth-login-failure-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。
6. 於 `iplanet-am-auth-login-failure-url` 屬性之 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
7. 於使用者項目 (`amUser.xml`) 中設定 `iplanet-am-user-failure-url` 屬性的 URL。
8. 針對使用者角色項目之 `iplanet-am-auth-login-failure-url` 屬性設定的 URL。
9. 設定使用者範圍項目之 `iplanet-am-auth-login-failure-url` 屬性的 URL。
10. 針對 `iplanet-am-auth-login-failure-url` 屬性設定的 URL，作爲全域預設值。

若要配置基於範圍的認證

要爲範圍設定認證模組，先對範圍新增核心認證服務。

▼ 若要配置範圍的認證屬性

1. **瀏覽至您要新增認證鏈接的範圍。**
2. **按一下 [認證] 標籤。**
3. **由下拉式功能表選取 [預設認證鏈接]。**
4. **由下拉式功能表選取 [管理認證鏈接]。如果需要管理員的認證模組與使用者的認證模組有所不同，則可以使用此屬性。預設認證模組為 LDAP。**
5. **定義了認證鏈接之後，按一下 [儲存]。**

基於組織的認證

此認證類型僅可套用至以「舊有」模式安裝的 Access Manager 部署。

此認證方法可讓使用者對一個組織或子組織進行認證。它是 Access Manager 的預設認證方法。用於組織的認證方法是透過註冊核心認證模組到組織，並定義組織認證配置屬性來設定的。

基於組織的認證登入 URL

藉由定義 `org` 參數或 `domain` 參數，可以在使用者介面登入 URL 中指定認證的組織。用於認證的請求組織從下列決定，優先順序爲：

1. `domain` 參數。
2. `org` 參數。
3. 管理服務中 `DNS` **別名** (組織別名) 屬性的值。

   在呼叫正確的組織後，會從核心認證服務的組織認證配置屬性擷取使用者將認證的認證模組。用於指定和初始化基於組織的認證的登入 URL 爲：

   ```
   http://server_name.domain_name:port/amserver/UI/Login

   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name

   http://server_name.domain_name:port/amserver/UI/Login?org=org_name
   ```

   如果沒有定義的參數，將從登入中的伺服器主機和網域決定組織。

基於組織的認證重新導向 URL

於基於組織的認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於組織的認證重新導向 URL

成功的基於組織的認證，其重新導向 URL 是以此優先順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `goto` 登入 URL 參數設定的 URL。
3. 使用者設定檔 (`amUser.xml`) 的 `iplanet-am-user-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
4. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
5. 對使用者組織項目的 `iplanet-am-auth-login-success-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。
6. 於 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
7. 設定於使用者設定檔 (`amUser.xml`) 之 `iplanet-am-user-success-url` 屬性中的 URL。
8. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性中設定的 URL。
9. 使用者組織項目之 `iplanet-am-auth-login-success-url` 屬性中設定的 URL。
10. `iplanet-am-auth-login-success-url` 屬性中設定的 URL，作爲全域預設值。

失敗的基於組織的認證重新導向 URL

失敗的基於組織的認證，其重新導向 URL 是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `gotoOnFail` 登入 URL 參數設定的 URL。
3. 對使用者項目 (`amUser.xml`) 的 `iplanet-am-user-failure-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。
4. 使用者角色項目的 `iplanet-am-auth-login-failure-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
5. 對使用者組織項目的 `iplanet-am-auth-login-failure-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。
6. 於 `iplanet-am-auth-login-failure-url` 屬性之 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
7. 於使用者項目 (`amUser.xml`) 中設定 `iplanet-am-user-failure-url` 屬性的 URL。
8. 針對使用者角色項目之 `iplanet-am-auth-login-failure-url` 屬性設定的 URL。
9. 針對使用者組織項目之 `iplanet-am-auth-login-failure-url` 屬性設定的 URL。

10. 針對 iplanet-am-auth-login-failure-url 屬性設定的 URL，作爲全域預設值。

若要配置基於組織的認證

要爲組織設定認證模組，先爲組織加入核心認證服務。

▼ 若要配置組織的認證屬性

1. **瀏覽至您要新增認證鏈接的組織。**
2. **按一下 [認證] 標籤。**
3. **由下拉式功能表選取 [預設認證鏈接]。**
4. **由下拉式功能表選取 [管理認證鏈接]。如果需要管理員的認證模組與使用者的認證模組有所不同，則可以使用此屬性。預設認證模組為 LDAP。**
5. **定義了認證鏈接之後，按一下 [儲存]。**

基於角色的認證

此認證方法可讓使用者對組織或是子組織之中的角色 (靜態或篩選) 進行認證 。

備註 – 於認證配置服務可註冊爲實例或角色之前，必需先註冊至範圍中。

若要成功認證，使用者必需屬於該角色，並且必需認證到爲該角色配置的認證配置服務實例中定義的每個模組。對每個基於角色的認證之實例，可指定下列屬性：

衝突解決層級。 這爲認證配置服務實例 (爲包含相同使用者的不同角色所定義) 設定優先層級。例如，如果同時將 User1 指定給 Role1 與 Role2，可設定較高的衝突解決層級給 Role1，以便在使用者嘗試認證時，Role1 將具有較高的成功或失敗重新導向及認證後程序優先順序。

認證配置。這會定義針對角色的認證程序配置之認證模組。

登入成功 **URL**。此項定義在成功認證上重新導向使用者的 URL。

登入失敗 **URL**。此項定義在失敗認證上重新導向使用者的 URL。

認證處理後類別。此將定義後認證介面。

基於角色的認證登入 URL

透過定義角色參數，可以在使用者介面登入 URL 中指定基於角色的認證。在呼叫正確的角色後，會從爲角色定義的認證配置服務實例擷取使用者將認證的認證模組。

用於指定和初始化基於角色的認證的登入爲：

```
http://server_name.domain_name:port/amserver/UI/Login?role=role_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&role=role_name
```

如果未配置範圍參數，會從指定於登入 URL 自身中的伺服器主機和網域決定角色所屬的範圍。

基於角色的認證重新導向 URL

於基於角色的認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於角色的認證重新導向 URL

成功的基於角色的認證，其重新導向 URL 是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `goto` 登入 URL 參數設定的 URL。
3. 使用者設定檔 (`amUser.xml`) 的 `iplanet-am-user-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
4. 已對其認證使用者之角色的 `iplanet-am-auth-login-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
5. 已認證使用者另一個角色項目的 `iplanet-am-auth-login-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。(如果前一個重新導向 URL 失敗，此選項爲備案。)
6. 使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
7. 於 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
8. 設定於使用者設定檔 (`amUser.xml`) 之 `iplanet-am-user-success-url` 屬性中的 URL。
9. 已對其認證使用者的角色之 `iplanet-am-auth-login-success-url` 屬性中設定的 URL。
10. 已認證使用者另一個角色項目之 `iplanet-am-auth-login-success-url` 屬性中設定的 URL。(如果前一個重新導向 URL 失敗，此選項爲備案。)
11. 設定於使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性中的 URL。
12. `iplanet-am-auth-login-success-url` 屬性中設定的 URL，作爲全域預設值。

失敗的基於角色的認證重新導向 URL

失敗的基於角色的認證，其重新導向 URL 是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. goto 登入 URL 參數設定的 URL。
3. 使用者設定檔 (amUser.xml) 的 iplanet-am-user-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
4. 已對其認證使用者之角色的 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
5. 已認證使用者另一個角色項目的 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL。(如果前一個重新導向 URL 失敗，此選項爲備案。)
6. 對使用者範圍項目的 iplanet-am-auth-login-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
7. 於 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL，做爲全域預設值。
8. 於使用者設定檔 (amUser.xml) 之 iplanet-am-user-failure-url 屬性中設定的 URL。
9. 已對其認證使用者的角色之 iplanet-am-auth-login-failure-url 屬性中設定的 URL。
10. 已認證使用者另一個角色項目之 iplanet-am-auth-login-failure-url 屬性中設定的 URL。(如果前一個重新導向 URL 失敗，此選項爲備案。)
11. 設定於使用者範圍項目之 iplanet-am-auth-login-failure-url 屬性中的 URL。
12. 於 iplanet-am-auth-login-failure-url 屬性中設定的 URL，作爲全域預設值。

▼ 若要配置基於角色的認證

1 瀏覽至您將新增認證配置服務的範圍 (或組織)。

2 按一下 [主旨] 標籤。

3 篩選的角色或角色。

4 選取要設定認證配置的角色。

若尚未將認證配置服務新增至角色，請按一下 [新增]，選取 [認證服務]，再按一下 [下一步]。

5 由下拉式功能表選取您要啓用的 [預設認證鏈接]。

6 按一下 [儲存]。

備註 – 如果您要建立新的角色，系統不會自動爲此角色指定認證配置服務。請確定先選取角色設定檔頁面頂部的 [認證配置服務] 選項，然後再建立角色。

啓用基於角色的認證後，可以保留 LDAP 認證模組做爲預設方式，因爲無需配置成員身份。

基於服務的認證

此認證方法可讓使用者對特定的服務或註冊至範圍或子範圍的應用程式進行認證。服務配置爲認證配置服務中的服務實例並且與一個實例名稱相關。若要成功認證，使用者必需認證到每個爲服務配置的認證配置服務實例中定義的模組。對每個基於服務的認證之實例，可指定下列屬性：

認證配置。這會定義針對 service 的認證程序配置之認證模組。

登入成功 **URL**。此項定義在成功認證上重新導向使用者的 URL。

登入失敗 **URL**。此項定義在失敗認證上重新導向使用者的 URL。

認證處理後類別。此將定義後認證介面。

基於服務的認證登入 URL

透過定義服務參數，可以在使用者介面登入中指定基於服務的認證。在呼叫服務後，會從爲服務定義的認證配置服務實例擷取使用者將認證的認證模組。

用於指定和初始化基於服務的認證的登入 URL 爲：

```
http://server_name.domain_name:port/amserver/UI/

Login?service=auth-chain-name
```

和

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&service=auth-chain-name
```

e

如果沒有配置 org 參數，將從指定於登入 URL 自身中的伺服器主機和網域決定範圍。

基於服務的認證重新導向 URL

於基於服務的認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於服務的認證重新導向 URL

成功的基於服務的認證，其重新導向 URL 是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. goto 登入 URL 參數設定的 URL。
3. 使用者設定檔 (amUser.xml) 的 iplanet-am-user-success-url 屬性之 clientType 自訂檔案中設定的 URL。
4. 已對其認證使用者之服務的 iplanet-am-auth-login-success-url 屬性之 clientType 自訂檔案中設定的 URL。
5. 使用者角色項目之 iplanet-am-auth-login-success-url 屬性的 clientType 自訂檔案中設定的 URL。
6. 使用者範圍項目之 iplanet-am-auth-login-success-url 屬性的 clientType 自訂檔案中設定的 URL。
7. 於 iplanet-am-auth-login-success-url 屬性的 clientType 自訂檔案中設定的 URL，做爲全域預設值。
8. 設定於使用者設定檔 (amUser.xml) 之 iplanet-am-user-success-url 屬性中的 URL。
9. 已對其認證使用者的服務之 iplanet-am-auth-login-success-url 屬性中設定的 URL。
10. 使用者角色項目之 iplanet-am-auth-login-success-url 屬性中設定的 URL。
11. 設定於使用者範圍項目之 iplanet-am-auth-login-success-url 屬性中的 URL。
12. iplanet-am-auth-login-success-url 屬性中設定的 URL，作爲全域預設值。

失敗的基於服務的認證重新導向 URL

失敗的基於服務的認證，其重新導向是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. goto 登入 URL 參數設定的 URL。
3. 使用者設定檔 (amUser.xml) 的 iplanet-am-user-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
4. 已對其認證使用者之服務的 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
5. 使用者角色項目的 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
6. 對使用者範圍項目的 iplanet-am-auth-login-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
7. 於 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL，做爲全域預設值。
8. 設定於使用者設定檔 (amUser.xml) 之 iplanet-am-user-failure-url 屬性中的 URL。
9. 已對其認證使用者的服務之 iplanet-am-auth-login-failure-url 屬性中設定的 URL。

10. 於使用者角色項目之 iplanet-am-auth-login-failure-url 屬性中設定的 URL。
11. 設定於使用者範圍項目之 iplanet-am-auth-login-failure-url 屬性中的 URL。
12. 於 iplanet-am-auth-login-failure-url 屬性中設定的 URL，作爲全域預設值。

▼ 若要配置基於服務的認證

加入認證配置服務之後，爲服務設定認證模組。若要如此，請：

1. **選擇您要配置基於服務的認證的範圍。**
2. **按一下 [認證] 標籤。**
3. **建立認證模組實例。**
4. **建立認證鏈接。**
5. **按一下 [儲存]。**
6. **若要存取範圍的基於服務的認證，請輸入下列位址：**

   http://*server_name.domain_name:port*/amserver/UI/Login?realm=*realm_name&service=auth-chain-name*

基於使用者的認證

此認證方法可讓使用者對特別爲使用者配置的認證程序進行認證。該程序被配置爲使用者設定檔中使用者認證配置屬性的值。若要成功認證，使用者必需認證到每個定義的模組。

基於使用者的認證登入 URL

透過定義使用者參數，可以在使用者介面登入中指定基於使用者的認證。在呼叫正確的使用者後，將從爲使用者定義的使用者認證配置服務實例擷取使用者將認證的認證模組。

用於指定和初始化基於角色的認證的登入爲：

```
http://server_name.domain_name:port/amserver/UI/Login?user=user_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&user=user_name
```

如果沒有配置的範圍參數，會從指定於登入 URL 自身中的伺服器主機和網域決定角色所屬的範圍。

使用者別名清單屬性

在接收基於使用者的認證的請求時，認證服務會先驗證使用者是有效的使用者，然後爲其擷取認證配置資料。在有一個以上有效使用者設定檔與使用者參數有關的情形時，所有的設定檔必需對映到指定的使用者。使用者設定檔中的使用者別名屬性 (`iplanet-am-user-alias-list`) 是能定義其他屬於該使用者的設定檔之位置。如果對映失敗，則使用者會受到有效階段作業的拒絕。異常將是若其中一個使用者爲一個頂層管理，則使用者對映驗證並未執行並給予使用者最高的管理權限。

基於使用者的認證重新導向 URL

於基於使用者的認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於使用者的認證重新導向 URL

成功的基於使用者的認證，其重新導向是以此優先順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `goto` 登入 URL 參數設定的 URL。
3. 使用者設定檔 (`amUser.xml`) 的 `iplanet-am-user-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
4. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
5. 使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
6. 於 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
7. 設定於使用者設定檔 (`amUser.xml`) 之 `iplanet-am-user-success-url` 屬性中的 URL。
8. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性中設定的 URL。
9. 設定於使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性中的 URL。
10. `iplanet-am-auth-login-success-url` 屬性中設定的 URL，作爲全域預設值。

失敗的基於使用者的認證重新導向 URL

失敗的基於使用者的認證，其重新導向 URL 是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `gotoOnFail` 登入 URL 參數設定的 URL。
3. 對使用者項目 (`amUser.xml`) 的 `iplanet-am-user-failure-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。

4. 使用者角色項目的 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
5. 對使用者範圍項目的 iplanet-am-auth-login-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
6. 於 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL，做爲全域預設值。
7. 於使用者項目 (amUser.xml) 中設定 iplanet-am-user-failure-url 屬性的 URL。
8. 針對使用者角色項目之 iplanet-am-auth-login-failure-url 屬性設定的 URL。
9. 設定使用者範圍項目之 iplanet-am-auth-login-failure-url 屬性的 URL。
10. 針對 iplanet-am-auth-login-failure-url 屬性設定的 URL，作爲全域預設值。

▼ 若要配置基於使用者的認證

1 瀏覽至您要為使用者配置認證的範圍。

2 按一下 [主旨] 標籤並按一下 [使用者]。

3 按一下您要修改的使用者名稱

[使用者設定檔] 隨即顯示。

備註 – 如果您要建立新的使用者，系統不會自動爲此使用者指定認證配置服務。請確定先於服務設定檔中選取 [認證配置服務] 選項，然後再建立使用者。如果未選取此選項，使用者將無法繼承爲角色定義的認證配置。

---

4 於使用者認證配置屬性中，選取您要套用的認證鏈接。

5 按一下 [儲存]。

基於認證層級的認證

每個認證模組均可與其認證層級的整數值相關聯。藉著按一下 [服務配置] 中認證模組的 [特性] 箭頭，並變更模組之 [認證層級] 屬性的相應值，可以指定認證層級。使用者在一個或多個認證模組中經過認證後，較高的認證層級爲使用者定義較高的信任層級。

對模組成功認證使用者後，將在使用者的 SSO 記號上設定認證層級。若必須對多個認證模組認證使用者，同時也成功完成這些認證，將會在使用者的 SSO 記號中設定最高認證層級值。

若使用者嘗試存取服務，服務可檢查使用者的 SSO 記號中之認證層級，來決定是否允許使用者進行存取。然後，它將重新導向使用者以標記的認證層級通過認證模組。

使用者還可以使用特定的認證層級存取認證模組。例如，某使用者使用以下語法執行登入：

```
http://hostname:port/deploy_URI/UI/Login?authlevel=
```

auth_level_value

其認證層級大於或等於 *auth_level_value* 的所有模組將顯示爲認證功能表，供使用者選擇。如果僅找到一個相符的模組，則會直接顯示此認證模組的登入頁面。

此認證方法可讓管理員指定可認證身份的模組的安全層級。每個認證模組都有個別的認證層級屬性，而此屬性的值可以被定義爲任何有效的整數。藉由認證基於層級的認證，認證服務使用包含認證模組具有等於或大於參數中指定值的認證層級的功能表顯示模組登入頁。使用者可從現有的清單選取一個模組。一旦使用者選取模組後，剩餘的程序則根據基於模組的認證。

基於認證層級的認證登入 URL

透過定義 參數，可以在使用者介面登入中指定認證基於層級的認證。在以模組的相關清單呼叫登入螢幕後，使用者必需選擇一項來認證。用於指定和初始化認證基於層級的認證的登入爲：

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=authentication_level
```

和

```
http://server_name.domain_name:port/amserver/UI/
```

```
Login?realm=realm_name&authlevel=authentication_level
```

如果沒有配置 `realm` 參數，將從指定於登入 URL 自身中的伺服器主機和網域決定使用者所屬的範圍。

認證基於層級的認證重新導向 URL

於認證基於層級的認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於認證層級的認證重新導向 URL

成功的基於認證層級的認證重新導向 URL 是以此優先順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `goto` 登入 URL 參數設定的 URL。
3. 對使用者設定檔 (`amUser.xml`) 的 `iplanet-am-user-success-url` 屬性，於 `clientType` 自訂檔案中設定一個 URL。

4. 使用者角色項目之 iplanet-am-auth-login-success-url 屬性的 clientType 自訂檔案中設定的 URL。
5. 使用者範圍項目之 iplanet-am-auth-login-success-url 屬性的 clientType 自訂檔案中設定的 URL。
6. 於 iplanet-am-auth-login-success-url 屬性的 clientType 自訂檔案中設定的 URL，做爲全域預設值。
7. 於使用者設定檔 (amUser.xml) 中的 iplanet-am-user-success-url 屬性中設定一個 URL。
8. 使用者角色項目之 iplanet-am-auth-login-success-url 屬性中設定的 URL。
9. 設定於使用者範圍項目之 iplanet-am-auth-login-success-url 屬性中的 URL。
10. iplanet-am-auth-login-success-url 屬性中設定的 URL，作爲全域預設值。

失敗的基於認證層級的認證重新導向 URL

失敗的基於認證層級的認證重新導向 URL 是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. gotoOnFail 登入 URL 參數設定的 URL。
3. 對使用者項目 (amUser.xml) 的 iplanet-am-user-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
4. 使用者角色項目的 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL。
5. 對使用者範圍項目的 iplanet-am-auth-login-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
6. 於 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL，做爲全域預設值。
7. 於使用者項目 (amUser.xml) 中設定 iplanet-am-user-failure-url 屬性的 URL。
8. 針對使用者角色項目之 iplanet-am-auth-login-failure-url 屬性設定的 URL。
9. 設定使用者範圍項目之 iplanet-am-auth-login-failure-url 屬性的 URL。
10. 針對 iplanet-am-auth-login-failure-url 屬性設定的 URL，作爲全域預設值。

基於模組的認證

使用者可以使用以下語法存取特定認證模組：

http://*hostname:port/deploy_URI*/UI/Login?module=

module_name

存取認證模組之前，必須先修改 [核心認證] 服務屬性 [範圍認證模組] ，使之包括此認證模組名稱。如果該屬性中未包括此認證模組名稱，使用者嘗試認證時，系統將顯示 [認證模組遭拒] 頁面。

此認證方法可讓使用者指定他們要認證的模組。指定的模組必須註冊至使用者存取的範圍或子範圍。此將配置於範圍核心認證服務的範圍認證模組屬性。在接收此項基於模組的認證請求時，認證服務會驗證模組如說明一樣正確配置，如果未定義模組，使用者會被拒絕存取。

基於模組的認證登入 URL

透過定義模組參數，可以在使用者介面登入中指定基於模組的認證。用於指定和初始化基於模組的認證的登入 URL 爲：

```
http://server_name.domain_name:port/amserver/UI/Login?module=authentication_module_name
```

```
http://server_name.domain_name:port/amserver/UI/
```

```
Login?org=org_name&module=authentication_module_name
```

如果沒有配置的 `org` 參數，將從指定於登入 URL 自身中的伺服器主機和網域決定使用者所屬的範圍。

基於模組的認證重新導向 URL

於模組型認證成功或失敗後，Access Manager 會尋找重新導向使用者的位置之相關資訊。以下爲應用程式尋找此資訊的優先順序。

成功的基於模組的認證重新導向 URL

成功的基於模組的認證，其重新導向 URL 是以此優先順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. `goto` 登入 URL 參數設定的 URL。
3. 使用者設定檔 (`amUser.xml`) 的 `iplanet-am-user-success-url` 屬性之 `clientType` 自訂檔案中設定的 URL。
4. 使用者角色項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
5. 使用者範圍項目之 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL。
6. 於 `iplanet-am-auth-login-success-url` 屬性的 `clientType` 自訂檔案中設定的 URL，做爲全域預設值。
7. 於使用者設定檔 (`amUser.xml`) 中的 `iplanet-am-user-success-url` 屬性中設定一個 URL。

8. 使用者角色項目之 iplanet-am-auth-login-success-url 屬性中設定的 URL。
9. 設定於使用者範圍項目之 iplanet-am-auth-login-success-url 屬性中的 URL。
10. iplanet-am-auth-login-success-url 屬性中設定的 URL，作爲全域預設值。

失敗的基於模組的認證重新導向 URL

失敗的基於模組的認證，其重新導向是以此順序檢查下列位置決定的：

1. 認證模組設定的 URL。
2. gotoOnFail 登入 URL 參數設定的 URL。
3. 對使用者項目 (amUser.xml) 的 iplanet-am-user-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
4. 對使用者角色項目的 iplanet-am-auth-login-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
5. 對使用者範圍項目的 iplanet-am-auth-login-failure-url 屬性，於 clientType 自訂檔案中設定一個 URL。
6. 於 iplanet-am-auth-login-failure-url 屬性之 clientType 自訂檔案中設定的 URL，做爲全域預設值。
7. 針對使用者角色項目之 iplanet-am-auth-login-failure-url 屬性設定的 URL。
8. 設定使用者範圍項目之 iplanet-am-auth-login-failure-url 屬性的 URL。
9. 針對 iplanet-am-auth-login-failure-url 屬性設定的 URL，作爲全域預設值。

使用者介面登入 URL

輸入登入 URL 到網路瀏覽器的位置列可存取認證服務使用者介面。此 URL 爲：

http://*AccessManager-root*/.*domain_name*:*port* /*service_deploy_uri* /UI/Login

---

備註 – 於安裝期間，將 *service_deploy_uri* 配置爲 amserver。本文件中將使用此預設的服務部署 URI。

使用者介面登入 URL 亦可與登入 URL 參數隨附一起，以定義指定的認證方法或成功/失敗的認證重新導向 URL。

登入 URL 參數

URL 參數是附加到 URL 尾端的名稱/值對。參數以問號開頭 (?)，形式爲 name=value。一些參數可以合併到一個登入中，例如：

```
http://server_name.domain_name:port/amserver/UI/

Login?module=LDAP&locale=ja&goto=http://www.sun.com
```

如果有一個或多個參數，會以 & 符號做爲分隔符號。不過組合必須遵守下列指導方針：

- 每個參數在一個 URL 中只能出現一次。例如：`module=LDAP&module=NT` 是不可以計算的。
- `org` 參數與 `domain` 參數兩者皆可決定登入範圍。在這種情形下，兩個參數中只應在登入 URL 中使用一個。如果兩者都使用了而且未指定優先順序，只有其中一個會生效。
- 參數 `user`、`role`、`service`、`module` 及 `authlevel` 用於定義認證模組 (根據其各自的準則)。因此，只應於登入 URL 中使用其中之一。如果使用了一個以上而且未指定優先順序，只有其中一個會生效。

下節描述參數在附加到使用者介面登入 URL，以及鍵入網路瀏覽器的位置列時，可達到的多種認證功能。

備註 – 若要簡化在範圍內發佈的認證 URL 和參數，管理員可配置一個具備單一 URL 的 HTML 網頁，其中包含所有已配置的認證方法的更爲複雜的登入 URL。

---

goto 參數

`goto=`*successful_authentication_URL* 參數會覆寫認證配置服務之 [登入成功 URL] 中定義的值。當達到成功認證時，它會連結到指定的 URL。使用者登出時，也可以使用 `goto=logout_URL` 參數連結至指定的 URL。例如，成功的認證 URL：

```
http://server_name.domain_name:port/amserver/

UI/Login?goto=http://www.sun.com/homepage.html
```

範例的 `goto` 登出 URL：

```
http://server_name.domain_name:port/amserver/

UI/Logout?goto=http://www.sun.com/logout.html.
```

備註 – Access Manager 尋找成功認證重新導向 URL 時有一項優先順序。因爲這些重新導向 URL 及其順序是以認證方法爲基礎，此順序 (及相關資訊) 於「認證類型」一節中有詳細說明。

---

gotoOnFail 參數

gotoOnFail=failed_authentication_URL 參數會覆寫認證配置服務之 [登入失敗 URL] 中定義的值。如果使用者認證失敗，它將會連結到指定的 URL。範例的 gotoOnFail URL 爲：http:// *server_name.domain_name*:*port* /amserver/UI/Login? gotoOnFail=http://www.sun.com/auth_fail.html。

備註 – Access Manager 使用優先順序尋找失敗的認證重新導向 URL。因爲這些重新導向 URL 及其順序是以認證方法爲基礎，此順序 (及相關資訊) 於「認證類型」一節中有詳細說明。

---

realm 參數

org=*realmName* 參數允許使用者認證成爲指定範圍中的使用者。

備註 – 當使用者嘗試以 realm 參數認證時，若其不是指定範圍的成員，就會收到錯誤訊息。如果以下全部皆爲 TRUE 時，可以於 Directory Server 中動態建立使用者設定檔：

- 核心認證服務中的使用者設定檔屬性必須設定爲**動態**或**隨使用者別名動態變化**。
- 使用者必須成功認證爲需要的模組。
- Directory Server 中還沒有使用者的設定檔。

因爲這項參數，將顯示正確的登入頁 (根據範圍及其系統語言設定)。若未設定此參數，預設值爲頂層範圍。例如：org URL 可以是：

```
http://server_name.domain_name:port/amserver/UI/Login?realm=sun
```

---

org 參數

org=*orgName* 參數允許使用者認證成爲指定組織中的使用者。

備註 – 當使用者嘗試以 org 參數認證時，若其不是指定組織的成員，就會收到錯誤訊息。如果以下全部皆爲 TRUE 時，可以於 Directory Server 中動態建立使用者設定檔：

- 核心認證服務中的使用者設定檔屬性必須設定爲**動態**或**隨使用者別名動態變化**。
- 使用者必須成功認證爲需要的模組。
- Directory Server 中還沒有使用者的設定檔。

因爲這項參數，將顯示正確的登入頁根據其組織與系統語言設定。如果未設定此參數，預設值爲頂層組織。例如：org URL 可以是：

```
http://server_name.domain_name:port/amserver/UI/Login?org=sun
```

---

user 參數

user=*userName* 參數基於使用者設定檔之 [使用者認證配置] 屬性中配置的模組進行強制認證。例如，可將一個使用者設定檔配置爲使用憑證模組進行認證，而將另一個使用者設定檔配置爲使用 LDAP 模組進行認證。新增此參數會將使用者傳送到其配置的認證程序，而非爲其組織配置的方法。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?user=jsmith
```

role 參數

role=roleName 參數會將使用者傳送至指定角色配置的認證程序。當使用者嘗試以參數認證時，若不是指定角色的成員，則會收到錯誤訊息。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?role=manager.
```

locale 參數

Access Manager 具有爲認證程序及主控台本身顯示本土化的畫面 (譯爲非英語的語言) 的功能。locale=*localeName* 允許指定的語言環境優先於任何其他定義的語言環境。以下列位置、指定順序搜尋配置後，登入語言環境會由用戶端顯示：

1. 登入 URL 中的語言環境參數值

   locale=*localeName* 參數的值優先於所有其他定義的語言環境。
2. 使用者設定檔中定義的語言環境

   如果沒有 URL 參數，會根據在使用者設定檔的 [使用者喜好的語言] 屬性中設定的值顯示語言環境。
3. 在標頭中定義的語言環境

   語言環境由網路瀏覽器所定義。
4. [核心認證服務] 中定義的語言環境

   這是在 [核心認證] 模組中 [預設認證語言環境] 屬性的值。
5. 在 [平台服務] 中定義的語言環境

   這是在 [平台] 服務中 [平台語言環境] 屬性的值。

作業系統語言環境

由此等級順序導出的語言環境儲存於使用者的階段作業記號中，且 Access Manager 僅用它來載入本地化的認證模組。成功認證後，會使用於使用者設定檔之使用者喜好的語言屬性中定義的語言環境。如果都沒有設定，將繼續保持認證所使用的語言環境。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?locale=ja.
```

備註 – 如何本地化畫面文字和錯誤訊息的資訊可於 Access Manager 中找到。

module 參數

`module=`*moduleName* 參數允許經由指定的認證模組進行認證。可指定任何模組，即使必須先於範圍之下註冊模組，此範圍爲使用者所屬且選取爲核心認證模組中該範圍認證的其中一個。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?module=Unix.
```

備註 – 在參數中使用認證模組名稱時要區分大小寫。

service 參數

`service=`*serviceName* 參數允許經由服務已配置的認證方案來認證使用者。可配置不同的認證方案給使用 [認證配置] 服務的不同服務。例如，當範圍員工目錄應用程式可能僅需要 LDAP 認證模組的同時，一個線上薪資應用程式可能需要使用更安全憑證認證模組來進行認證。認證方案可以被配置、命名給這些服務的每一項。例如：

`http://`*server_name.domain_name*`:port/amserver/UI/Login?service=sv1.`

備註 – 認證配置服務用於定義方案給以服務爲基礎的認證。

arg 參數

`arg=`*newsession* 參數用於結束使用者的目前階段作業，並開始新的階段作業。認證服務會銷毀使用者現有的階段作業記號，並接受一個請求執行新的登入。此選項通常用於 [匿名認證] 模組中。使用者先以匿名階段作業認證，然後點一下註冊或登入連結。例如：

`http://`*server_name.domain_name*`:port/amserver/UI/Login?arg=newsession`。

authlevel 參數

`authlevel=`*value* 參數會指示認證服務呼叫認證層級等於或大於指定認證層級值的模組。每個認證模組都使用固定的整數認證層級定義。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=1.
```

備註 – 認證層級是於每個模組的特定設定檔中設定。。

domain 參數

此參數可讓使用者登入由指定的網域所標識的範圍。指定的網域必須符合定義於範圍設定檔之網域名稱屬性中的值。例如：

`http://`*server_name.domain_name*`:port/amserver/UI/Login?domain=sun.com`。

備註 – 當使用者嘗試以 `org` 參數認證時，若其不是指定網域/範圍的成員，就會收到錯誤訊息。如果以下各點全部皆爲 TRUE 時，可以於 Directory Server 中動態建立使用者設定檔：

- 核心認證服務中的使用者屬性必須設定爲**動態**或**隨使用者別名動態變化**。
- 使用者必須成功認證爲需要的模組。
- Directory Server 中還沒有使用者的設定檔。

iPSPCookie 參數

`iPSPCookie=yes` 參數允許使用者以永久性 Cookie 登入。永久性 Cookie 在瀏覽器視窗關閉後仍然繼續存在。要使用此參數，使用者登入的範圍必須在其核心認證模組中啓用永久性 Cookie。一旦使用者認證及瀏覽器關閉，使用者可以新的階段作業登入，並將導向至控制台而不需重新認證。在核心服務中指定的永久性 Cookie 最大時間屬性消逝前，該功能都有效。例如：

`http://`*server_name.domain_name*`:port/amserver/UI/Login?org=example&iPSPCookie=yes`

IDTokenN 參數

此參數可讓使用者藉由 URL 或 HTML 形式傳送認證憑證。利用 `IDTokenN=` *value* 參數，使用者毋須存取認證服務使用者介面便可被認證。此程序稱爲零頁登入。零頁登入只適用於使用單一登入頁的認證模組。`IDToken0`、`IDToken1`、`...`、`IDTokenN` 值對映至認證模組登入頁面上的欄位。例如，LDAP 認證模組可能將 `IDToken1` 用於 `userID` 資訊、將 `IDToken2` 用於密碼資訊。在這種情形下，LDAP 模組 IDTokenN URL 將是：

`http://`*server_name.domain_name*`:port/amserver/UI/`

`Login?module=LDAP&IDToken1=userID&IDToken2=password`

(如果 LDAP 是預設認證模組，可以忽略`module=LDAP`。)

就匿名認證而言，登入 URL 參數會是：

`http://`*server_name.domain_name:port*`/amserver/UI/Login?module=Anonymous&IDToken1=anonymousUserID`。

備註 – 名稱爲 `Login.Token0`、 `Login.Token1`、 ...、 `Login.TokenN` (來自上一個版本) 的記號仍受支援，但將於未來版本中停用。建議您使用新的 `IDTokenN` 參數。

帳號鎖定

認證服務提供一項功能，於其中使用者將在 *n* 次失敗後被鎖定，無法認證。這項功能預設爲關閉，但可以使用 Access Manager 主控台啓用。

備註 – 只有拋出有效密碼異常的模組可以充分利用帳號鎖定功能。

核心認證服務包含啓用和自訂此功能的屬性，包括但不限於：

- 會啓用帳號鎖定的登入失敗鎖定模式。
- 登入失敗鎖定計數 定義使用者被鎖定前可嘗試認證的次數。此計數只對每個使用者有效；相同的使用者在賦予計數時必需失效，而後該使用者會被鎖定。
- 登入失敗鎖定間隔定義使用者被鎖定前，必須完成的登入失敗鎖定計數值之時間數 (以分鐘計)。
- 傳送鎖定通知的電子郵件位址指定使用者鎖定通知將被傳送的電子郵件位址。
- **N** 次失敗後警告使用者指定對使用者顯示警告訊息前，可發生的認證失敗次數。這可讓管理員設定在使用者被警告即將被鎖定後，額外的登入嘗試次數。
- 登入失敗鎖定持續時間定義鎖定使用者後，再次嘗試認證前必須等待的時間 (以分鐘爲單位)。
- 鎖定屬性名稱定義使用者設定檔中要設定爲對實際鎖定**無效**的 LDAP 屬性。
- 鎖定屬性值定義鎖定屬性名稱中指定的 LDAP 屬性將設定爲：**非作用中**或**作用中**。

電子郵件通知將被傳送到與任何帳號鎖定有關的管理員。帳號鎖定活動也會被記錄。

備註 – 當於 Microsoft® Windows 2000 作業系統上使用此功能，如需特殊指示時，請參閱「附錄 A，AMConfig.properties 檔案」中的「簡易郵件傳輸協定 (SMTP)」。

Access Manager 支援兩種帳號鎖定類型：實體鎖定與記憶體鎖定，定義於下列章節中。

實體鎖定

這是 Access Manager 的預設鎖定行爲。藉由變更使用者設定檔中的 LDAP 屬性爲非作用中，啓動鎖定。**鎖定屬性名稱**屬性定義用於鎖定作用的 LDAP 屬性。

備註 – 以別名爲名稱的使用者是藉由配置 LDAP 設定檔中使用者別名清單屬性 (amUser.xml **中的** iplanet-am-user-alias-list) ，以對映至現有 LDAP 使用者設定檔的使用者。藉由新增 iplanet-am-user-alias-list 至 核心認證服務之 [別名搜尋屬性名稱] 欄位，可驗證以別名爲名稱的使用者。也就是說，如果一個別名使用者被鎖定，被別名化的使用者其實際設定檔將被鎖定。這只適用於使用 LDAP 和 Membership 之外的認證模組的實體鎖定。

記憶體鎖定

將**登入失敗鎖定持續時間**屬性的值變更爲大於零，可啓用記憶體鎖定。啓用後，使用者帳號會被鎖定在記憶體中一段指定的時間 (以分鐘計)。經過該段時間後，將解除鎖定帳號。以下是使用記憶體鎖定功能時，一些特殊的考量：

- 若重新啓動了 Access Manager，所有鎖定於記憶體中的帳號都會被解除。
- 若使用者的帳號被鎖定在記憶體中，而管理員將帳號鎖定機制變更爲實際鎖定 (以將鎖定持續時間設回零的方式進行)，則使用者帳號將在記憶體中被解除鎖定，鎖定計數也會重設。
- 記憶體鎖定後，當使用 LDAP 與成員身份之外的認證模組時，若使用者嘗試以正確的密碼登入，則將傳回使用者於此範圍中並無設定檔訊息。錯誤，會傳回，而不是傳回使用者非作用中。錯誤。

備註 – 如果在使用者設定檔中設定了 Failure URL 屬性，則鎖定警告訊息和指出使用者帳號已遭鎖定的訊息都不會顯示，系統會將使用者重新導向至定義的 URL。

認證服務容錯移轉

若主伺服器因爲硬體或軟體問題或伺服器暫時關機而失敗，則認證服務容錯移轉會自動將認證請求重新導向至次伺服器中。

認證內容必須先在可使用認證服務的實例上建立。如果此實例無法使用，則可透過認證錯誤修復機制在上建立認證內容。認證內容會依下列順序檢查伺服器可用性：

1. 認證服務 URL 會傳到 AuthContext API。例如：

   ```
   AuthContext(orgName, url)
   ```

   如果使用 API，僅使用 URL 參照的伺服器。即使伺服器上可以使用該認證服務，也不會發生錯誤修復。
2. 認證內容將檢查定義於 AMConfig.properties 檔案的 com.iplanet.am.server* 屬性中的伺服器。

3. 如果步驟 2 失敗，則認證內容會從可取得命名服務的伺服器查詢平台清單。在共用一個實例安裝通常是爲了錯誤修復的多重實例時，會自動建立此平台。

   例如，如果平台清單包含 Server1、Server2 及 Server3 的 URL，則認證內容會在 Server1 、Server2 及 Server3 間循環，直到成功認證其中一個爲止。

   平台清單有時不是從同一個伺服器取得，而是視「命名」服務可用性而異。另外，「命名」服務的錯誤修復可能先發生。將多重命名服務 URL 指定於 com.iplanet.am.naming.url **特性中** (在 AMConfing.properties 之中)。第一個可用的「命名」服務 URL 會用來辨識伺服器，包含將發生錯誤修復的伺服器清單 (位於其平台伺服器清單中)。

完全合格的網域名稱對映

完全合格的網域名稱 對映會啓用認證服務以便在使用者輸入錯誤的時採取修正行動 例如指定部分的主機名稱或位址存取受保護的資源。FQDN 對映是藉由修改 AMConfig.properties 檔案中的 com.sun.identity.server.fqdnMap 屬性來啓用。指定此屬性的格式爲：

com.sun.identity.server.fqdnMap[*invalid-name*]=*valid-name*

值 *invalid-name* 可以是使用者輸入的無效 FQDN 主機名稱，*valid-name* 則爲篩選器將重新導向使用者的目標實際主機名稱。可以指定的對映數不限 (如程式碼範例 1-1 所說明的)，只要它們符合明確指出的要求即可。若未設定此特性，使用者將被傳送到在 com.iplanet.am.server.host= *server_name* 特性中配置的預設伺服器名稱 (也可在 AMConfig.properties 檔案中找到)。

範例 7–1 AMConfig.properties 中的 FQDN 對映屬性

```
com.sun.identity.server.fqdnMap[isserver]=isserver.mydomain.com

com.sun.identity.server.fqdnMap[isserver.mydomain]=isserver.mydomain.com

com.sun.identity.server.fqdnMap[

        IP address]=isserver.mydomain.com
```

可能用於 FQDN 對映

此屬性可以用於建立對一個以上主機名稱的對映，在常駐於伺服器上的應用程式可被一個以上的主機名稱存取時。此特性亦可用於配置 Access Manager，不對某些 URL 採取修正動作。例如，如果使用位址存取應用程式的使用者不需要重新導向時，可藉由指定對映項目執行此功能，例如：

`com.sun.identity.server.fqdnMap[`*IP address* `]=`*IP address*。

備註 – 如果定義了一個以上的對映，請確定在無效的名稱中沒有重疊值。如果沒有這麼做，可能會導致應用程式無法存取。

永久性 Cookie

永久性 cookie 將於 Web 瀏覽器關閉後仍持續存在，可讓使用者以新的瀏覽器階段作業登入而不必重新認證。Cookie 的名稱是依據 `AMConfig.properties` 中的 `com.iplanet.am.pcookie.name` 特性定義；預設值爲 `DProPCookie`。cookie 值是一個 3DES 加密的字串，包含 userDN、範圍名稱、認證模組名稱、最長階段作業時間、閒置時間和快取時間。

▼ 若要啓用永久性 Cookie

1. **開啓核心認證模組中的永久性 `Cookie` 模式**。
2. **配置核心認證模組中永久性 `Cookie` 最長時間屬性之時間值**。
3. **將 iPSPCookie 參數 (值為 `yes`) 附加到使用者介面登入 URL**。

   一旦使用者使用此 URL 進行認證，若瀏覽器關閉，其可開啓一個新的瀏覽器視窗並將重新導向至主控台而不需重新認證。這項作業的運作時間爲直到步驟 2 中定義的時間結束爲止。

   可以使用認證方法開啓永久性模式：

   `AMLoginModule.setPersistentCookieOn()`。

「舊有」模式的多重 LDAP 認證模組配置

做爲一種容錯移轉，或當 Access Manager 主控台僅提供一個值欄位時要配置屬性的多個值，管理員可於一個範圍之下定義多重 LDAP 認證模組配置。儘管這些附加配置不會顯示在主控台中，但它們仍可在找不到用於請求使用者認證的初始搜尋時與主配置配合使用。例如，一個範圍可於兩種不同網域中透過 LDAP 伺服器爲認證定義搜尋，或於一個網域中配置多重使用者命名屬性。就後者而言，在主控台中只有一個文字欄位，如果使用主要搜尋準則找不到使用者，模組將會使用次要範圍搜尋。依照下列步驟配置其他的配置。

▼ 若要新增其他的配置

1 **撰寫一個 XML 檔案，其中包含完整屬性集和次要 (或第三) LDAP 認證配置需要的新值。**

檢視 amAuthLDAP.xml (位於 etc/opt/SUNWam/config/xml) 就可以參照可用的屬性。此 XML 檔案於此步驟中建立，然而，不像 amAuthLDAP.xml，它是以 amadmin.dtd 的結構爲基礎。任何或是全部屬性都能定義給這個檔案。程式碼範例 1-2 爲子配置檔案的範例，其包括 LDAP 認證配置可用的所有屬性值。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!--

  Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

  Use is subject to license terms.

-->

<!DOCTYPE Requests

    PUBLIC "-//iPlanet//Sun ONE Access Manager 6.0 Admin CLI DTD//EN"

    "jar://com/iplanet/am/admin/cli/amAdmin.dtd"

>

<!--

  Before adding subConfiguration load the schema with

GlobalConfiguration defined and replace corresponding

 serviceName and subConfigID in this sample file OR load

 serviceConfigurationRequests.xml before loading this sample
```

```
-->
<Requests>
<realmRequests DN="dc=iplanet,dc=com">
    <AddSubConfiguration subConfigName = "ssc"
        subConfigId = "serverconfig"
        priority = "0" serviceName="iPlanetAMAuthLDAPService">


              <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-server"/>
            <Value>vbrao.red.iplanet.com:389</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-base-dn"/>
            <Value>dc=iplanet,dc=com</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="planet-am-auth-ldap-bind-dn"/>
            <Value>cn=amldapuser,ou=DSAME Users,dc=iplanet,dc=com</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-bind-passwd"/>
            <Value>
                    plain text password</Value>
        </AttributeValuePair>
```

```
<AttributeValuePair>
    <Attribute name="iplanet-am-auth-ldap-user-naming-attribute"/>
    <Value>uid</Value>
</AttributeValuePair>
<AttributeValuePair>
    <Attribute name="iplanet-am-auth-ldap-user-search-attributes"/>
    <Value>uid</Value>
</AttributeValuePair>
<AttributeValuePair>
    <Attribute name="iplanet-am-auth-ldap-search-scope"/>
    <Value>SUBTREE</Value>
</AttributeValuePair>
<AttributeValuePair>
    <Attribute name="iplanet-am-auth-ldap-ssl-enabled"/>
    <Value>false</Value>
</AttributeValuePair>
<AttributeValuePair>
    <Attribute name="iplanet-am-auth-ldap-return-user-dn"/>
    <Value>true</Value>
</AttributeValuePair>
<AttributeValuePair>
    <Attribute name="iplanet-am-auth-ldap-auth-level"/>
    <Value>0</Value>
```

```
        </AttributeValuePair>

        <AttributeValuePair>

            <Attribute name="iplanet-am-auth-ldap-server-check"/>

            <Value>15</Value>

        </AttributeValuePair>


    </AddSubConfiguration>


</realmRequests>

</Requests>
```

2 **複製純文字密碼做為建立於步驟 1 之 XML 檔案中 iplanet-am-auth-ldap-bind-passwd 的值。**
此屬性的值於程式碼範例中以粗體顯示。

3 **使用 `amadmin` 指令行工具載入 XML 檔案。**

```
./amadmin -u amadmin -w administrator_password -v -t name_of_XML_file.
```

請注意此次要 LDAP 配置無法使用主控台顯示或修改。

提示 – 這是多重 LDAP 配置可用的範例。請參閱 `/AccessManager-base /SUNWam/samples/admin/cli/bulk-ops/` 中的 `serviceAddMultipleLDAPConfigurationRequests.xml` 指令行範本。可於 `/AccesManager-base /SUNWam/samples/admin/cli/` **的** Readme.html **取得指示。**

階段作業升級

認證服務可讓您根據相同使用者對單一範圍第二次執行的成功認證啓用有效的階段作業記號升級。若具有有效階段作業的使用者試圖認證到由目前範圍保護的資源，且第二次認證請求成功，階段作業會根據新認證使用新特性更新。如果認證失敗，使用者目前的階段作業會被退回，不會升級。若具有有效階段作業的使用者試圖認證到由不同範圍保護的資源，使用者將收到詢問其是否要認證到新組織的訊息。使用者在此時可以維持目前的階段作業，或嘗試對新範圍進行認證。成功的認證將導致舊階段作業被銷毀，並建立新的階段作業。

在階段作業升級期間，如果登入頁逾時，將會重新導向到原始的成功。逾時值的決定是基於：

- 爲每個模組設定的頁面逾時值 (預設爲 1 分鐘)
- `AMConfig.properties` 中的 `com.iplanet.am.invalidMaxSessionTime` 特性 (預設值爲 10 分鐘)
- `iplanet-am-max-session-time` (預設值爲 120 分鐘)

`com.iplanet.am.invalidMaxSessionTimeout` 和 `iplanet-am-max-session-time` 的值應大於頁逾時值，否則階段作業升級期間的有效階段作業資訊將會遺失，而且到前一個成功 URL 的 URL 重新導向將會失敗。

驗證外掛程式介面

管理員可以撰寫適合其範圍的使用者名稱或是密碼驗證邏輯，並外掛至認證服務中。這項功能只有和認證模組支援。認證使用者或變更密碼之前，Access Manager 將呼叫此外掛程式。如果驗證成功，認證將繼續；如果失敗，將拋出認證失敗頁。外掛程式會延伸 `com.iplanet.am.sdk.AMUserPasswordValidation` 類別，其爲「服務管理 SDK」的一部分。關於此 SDK 的資訊，可以參考 Access Manager Javadocs 中的 `com.iplanet.am.sdk` 套裝軟體。

▼ 若要撰寫與配置驗證外掛程式

1. **新的外掛程式類別將延伸 `com.iplanet.am.sdk.AMUserPasswordValidation` 類別，並實作 `validateUserID()` 與 `validatePassword()` 方法。如果驗證失敗，應該會拋出 `AMException`。**
2. **編譯外掛程式並將 `.class` 檔案置於想要的位置中。更新類別路徑，以便在執行階段期間可由 Access Manager 存取。**
3. **以頂層管理員的身份登入 Access Manager 主控台。按一下 [服務管理] 標籤，然後到管理服務的屬性。於 `UserID` 與密碼驗證外掛程式類別欄位中鍵入外掛程式類別的名稱 (包括套裝軟體名稱)。**

4 登出並登入。

JAAS 共用狀態

共用狀態提供認證模組間使用者和密碼的共用。爲每個認證模組定義的選項用於：

- 範圍 (或組織)
- 使用者
- 服務
- 角色

在失敗時，模組會提示需要的憑證。在認證失敗後，模組停止執行，或是登出共用狀態清除。

啓用 JAAS 共用狀態

若要配置 JAAS 共用狀態：

- 使用 `iplanet-am-auth-shared-state-enabled` 選項。
- 共用狀態選項的用法爲：`iplanet-am-auth-shared-state-enabled=true`
- 此選項預設爲 true。
- 將此變數指定於認證鏈接配置的 [選項] 欄位中。

失敗時，認證模組會提示需要的憑證，如同 JASS 規格中建議的 `tryFirstPass` 選項運作方式。

JAAS 共用狀態儲存選項

若要配置 JAAS 共用狀態儲存選項：

- 使用 `iplanet-amauth-store-shared-state-enabled` 選項。
- 儲存共用狀態選項的用法爲：`iplanet-am-auth-store-shared-state-enabled=true`
- 此選項預設爲 false。
- 將此變數指定於認證鏈接配置的 [選項] 欄位中。

在確認、中斷或登出後，將清除共用狀態。

◆ ◆ ◆ 第 8 章

管理策略

本章描述 Sun Java™ System Access Manager 的策略管理功能。Access Manager 的「策略管理」功能使頂層管理員或頂層策略管理員可檢視、建立、刪除和修改用於所有範圍的特定服務的策略。它也爲範圍或子範圍管理員或策略管理員提供一種方式，以檢視、刪除和修改範圍層級的策略。

本章包含下列小節：

簡介

策略定義指定擁有組織受保護資源存取權限的規則。公司擁有需要保護、管理和監視的資源、應用程式和服務。策略透過定義使用者對特定資源行動的時機和方法，控制存取權限以及這些資源的用途。策略定義特定主體的資源。

備註 – 主體可以是個人、企業、角色或群組；或是任何可以具有識別的個體。如需更多資訊，請參閱 Java™ 2 Platform Standard Edition Javadoc (`http://java.sun.com/j2se/1.4.2/docs/api/java/security/Principal.html`)。

單一策略可以定義二進位或非二進位決策。二進位決策爲 *yes*/*no*、*true*/*false* 或 *allow*/*deny*。非二進位決策代表屬性值。例如，郵件服務可能包含一個 `mailboxQuota` 屬性，每位使用者擁有最大儲存值集。一般來說，策略是配置爲定義主體可以在什麼情況下對哪一個資源進行什麼動作。

策略管理功能

策略管理功能提供建立及管理策略的策略服務。策略服務允許管理員定義、修改、取得、取消及刪除權限，以保護 Access Manager 部署內的資源。通常，策略服務包括資料庫、允許建立、管理及評估策略的介面之程式庫、及策略執行程式或策略代理程式。依預設，Access Manager 將 Sun Java Enterprise System Directory Server 用於資料存放區，爲策略評估和策略服務自訂提供 Java 和 C API (如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Developer's Guide」)。它也讓管理員可使用 Access Manager 主控台來管理策略。Access Manager 提供一個啓用策略的服務，即「URL 策略代理程式」服務，它使用可下載的策略代理程式來強制執行策略。

URL 策略代理程式服務

在安裝時，Access Manager 提供的「URL 策略代理程式」服務可定義策略來保護 HTTP URL。此服務可讓管理員透過策略執行程式或策略代理程式建立與管理策略。

策略代理程式

策略代理程式是儲存企業資源的伺服器之策略執行點 (PEP)。策略代理程式與安裝在不同的 Web 伺服器上，且於使用者發出對受保護的 Web 伺服器上的網路資源的請求時，做爲一個額外的認證步驟。此認證在執行資源的任何使用者認證請求之外。此代理程式保護 Web 伺服器，並且資源也會受到認證外掛程式的保護。

例如，受遠端安裝的 Access Manager 保護之人力資源 Web 伺服器可能已安裝一個代理程式。此代理程式可以防止沒有適當策略的人員檢視機密薪資資訊或其他敏感資料。策略是由 Access Manager 管理員所定義、儲存在 Access Manager 部署中，且由策略代理程式用於允許或拒絕使用者存取遠端 Web 伺服器的內容。

最新的 Access Manager 策略代理程式可以從 Sun Microsystems 下載中心下載。

有關安裝與管理策略代理程式的詳細資訊，請參閱「Sun Java System Access Manager Policy Agent 2.2 User's Guide」。

備註 – 策略是以一般順序進行評估，但在評估時，如果一個動作值評估爲 *deny*，就不會評估後續策略，除非策略配置服務中已啓用 [繼續評估拒絕決定] 屬性。

Access Manager 策略代理程式只會強制執行 Web URL (`http://...` 或 `https://...`) 的決策。然而，可使用 Java 和 C 策略評估 API 編寫代理程式，以在其他資源上強制執行策略。

此外，策略配置服務中的 [資源比較程式] 屬性可能也需要從預設配置變更爲：

```
serviceType=Name_of_LDAPService
|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*

|delimiter=,|caseSensitive=false
```

或者，也可以提供如 LDAPResourceName 等實作來實作 com.sun.identity.policy.interfaces.ResourceName，並正確配置 [資源比較程式]。

策略代理程式程序

當網路瀏覽器請求一個駐留在受策略代理程式保護的伺服器之 URL 時，保護網路資源的程序即開始。伺服器的已安裝策略代理程式會截取請求，並檢查現有的認證憑證 (階段作業記號)。

如果代理程式截獲請求並驗證現有階段作業記號，將遵循下列程序。

1. 如果階段作業記號爲有效，允許或拒絕使用者存取。如果記號爲無效，使用者僅限於認證服務，如下列步驟所述。

   假設代理程式截獲一個沒有現存階段作業記號的請求，代理程式將重新導向使用者到登入頁，不論該資源是否已經使用不同的認證方法保護。
2. 一旦正確的認證了使用者的憑證，代理程式會核發一個請求給命名服務，以將使用的 URL 定義爲連接至 Access Manager 的內部服務。
3. 若資源符合在代理程式配置的不予執行清單，則允許存取。
4. [命名服務] 會傳回策略服務、階段作業服務和記錄服務的定址器。
5. 代理程式會傳送請求給 [策略服務]，以取得適用於使用者的策略決策。
6. 基於存取資源的策略決策，決定使用者是否可以存取。如果策略決策建議不同的認證層級或認證機制，代理程式將重新導向請求到認證服務，直到驗證所有準則爲止。

策略類型

使用 Access Manager 配置的策略有兩種：

- 第 121 頁的 「一般策略」
- 第 125 頁的 「參照策略」

一般策略

在 Access Manager 中，定義存取權限的策略是指一般策略。一般策略由規則、主旨、條件與回應提供者組成。

規則

規則包含一個資源、一或多個動作及一個值。每個動作可以有一或數個值。

- 資源定義受保護的特定物件；例如，使用人力資源服務存取的 HTML 網頁或使用者之薪資資訊。
- 動作爲一項可於資源上執行的作業之名稱；Web 伺服器動作的範例有：POST 或 GET。例如，變更爲住家電話號碼爲人力資源服務可允許的一個動作。

- 值定義動作的權限，例如允許或拒絕。

備註 – 部份服務可接受只定義動作但沒有資源。

主旨

主旨定義策略影響的使用者或使用者集合 (例如：擁有特定角色的群組或人員)。指定主旨到策略。主旨的一般原則是，只有當使用者爲策略中至少一個主旨的成員時，策略才適用。預設主旨爲：

AM 識別主旨	您在 [範圍主旨] 標籤下建立和管理的識別可新增爲主旨的一個值。
Access Manager 角色	任何 LDAP 角色皆可新增爲此主旨的一個值。LDAP 角色是使用 Directory Server 角色功能定義的任何角色。這些角色具有 Directory Server 角色定義寄存的物件類別。可以在策略配置服務中修改 LDAP 角色搜尋篩選器，以縮小範圍和改善效能。
經認證的使用者	具備有效 SSOToken 的使用者都是此主旨的成員。所有認證的使用者將成爲此主旨的成員，即使這些使用者被認證到與定義策略之組織不同的組織。如果資源所有者想要將存取權限授與其他組織的使用者所管理的資源，這個功能很有用。
LDAP 群組	LDAP 群組的任何成員皆可新增爲此主旨的一個值。
LDAP 角色	任何 LDAP 角色皆可新增爲此主旨的一個值。LDAP 角色是使用 Directory Server 角色功能定義的任何角色。這些角色具有 Directory Server 角色定義寄存的物件類別。可以在策略配置服務中修改 LDAP 角色搜尋篩選器，以縮小範圍和改善效能。
LDAP 使用者	任何 LDAP 使用皆可新增爲此主旨的一個值。
組織	組織的任何成員都是此主旨的成員。
Web 服務用戶端	有效值爲本機 JKS 鍵值儲存區中可信任憑證的 DN (與可信任 WSC 的憑證相對應)。此主旨取決於 Liberty Web 服務架構，並且僅應該由 Liberty 服務提供者用來授權 WSC。如果包含在 SSOToken 中的任何主體之 DN 與此主旨的任意所選值相符，則由 SSOToken 識別的 Web 服務用戶端 (WSC) 爲此主旨的成員。 確定建立鍵值儲存區後再將此主旨加入策略。以下位置可以找到設定鍵值儲存區的資訊： *AccessManager-base* `/SUNWam/samples/saml/xmlsig/keytool.html`

Access Manager 角色與 LDAP 角色的比較

Access Manager 角色是使用 Access Manager 建立的，這些角色具有 Access Manager 指派的物件類別。LDAP 角色是使用 Directory Server 角色功能定義的任何角色。這些角色具有

Directory Server 角色定義寄存的物件類別。所有 Access Manager 角色皆可用來做爲 Directory Server 角色。不過，不是所有的 Directory Server 角色都一定會是 Access Manager 角色。藉由配置第 137 頁的「策略配置服務」，您可從現有目錄取用 LDAP 角色。Access Manager 角色僅可透過託管 Access Manager 策略服務存取。可以在策略配置服務中修改 LDAP 角色搜尋篩選器，以縮小範圍和改善效能。

巢式角色

在策略定義中，巢式角色可以正確評估爲 LDAP 角色。

條件

此條件允許您定義對策略的限制。例如，如果您在爲薪金應用程式定義策略，可以定義僅在特定幾小時限制此動作存取應用程式的條件。或者，如果請求來自給定 IP 位址集或企業內部網路，可能希望定義僅允許此動作存取的條件。

此條件可能還用於在同一網域的不同 URL 中配置不同的策略。例如，`http://org.example.com/hr/*jsp` 只可由 `org.example.net` 在 9 a.m. 至 5 p.m. 之間存取，而 `http://org.example.com/finance/*.jsp` 可由 `org.example2.net` 在 5 a.m. 至 11 p.m. 之間存取。這可藉由使用 [IP 條件] 和 [時間條件] 來達成。將規則資源指定爲 `http://org.example.com/hr/*.jsp`，此策略會套用於 `http://org.example.com/hr` 下的所有 JSP (包括子目錄中的 JSP)。

備註 – 參考、規則、資源、主旨、條件、動作及值分別對應於 `policy.dtd` 中之元素 *Referral*、*Rule*、*ResourceName*、*Subject*、*Condition*、*Attribute* 及 *Value*。

您可新增的預設條件有：

認證層級 — 若使用者的認證層級大於或等於條件中設定的認證層級，則會套用策略。

此屬性指示認證的可信度。

認證層級條件可用來指定該範圍的已註冊認證層級以外的層級。要將策略套用到其他範圍認證的使用者時，這會很有用。

對於「LE 認證」，若使用者的認證層級低於或等於條件中設定的認證層級，則會套用策略。認證層級條件可用來指定該範圍的已註冊認證層級以外的層級。要將策略套用到其他範圍認證的使用者時，這會很有用。

認證方案 — 從下拉式功能表中選擇條件的認證方案。這些認證方案是在範圍的核心認證服務中定義的認證模組。

IP 位址 — 根據 IP 位址的範圍設定條件。您可以定義的欄位爲：

- 起始/終止 IP 位址 — 指定 IP 位址的範圍。

- DNS 名稱 — 指定 DNS 名稱。此欄位可以爲完整的主機名稱或以下之一格式的字串：

  domainname

  **.domainname*

階段作業　根據使用者階段作業資料設定條件。您可以修改的欄位爲：

- 最長階段作業時間 — 指定自階段作業初始開始時可套用策略的最長持續時間。
- 終止階段作業 — 選取時，如果階段作業時間超過 [最長階段作業時間] 欄位中定義所允許的最長時間，使用者階段作業將被終止。

  您可使用此條件來保護機密資源，限制認證後能使用資源的時間。

階段作業特性　根據設定於使用者 Access Manager 階段作業中的特性值來決定策略是否適用於請求。於策略評估期間，僅當使用者階段作業具有條件中定義的特性值時，條件才傳回 true。對於條件中以多重值定義於的特性，需記號具有至少一個條件中爲特性列出的值。例如，您可使用此條件，根據外部儲存庫中的屬性套用策略。認證後外掛程式可根據外部屬性設定階段作業特性。

時間　根據時間限制設定條件。這些欄位包括：

- 起始/終止日期 — 指定日期的範圍。
- 時間 — 指定一天內的時間範圍。
- 日 — 指定天數範圍。
- 時區 — 指定時區 (標準或自訂)。自訂時區僅可爲 Java 識別的時區 ID (例如，PST)。如果未指定值，則預設值爲 Access Manager JVM 中設定的時區。

回應提供者

回應提供者爲提供策略型回應屬性的外掛程式。回應提供者屬性會和策略決策一起傳送給 PEP。Access Manager 包括一個實作，即 `IDResponseProvider`。此版本的 Access Manager 不支援自訂回應提供者。代理程式 PEP 通常會將這些回應以標頭的形式傳遞給應用程式。應用程式通常使用這些屬性將應用程式頁面個人化，例如入口網站頁面。

策略建議

如果無法根據條件的決定來套用策略，條件可能會產生建議訊息，指出無法將策略套用至請求的原因。這些建議訊息會在策略決策中傳播至 [策略執行點]。[策略執行點] 可以擷取此建議，並嘗試採取適當的行動，例如將使用者重新導向回認證機制，以便進行更高層級認證。採取建議的適當行動後，接著，使用者可能會收到更高層級認證的提示，只要能夠使用策略，使用者可能可以存取資源。

以下類別有更多資訊：

```
com.sun.identity.policy.ConditionDecision.getAdvices()
```

如果條件不符，只有 `AuthLevelCondiiton` 和 `AuthSchemeCondition` 會提供建議。

`AuthLevelCondition` 建議與以下鍵值相關聯：

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_LEVEL_CONDITION_ADVICE
```

`AuthSchemeCondition` 建議與以下鍵值相關聯：

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_SCHEME_CONDITION_ADVICE
```

自訂條件也會產生建議。但是，Access Manager 策略代理程式僅回應認證層級認證和認證方案建議。可以寫入自訂代理程式來瞭解及回應其他建議，而現有 Access Manager 代理程式可以延伸來瞭解及回應其他建議。如需更多資訊，請參閱「Sun Java System Access Manager Policy Agent 2.2 User's Guide」。

參照策略

管理員可能需要將一個範圍的策略定義委託給另一個範圍。(或者，可以將資源的策略決策委託給其他策略產品。)參照策略控制此策略委託，以建立與評估策略。它是由一或多項規則及一或多個參考所組成。

規則

規則定義其策略定義與評估正在被參照的資源。

參照

參照定義策略評估正在參照的組織。依預設，有兩種類型的參照：同級範圍與子範圍。其分別委派至相同層次上的範圍與子層次上的範圍。如需更多資訊，請參閱第 131 頁的「建立同級範圍與子範圍的策略」。

備註 – 被參照的範圍可以僅爲那些已參照了該範圍的資源 (或子資源) 定義或評估策略。然而，此限制不會套用至頂層範圍。

策略定義類型文件

建立與配置好策略之後，會將其以 XML 的形式儲存於 Directory Server。在 Directory Server 中，以 XML 編碼的資料會儲存在同一位置。雖然策略是使用 amAdmin.dtd (或主控台) 定義和配置，實際上是以根據 policy.dtd 以 XML 的形式儲存在 Directory Server。policy.dtd 包含從 amAdmin.dtd 中擷取的 policy 元素標籤 (不含策略建立標籤)。因此，當策略服務從 Directory Server 載入策略時，將根據 policy.dtd 剖析 XML。只有在使用指令行建立策略時，才會使用 amAdmin.dtd。本節將描述 policy.dtd 的結構。policy.dtd 位於下列位置：

```
AccessManager-base/SUNWam/dtd (Solairs)
AccessManager-base/identity/dtd (Linux)
```

備註 – 本章其他部分僅提供 Solaris 目錄資訊。請注意 Linux 的目錄結構不同。

Policy 元素

Policy 是根元素，其定義策略的權限或規則，及套用規則的對象或主旨。它也定義策略是否爲參考 (委託的) 策略，及該策略是否有任何限制 (或條件)。可能包含下列一或多個子元素：*Rule*、*Condition*、*Subject*、*Referral* 或 *response provider*。必要的 XML 屬性爲 name，其指定策略的名稱。referralPolicy 屬性辨識策略是否爲參照策略；若未定義，預設值爲一般策略。選用的 XML 屬性包括 *name* 與 *description*。

備註 – 將策略標示爲參照時， 策略評估期間將略過主旨與條件。相對的，將策略標示爲一般時，策略評估期間將略過所有參考。

Rule 元素

Rule 元素定義策略特性並可接受三個子元素：*ServiceName*、*ResourceName* 或 *AttributeValuePair*。可定義爲其建立策略服務類型或應用程式，以及於其中執行的資源和動作。規則可被定義爲不具任何動作；例如，參照策略規則不具任何動作。

備註 – 已定義策略不含已定義 *ResourceName* 元素是可接受的。

ServiceName 元素

ServiceName 元素定義套用策略的服務之名稱。此元素代表服務類型。不包含任何其他元素。此值與服務的 XML 檔案中定義之值完全相同 (以 sms.dtd 爲根據)。*ServiceName* 元素的 XML 服務屬性爲服務的名稱 (可接受字串值)。

ResourceName 元素

ResourceName 元素定義據以行動的物件。策略已經特別配置爲保護這個物件。不包含任何其他元素。*ResourceName* 元素的 XML 服務屬性爲物件的名稱。*ResourceName* 的範例可以是 `http://www.sunone.com:8080/images` (在 Web 伺服器上) 或 `ldap://sunone.com:389/dc=example,dc=com` (在目錄伺服器上)。更特定的資源可以是 `salary://uid=jsmith,ou=people,dc=example,dc=com`，其中將據以行動的物件是 John Smith 的薪資資訊。

AttributeValuePair 元素

AttributeValuePair 元素定義動作和動作的值。它被用來做爲 第 128 頁的 「Subject 元素」、第 128 頁的 「Referral 元素」及 第 128 頁的 「Condition 元素」的子元素。其同時包含 *Attribute* 與 *Value* 元素，而且沒有 XML 服務屬性。

Attribute 元素

Attribute 元素定義動作的名稱。一個動作爲在資源上執行的作業或事件。POST 或 GET 爲 Web 伺服器資源上執行的動作，READ 或 SEARCH 爲目錄伺服器上執行的動作。*Attribute* 元素必須與 *Value* 元素配對使用。*Attribute* 元素本身不包含其他任何元素。*Attribute* 元素的 XML 服務屬性爲動作的名稱。

Value 元素

Value 元素定義動作值。Allow/deny 或 yes/no 爲動作值範例。其他動作值可以是布林值、數字或字串。其值在定義於服務的 XML 檔案中 (以 `sms.dtd` 爲根據)。*Value* 元素不包含其他任何元素，而且也不包含 XML 服務屬性。

備註 – 拒絕規則永遠優先於允許規則。例如，如果一個策略是拒絕，另一種是允許，則結果是拒絕 (假如同時滿足這兩種策略條件)。由於拒絕策略可能導致這兩種策略之間產生潛在的衝突，因此建議您使用拒絕策略時要非常謹慎。如果使用明確的拒絕規則，透過不同主旨 (如角色和/或群組成員身份) 爲給定使用者指定的策略也可能會導致拒絕對資源存取。通常，策略定義程序應該僅使用允許規則。如果未套用其他策略則可能使用預設的拒絕。

Subject 元素

Subject 子元素辨識套用策略的主體集合；此簡介集合是根據群組中的成員、角色的擁有權或個別使用者進行選擇的。它接受 *Subject* 子元素。XML 屬性可定義爲：

name。可定義物件集合的名稱。

description。可定義主旨的描述。

includeType。 目前不使用。

Subject 元素

Subject 子元素辨識套用策略的主體集合；此集合指出 Subject 元素所定義的集合中較特別的物件。成員可以根據角色、群組成員或只是一些個別使用者。其包含子元素第 127 頁的「AttributeValuePair 元素」。必要的 XML 屬性爲 `type`，其辨識可從其中取得定義特殊之主旨的一般物件集合。其他的 XML 屬性包括 `name`，其定義物件集合的名稱、`includeType`，其定義是否已定義物件集合，並決定策略是否適用於「非」主旨成員的使用者。

備註 – 定義多重主旨時，至少一項主旨必須套用到使用者，才能套用策略。若主旨定義的 `includeType` 設爲 false，使用者不可以是策略套用的主旨之成員。

Referrals 元素

Referrals 子元素辨識策略參照集合。它接受 *Referral* 子元素。可對其定義的 XML 屬性爲 `name`，其定義物件集合的名稱及 `description` ，其接受描述。

Referral 元素

Referral 子元素辨識特定策略參照。其接受子元素 第 127 頁的「AttributeValuePair 元素」。對其而言必要的 XML 屬性是 `type`，其辨識可從其中取得定義特殊之參照的一般指定集合。它也可包含定義集合名稱的 `name` 屬性。

Conditions 元素

Conditions 子元素辨識策略限制集合 (時間範圍、認證層級等等)。它必須包含一或多個 *Condition* 子元素。可對其定義的 XML 屬性爲 `name`，其定義物件集合的名稱及 `description` ，其接受描述。

備註 – Conditions 元素爲策略中的選擇性元素。

Condition 元素

Condition 子元素辨識特定策略限制 (時間範圍、認證層級等等)。其接受子元素 第 127 頁的「AttributeValuePair 元素」。它的必要 XML 屬性爲 `type`，其辨識可從其中取得定義特殊的條件之一般限制集合。它也可包含定義集合名稱的 `name` 屬性。

新增啓用策略的服務

只有當服務模式的 <Policy> 元素配置爲 sms.dtd 時，才可以爲指定服務的資源定義策略。

依預設，Access Manager 提供 URL 策略代理程式服務 (iPlanetAMWebAgentService)。此服務於下列目錄中的 XML 檔案中定義：

```
/etc/opt/SUNWam/config/xml/
```

不過您可以增加其他策略服務到 Access Manager。一旦建立了策略服務，就可以透過 amadmin 指令行公用程式將其新增至 Access Manager。

▼ 新增啓用策略的服務

1 **在 XML 檔案中以 sms.dtd 爲根據開發新的策略服務。Access Manager 提供兩種策略服務 XML 檔案，您會想要使用以下兩種檔案作為新策略服務檔案的基礎：**

amWebAgent.xml - 這是預設 URL 策略代理程式服務的 XML 檔案。它位於 /etc/opt/SUNWam/config/xml/ 中。

SampleWebService.xml- 此範例策略服務檔位於 AccessManager-base/samples/policy。

2 **將 XML 檔案儲存到您即將從其中載入新策略服務的目錄。例如：**

```
/config/xml/newPolicyService.xml
```

3 **使用 amadmin 指令行公用程式載入新的策略服務。例如：**

```
AccessManager-base/SUNWam/bin/amadmin
    --runasdn “uid=amAdmin,ou=People,default_org,
root_suffix
    --password  password
    --schema /config/xml/newPolicyService.xml
```

4 **載入新的策略服務後，您可以透過 Access Manager 主控台，或透過 amadmin 載入新策略，來定義策略定義的規則。**

建立策略

您可透過策略 API 與 Access Manager 主控台建立、修改和刪除策略，並透過 amadmin 指令行工具建立和刪除策略。您也可以使用 amadmin 公用程式在 XML 中取得和列出策略。本節重點在透過 amadmin 指令行公用程式與透過 Access Manager 主控台建立策略。如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Developer's Guide」。

策略通常是以 XML 檔案建立，並透過 amadmin 指令行公用程式新增至 Access Manager，然後透過 Access Manager 主控台管理 (但可透過主控台建立策略)。這是因爲不能直接使用 amadmin 修改策略。若要修改策略，必須先從 Access Manager 刪除策略，然後使用 amadmin 加入修改後的策略。

通常策略是在範圍 (或子範圍) 層級建立，可在範圍的整個樹狀結構中使用。

▼ 使用 amadmin 建立策略

1 **根據 amadmin.dtd 建立策略 XML 檔。此檔案位於下列目錄：**

AccessManager-base /SUNWam/dtd

2 **策略 XML 檔案開發完成後，您可使用下列指令加以載入：**

AccessManager-base/SUNWam/bin/amadmin
--runasdn "uid=amAdmin,ou=People,*default_org*,
root_suffix"
--password *password*
--data *policy.xml*

若要同時加入多重策略，請將這些策略放在一個 XML 檔案中，這一點與在每個 XML 檔案中放一個策略相反。如果使用多重 XML 檔案連續快速載入策略，則內部策略索引可能會損毀，而且某些策略可能不參與策略評估。

透過 amadmin 建立策略時請確定：當建立認證方案條件時認證模組是以範圍註冊；當建立範圍、LDAP 群組、LDAP 角色和 LDAP 使用者時對應的 LDAP 物件範圍、群組、角色和使用者存在；當建立 IdentityServerRoles 主旨時 Access Manager 角色存在；當建立子範圍或同級範圍參照時相關範圍存在。

請注意，在 SubrealmReferral、PeerRealmReferral 的 Value 元素之內容中，Realm 主旨、IdentityServerRoles 主旨、LDAPGroups 主旨、LDAPRoles 主旨和 LDAPUsers 主旨必須爲完整的 DN。

▼ 以 Access Manager 主控台建立一般策略

1 **選擇您要為其建立策略的範圍。**

2 **按一下 [策略] 標籤。**

3 **按一下 [策略] 清單中的 [新建策略]。**

4 **新增策略的名稱與描述。**

5 **若您要策略為作用中，請選取 [作用中] 屬性中的 [Yes]。**

6 並且此時，無需定義一般策略的所有欄位。您可以建立策略，隨後再加入規則、主旨、條件和回應等。如需更多資訊，請參閱第 132 頁的「管理策略」。

7 按一下 [建立]。

▼ 以 Access Manager 主控台建立參照策略

1 選擇您要建立策略的範圍。

2 按一下 [策略] 標籤下的 [新建參照]。

3 新增策略的名稱與描述。

4 若您要策略為作用中，請選取 [作用中] 屬性中的 [Yes]。

5 此時，無需定義參照策略的所有欄位。您可以建立策略，隨後再加入規則和參照等。如需更多資訊，請參閱第 132 頁的「管理策略」。

6 按一下 [建立]。

建立同級範圍與子範圍的策略

要爲同級組織或子範圍建立策略，必須先在父系範圍 (或另一個同級範圍) 中建立參照策略。參照策略的規則定義中必須包含正由子範圍管理的資源前綴。在父系範圍 (或另一個同級範圍) 中建立參照策略後，可在子範圍 (或另一個同級範圍) 建立一般策略。

在此範例中，o=isp 是父系範圍，o=example.com 是子範圍，管理 http://www.example.com 的資源和子資源。

▼ 建立子範圍的策略

1 於 o=isp 建立參照策略。如需參照策略的相關資訊，請參閱程序第 135 頁的「修改參照策略」。

參照策略必須定義 http://www.example.com 做爲規則中的資源，且必須包含以 example.com 做爲參照中的值之 SubRealmReferral。

2 瀏覽至子範圍 example.com。

3 目前，isp 將資源參考為 example.com，可以為資源 http://www.example.com 或任何以 http://www.example.com 開頭的資源建立一般策略。

若要定義由 example.com 管理的其他資源之策略，必須在 o=isp 建立額外的參照策略。

管理策略

建立一般策略或參照策略並加入 Access Manager 後，您即可透過 Access Manager 主控台管理策略，方法是修改規則、主旨、條件與參照。

修改一般策略

透過 [策略] 標籤，您可修改用來定義存取權限的一般策略。您可定義和配置數個規則、主旨、條件和資源主較程式。此節列出和說明其步驟。

▼ 新增或修改一般策略的規則

1 **若您已建立策略，按一下您要新增規則的策略名稱。若還沒建立，請參閱****第 130 頁的「以 Access Manager 主控台建立一般策略」**。

2 **於 [規則] 功能表下，按一下 [新建]**。

3 **為規則選取下列預設服務類型之一。啓用策略的服務越多，您可以參閱的清單就越大**：

探索服務	定義探索服務查詢的授權動作，並修改 Web 服務用戶端對特定資源的協定呼叫。
Liberty 個人設定檔服務	定義 Liberty 個人設定檔服務查詢的授權動作，並修改 Web 服務用戶端對特定資源的協定呼叫。
URL 策略代理程式	爲策略執行提供 URL 策略代理程式服務。此服務可讓管理員透過策略執行程式或策略代理程式建立與管理策略。

4 **按 [下一步]**。

5 **輸入規則的名稱與資源名稱**。

目前，策略代理程式僅支援 `http://` 與 `https://` 資源，而不支援以 IP 位址取代主機名稱。

主機、連接埠和資源名稱皆支援萬用字元。例如：

```
http*://*:*/*.html
```

對 URL 策略代理程式服務而言，若未輸入連接埠埠號，則 `http://` 的預設埠號爲 80、`https://` 的預設埠號爲 443。

6 **為此規則選取動作。若您是使用 URL 策略代理程式服務，可以選擇**：

- GET
- POST

7 **選取動作值**。

- 允許 — 允許您存取與規則中所定義資源相符的資源。
- 拒絕 — 不允許您存取與規則中所定義資源相符的資源。
- [拒絕] 規則永遠優先於 [允許] 規則。例如，如果指定的資源有兩種策略，一種是拒絕存取，另一種是允許存取，則結果是拒絕存取 (假如同時滿足這兩種策略條件)。由於拒絕策略可能導致這兩種策略之間產生潛在的衝突，因此建議您使用拒絕策略時要非常謹慎。策略定義程序應該僅使用允許規則。若資源未套用任何策略，會自動拒絕存取。

  如果使用明確的拒絕規則，即使有一個或多個策略允許存取，透過不同主旨如角色和或群組成員身份爲給定使用者指定的策略也可能會導致拒絕對資源存取。例如，如果存在一個適用於員工角色之資源的拒絕策略，還存在另一個適用於管理員角色之相同資源的允許策略，系統將會拒絕指定給使用者 (員工角色和管理員角色 的策略決策。

  解決此問題的一種方法爲使用條件外掛程式設計策略。在上述情況中，「角色條件」(將拒絕策略套用於認證爲員工角色之使用者，並將允許策略套用至認證爲經理角色之使用者) 協助區分這兩種策略。另一種方法爲使用 `authentication level` 條件，其中經理角色是在較高認證層級進行認證。

8 **按一下 [完成]。**

▼ 新增或修改一般策略的主旨

1 **若您已建立策略，按一下您要新增主旨的策略名稱。若您尚未建立策略，請參閱****第 130 頁的「以 Access Manager 主控台建立一般策略」****。**

2 **於 [主旨] 清單下，按一下 [新建]。**

3 **選取其中一個預設主旨類型。如需要主旨類型的說明，請參閱****第 122 頁的「主旨」****。**

4 **按 [下一步]。**

5 **輸入此主旨的名稱。**

6 **選取或取消選取 [專用] 欄位。**

如果未選取此欄位 (預設)，則此策略將套用於屬於主旨成員的識別。如果選取此欄位，則此策略將套用於不屬於主旨成員的識別。

若策略中有數個主旨，策略將套用至至少爲其中一個主旨之成員的識別。

7 **執行搜尋，以便顯示要加入至此主旨的識別。此步驟不適用於 [已認證的使用者] 主旨或 [Web 服務用戶端] 主旨。**

預設 (*) 搜尋式樣將顯示所有項目。

8 **選取要為此主旨加入的個別身份，或按一下 [全部加入] 以立即加入所有身份。按一下 [新增]，以將識別移至選取的清單。此步驟不適用於 [已認證的使用者] 主旨。**

9 按一下 [完成]。

10 若要從策略中移除某主旨，請選取此主旨並按一下 [刪除]。按一下主旨名稱可以編輯任何主旨定義。

▼ 將條件新增至一般策略

1 若您已建立策略，按一下您要新增規則的策略名稱。若您尚未建立策略，請參閱第 130 頁的「以 Access Manager 主控台建立一般策略」。

2 於 [條件] 清單下，按一下 [新建]。

3 選取條件類型並按 [下一步]。

4 定義條件類型的欄位。如需條件類型的說明，請參閱第 123 頁的「條件」。

5 按一下 [完成]。

▼ 將回應提供者新增至一般策略

1 若您已建立策略，按一下您要新增回應提供者的策略名稱。若您尚未建立策略，請參閱第 130 頁的「以 Access Manager 主控台建立一般策略」。

2 於 [回應提供者] 清單下，按一下 [新建]。

3 輸入回應提供者的名稱。

4 定義下列值：

StaticAttribute	含名字與值的回應屬性，定義於 `IDResponseProvider` 實例中並儲存於策略中。
DynamicAttribute	此處所選擇的回應屬性首先需要定義於對應之範圍的「策略配置服務」中。定義的屬性名稱應與那些存在於配置資料庫中的屬性相同。如需有關如何定義屬性的詳細資料，請參閱「Access Manager 線上說明」中的策略配置屬性定義。

5 按一下 [完成]。

6 若要從策略中移除回應提供者，請選取主旨，然後按一下 [刪除]。按一下名稱可以編輯任何回應提供者定義。

修改參照策略

您可將範圍的策略定義和決策委派其他使用參照策略的範圍。自訂參照可用以從任何策略目標點取得策略決策。建立參照策略後，可新增或修改關聯的規則、參照和資源提供者。

▼ 新增或修改參照策略的規則

1 **若您已建立策略，按一下您要新增規則的策略名稱。若還沒建立，請參閱****第 131 頁的 「以 Access Manager 主控台建立參照策略」**。

2 **於 [規則] 清單下，按一下 [新建]**。

3 **為規則選取下列預設服務類型之一。啓用策略的服務越多，您可以參閱的清單就越大：**

探索服務	定義探索服務查詢的授權動作，並修改 Web 服務用戶端對特定資源的協定呼叫。
Liberty 個人設定檔服務	定義 Liberty 個人設定檔服務查詢的授權動作，並修改 Web 服務用戶端對特定資源的協定呼叫。
URL 策略代理程式	爲策略執行提供 URL 策略代理程式服務。此服務可讓管理員透過策略執行程式或策略代理程式建立與管理策略。

4 **按 [下一步]**。

5 **輸入規則的名稱與資源名稱**。

目前，策略代理程式僅支援 `http://` 與 `https://` 資源，而不支援以 IP 位址取代主機名稱。

資源名稱、連接埠號和協定可以使用萬用字元。例如：

```
http://*:*/*.html
```

對 URL 策略代理程式服務而言，若未輸入連接埠埠號，則 `http://` 的預設埠號爲 80、`https://` 的預設埠號爲 443。

若要允許管理安裝於特定機器上所有伺服器的資源，您可將資源定義爲 `http://host*:*.`。另外，您可定義以下資源以授與管理員存取特定組織中所有服務的特定組織權限。

`http://*.`*`subdomain.domain.topleveldomain`*

6 **按一下 [完成]**。

▼ 新增或修改策略的參照

1 **若您已建立策略，按一下您要新增回應提供者的策略名稱。若您尚未建立策略，請參閱****第 131 頁的 「以 Access Manager 主控台建立參照策略」**。

2. **於 [規則] 清單下，按一下 [新建]。**

3. **選取 [服務] 類型。**

4. **定義 [規則] 欄位中的資源。這些欄位包括：**
   參照— 顯示目前的參照類型。

   名稱— 輸入參照的名稱。

   資源名稱— 輸入資源的名稱。

   篩選器— 指定將要顯示在 [值] 欄位中的組織名稱之篩選器。依預設，其將顯示所有組織名稱。

   值— 選取參照的組織名稱。

5. **按一下 [完成]。**
   若要從策略中移除某個參照，請選取此參照，然後按一下 [刪除]。

   可以透過按一下參照名稱旁邊的 [編輯] 連結，編輯任何參照定義。

▼ 將回應提供者新增至參照策略

1. **若您已建立策略，按一下您要新增回應提供者的策略名稱。若您尚未建立策略，請參閱**第 130 頁的「以 Access Manager 主控台建立一般策略」。

2. **於 [回應提供者] 清單下，按一下 [新建]。**

3. **輸入回應提供者的名稱。**

4. **定義下列值：**

StaticAttribute	含名字與值的回應屬性，定義於 `IDResponseProvider` 實例中並儲存於策略中。
DynamicAttribute	僅含所選取名稱的回應屬性，選取於策略中的 `IDResponseProvider`。根據策略評估期間的使用者識別請求，可從 `IDRepostitories` 讀取該值。

5. **按一下 [完成]。**

6. **若要從策略中移除回應提供者，請選取主旨，然後按一下 [刪除]。按一下名稱可以編輯任何回應提供者定義。**

策略配置服務

策略配置服務用來爲每個組織透過 Access Manager 主控台配置每個策略相關屬性。您也可定義資源名稱實作和 Directory Server 資料存放區，以和 Access Manager 策略架構一起使用。[策略配置服務] 中指定的 Directory Server 用於 LDAP 使用者、LDAP 群組、LDAP 角色和組織策略主旨的成員身份評估。

主旨結果存在時間

若要改善策略評估表現，成員身份評估將快取一段時間 (以策略配置服務中 [主旨結果存在時間] 屬性中定義的時間爲基準)。將一直使用這些快取成員身份決策，直到 [主旨結果存在時間] 屬性定義之時間結束。在這之後，成員身份評估會用於反映目錄中使用者的目前狀態。

動態屬性

這些爲允許的動態屬性名稱，其顯示於清單中，並可選取以定義策略回應提供者動態屬性。定義的名稱需要與資料儲存庫中定義的屬性名稱相同。

amldapuser 定義

`amldapuser` 是在安裝中建立的使用者，預設由 [策略配置] 服務中指定的 Directory Server 使用。若有必要，範圍的管理員或策略管理員可變更此值。

加入策略配置服務

建立範圍時，會自動設定範圍的 [策略配置] 服務屬性。然而，若有必要您可加以修改。

基於資源的認證

有些組織需要有進階認證方案，使用者可根據特定模組、根據試圖存取的資源進行認證。基於資源的認證是 Access Manager 的一項功能，使用者必須通過用以保護資訊的特定認證模組的認證，而非預設認證模組。此功能僅適用於首次使用者認證。

備註 – 這是與第 117 頁的 「階段作業升級」中描述的基於資源認證不同的功能。該特定功能並不具有任何限制。

限制

基於資源的認證有下列限制：

- 若適用於資源的策略具有多重認證模組，系統將任意選取一個認證模組。
- 層級和方案是唯一可以爲此策略定義的條件。
- 此功能不能跨不同 DNS 網域運作。

▼ 配置基於資源的認證

Access Manager 和策略代理程式都安裝好之後，就可以配置基於資源的認證。要這樣做，必須先將 Access Manager 指向 Gateway servlet。

1 開啓 `AMAgent.properties`。

`AMAgent.properties` 可以在 (於 Solaris 環境中) `/etc/opt//SUNWam/agents/config/` 中找到。

2 註釋下面的行：

```
#com.sun.am.policy.am.loginURL = http://Access
Manager_server_host.domain_name:port/amserver/UI/Login.
```

3 新增下列行到檔案中：

```
com.sun.am.policy.am.loginURL =
http://AccessManager_host.domain_name:port/amserver/gateway
```

備註 – 開道 servlet 使用策略評估 API 開發，並可用來撰寫自訂機制以完成基於資源的認證。「Sun Java System Access Manager 7 2005Q4 Developer's Guide」中的第 6 章「Using the Policy APIs」的第 6 章「Using the Policy APIs」。

---

4 重新啓動代理程式。

◆ ◆ ◆ 第 9 章

9 管理主旨

[主旨] 介面可在範圍內進行基本識別管理。您建立於 [主旨] 介面中的識別可用於以 Access Manager 識別物件類型建立之策略的主旨定義中。

您可以建立與修改的識別爲：

使用者

使用者代表一個個別的識別。可於群組中建立與刪除使用者，並可由角色和/或群組新增或移除。您亦可對使用者指定服務。

▼ 建立或修改使用者

1 **按一下 [使用者] 標籤**。

2 **按一下 [開啓新檔]**。

3 **輸入下列欄位的資料**：

使用者 **ID**。 此欄位採用其將登入 Access Manager 的使用者名稱。此特性可爲非 DN 值。

名字。此欄位中採用使用者的名字。

姓氏。此欄位採用使用者的姓氏。

全名 — 此欄位採用使用者的全名。

密碼。— 此欄位中爲 [使用者 ID] 欄位中所指定名稱的密碼。

密碼 (確認) — 確認密碼。

使用者狀態。此選項指出是否允許使用者透過 Access Manager 認證。

4 按一下 [建立]。

5 一旦建立了使用者，您可以按一下使用者名稱來編輯使用者資訊。如需使用者資訊，請參閱使用者屬性。您可執行的其他修改：

- 第 139 頁的 「建立或修改使用者」
- 第 140 頁的 「新增使用者至角色與群組」
- 第 140 頁的 「新增服務至一個識別」

▼ 新增使用者至角色與群組

1 按一下您要修改的使用者名稱。

2 選取角色或群組。僅顯示已指定給使用者的角色與群組。

3 由 [可用的] 清單選取角色或群組並按一下 [新增]。

4 一旦角色或群組顯示於 [選取的] 清單中，按一下 [儲存]。

▼ 新增服務至一個識別

1 選取您要新增服務的識別。

2 按一下 [服務] 標籤。

3 按一下 [加入]。

4 依據您所選取的識別類型，將顯示下列服務清單：

- 認證配置
- 探索服務
- Liberty 個人設定檔服務
- 階段作業
- 使用者

5 選取您要新增的服務，並按 [下一步]。

6 編輯服務的屬性。如需有關服務的說明，請按一下步驟 4 中的服務名稱。

7 按一下 [完成]。

代理程式

Access Manager 策略代理程式會保護 Web 伺服器和 Web 代理伺服器上的內容，以避免未經授權的侵入。它們會根據管理員配置的策略，來控制對服務和 Web 資源的存取。

代理程式物件定義策略代理程式設定檔，可讓 Access Manager 儲存認證及其他有關保護 Access Manager 資源之特定代理程式的設定檔資料。經由 Access Manager 主控台，管理員可以檢視、建立、修改和刪除代理程式設定檔。

在代理程式物件建立頁面，可以對 Access Manager 認證代理程式定義 UID/密碼。若您具有使用相同的 Access Manager 的多重 AM/WS，您可以對不同代理程式啓用多重 ID，並由 Access Manager 個別地啓用與停用。您亦可集中管理代理程式的某些喜好設定值，而不是在每個機器上編輯 `AMAgent.properties`。

▼ 建立或修改代理程式

1 **按一下 [代理程式] 標籤**。

2 **按一下 [開啓新檔]**。

3 **輸入下列欄位值**：

名稱。 輸入代理程式的名稱或識別。這是代理程式將用來登入到 Access Manager 的名稱。不接受多位元的名稱。

密碼。 輸入代理程式密碼。此密碼必須與 LDAP 認證期間代理程式所使用的密碼不同。

確認密碼。確認密碼。

裝置狀態。 輸入代理程式的裝置狀態。如果設定爲 [作用中]，則代理程式能夠認證進入並與 Access Manager 通訊。如果設定爲 [非作用中]，則代理程式無法認證進入 Access Manager。

4 **按一下 [建立]**。

5 **一旦您建立了代理程式，您可以另外編輯下列欄位**：

描述。 輸入代理程式的簡要描述。例如，您可以輸入代理程式實例名稱或其保護的應用程式名稱。

代理程式密鑰值。 以一個密鑰/值對設定代理程式特性。Access Manager 使用此特性來接收有關使用者憑證指定的代理程式請求。目前，僅有一個特性有效，且將忽略所有其他特性。請使用以下格式：

agentRootURL=`http://` *server_name:port/*

建立唯一的策略代理程式識別

依預設，當您於信任的環境中建立多個策略代理程式時，策略代理程式包含相同的 UID 與密碼。因爲共用 UID 與密碼，Access Manager 無法分辨代理程式，其使得階段作業保持開啓狀態可能被截取資訊。

當 [識別提供者] 提供有關爲協力廠商或企業中未授權群組所開發的應用程式 (或 [服務提供者]) 之使用者的認證、授權與設定檔資訊時，此弱點可能顯現。可能的安全性問題是：

- 所有應用程式會共用相同的 http 階段作業 cookie。這樣有可能會使得惡意的應用程式奪取階段作業 cookie 並於另一個應用程式中假冒使用者。
- 若應用程式並未使用 https 協定，階段作業 cookie 容易遭到網路竊聽。
- 只要有一個應用程式可被奪取，整個基礎架構的安全性就有受到危害的風險。
- 惡意的應用程式可使用階段作業 cookie 來取得使用者的設定檔屬性並有可能進行修改。若使用者擁有管理權限，應用程式將可能造成更大的災害。

▼ 建立唯一的策略代理程式識別

1 使用 Access Manager 管理控制台為每個代理程式建立項目。

2 執行下列於建立代理程式期間輸入的密碼指令。應在安裝代理程式的主機上呼叫此命令。

```
AccessManager-base/SUNWam/agents/bin/crypt_util agent123
```

如此將提供下列輸出：

```
WnmKUCg/y3l404ivWY6HPQ==
```

3 變更 AMAgent.properties 以反映新值，然後重新啓動代理程式。範例：

```
# The username and password to use for the Application

authentication module.



com.sun.am.policy.am.username = agent123

com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==



# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

com.sun.am.policy.agents.cdsso-enabled=true
```

```
# This is the URL the user will be redirected to after successful login

# in a CDSSO Scenario.

com.sun.am.policy.agents.cdcservletURL = http://server.example.com:port

/amserver/cdcservlet
```

4 **變更安裝 Access Manager 所在的** `AMConfig.properties` **以反映新值，然後重新啓動 Access Manager。範例：**

```
com.sun.identity.enableUniqueSSOTokenCookie=true

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer



com.sun.identity.authentication.uniqueCookieDomain=.example.com
```

5 **於 Access Manager 主控台中，選取 [配置] > [平台]。**

6 **在 [Cookie 網域] 清單中，變更 Cookie 網域名稱：**

a. **選取預設的** `iplanet.com` **網域，然後按一下 [移除]。**

b. **輸入安裝 Access Manager 的主機名稱，然後按一下 [新增]。**

範例：`server.example.com`

您應該會在瀏覽器上看見兩組 Cookie：

- iPlanetDirectoryPro – 伺服器。example.com (主機名稱)
- sunIdentityServerAuthNServer – example.com (主機名稱)

篩選的角色

篩選的角色是經由使用 LDAP 篩選器而建立的動態角色。建立角色時，所有使用者都會透過篩選器的篩選並指定給角色。篩選器會在項目中尋找任何屬性值對 (例如，`ca=user*`)，並自動指定包含該屬性的使用者給角色。

▼ 建立篩選的角色

1 **於 [瀏覽] 窗格中，跳至將建立角色的組織。**

2 **按一下 [開啓新檔]。**

3. **輸入篩選角色的名稱。**

4. **輸入搜尋條件的資訊。**

   例如，

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   若篩選器依預設爲空白，將建立下列角色：

   ```
   (objectclass = inetorgperson)
   ```

5. **按一下 [建立] 以根據篩選器條件初始搜尋。由篩選器條件定義的識別將自動地指定給角色。**

6. **一旦建立了篩選的角色，按一下角色名稱以檢視屬於角色的使用者。您亦可按一下 [服務] 標籤來新增服務至角色。**

角色

角色的成員是角色的 LDAP 項目。角色自己的條件已定義爲含屬性的 LDAP 項目，爲項目的識別名稱 (DN) 屬性所辨識。一旦建立了角色，您可以手動新增服務與使用者。

▼ 建立或修改角色

1. **按一下 [角色] 標籤。**
2. **在角色清單中按一下 [新建]。**
3. **輸入角色的名稱。**
4. **按一下 [建立]。**

▼ 新增使用者至角色或群組

1. **按一下您要新增使用者的角色或群組名稱。**
2. **按一下 [使用者] 標籤。**
3. **從 [可用] 清單選取您要新增的使用者並按一下 [新增]。**
4. **一旦使用者顯示於 [選取的] 清單中，按一下 [儲存]。**

群組

群組代表具有共同功能、特性或興趣的使用者集合。通常，此群組並無與之相關聯的權限。群組可以兩個層級存在；於組織內及於其他受管理群組內。

▼ 建立或修改群組

1 **按一下 [群組] 標籤**。

2 **按一下群組清單上的 [新建]**。

3 **輸入群組的名稱**。

4 **按一下 [建立]**。

一旦您建立了群組，您可以按一下群組名稱與 [使用者] 標籤，將使用者新增至群組。

第 III 部分

目錄管理和預設服務

這是「Sun Java System Access Manager 7 2005Q4 管理指南」的第三部分。「目錄管理」一章中描述以「舊有」模式部署 Access Manager 時，管理「目錄」物件的方法。其他章節描述配置與使用某些 Access Manager 預設服務的方法。本部分包含以下章節：

◆ ◆ ◆ 第 10 章

10 目錄管理

只有在於「舊有」模式下安裝 Access Manager 時，才會顯示 [目錄管理] 標籤。此目錄管理特性爲啓用 Sun Java System Directory Server 的 Access Manager 部署提供一個識別管理解決方案。

如需有關「舊有」模式安裝選項的更多資訊，請參閱「Sun Java Enterprise System 2005Q4 Installation Guide for UNIX」。

管理目錄物件

[目錄管理] 標籤包含檢視與管理 Directory Server 物件所需的所有元件。本節說明物件類型及有關如何配置它們的詳細資訊。使用 Access Manager 主控台或指令行介面可以定義、修改或刪除使用者、角色、群組、組織、子組織及容器物件。主控台有具權限程度不同的預設管理員，用以建立與管理目錄物件。(可基於角色建立其他管理員。)當與 Access Manager 一起安裝時，可於 Directory Server 內定義管理員。您可管理的 Directory Server 物件有：

組織

組織代表企業用來管理其部門與資源的階層式結構之頂層。安裝時，Access Manager 會動態建立頂層組織 (安裝期間定義) 以管理 Access Manager 企業配置。安裝後可以建立其他組織以管理個別企業。所有建立的組織均位於頂層組織之下。

▼ 建立組織

1 **按一下 [目錄管理] 標籤。**

2 **在 [組織] 清單中，按一下 [新建]。**

3 **輸入欄位的值。僅 [名稱] 是必需的。這些欄位包括：**

名稱 輸入組織名稱的值。

網域名稱 輸入組織的完整領域名稱系統 (DNS) 名稱 (如果有)。

組織狀態 選擇**作用中**或**非作用中**狀態。預設值爲**作用中**。在組織存在期間，可以透過選取 [內容] 圖示隨時變更該狀態。如果選擇**非作用中**，系統會在使用者登入組織時停用使用者存取。

組織別名 此欄位定義組織的別名，可讓您使用這些別名經由 URL 登入進行認證。例如，如果您有一個名爲 `exampleorg` 的組織，並將 `123` 與 `abc` 定義爲別名，則您可使用以下任一個 URL 登入該組織：

```
http://machine.example.com/amserver/UI/Login?org=exampleorg

http://machine.example.com/amserver/UI/Login?org=abc

http://machine.example.com/amserver/UI/Login?org=123
```

組織別名在整個組織中必須是唯一的。您可以使用 [唯一屬性清單] 強制唯一性。

DNS 別名名稱 允許加入組織的 DNS 名稱別名。此屬性僅接受「實際的」網域別名 (不允許使用隨機字串)。例如，如果您有一個名爲 `example.com` 的 DNS，並將 `example1.com` 與 `example2.com` 定義爲組織 `exampleorg` 的別名，則您可使用以下任一個 URL 登入該組織：

```
http://machine.example.com/amserver/UI/

Login?org=exampleorg

http://machine.example1.com/amserver/

UI/Login?org=exampleorg

http://machine.example2.com/amserver/

UI/Login?org=exampleorg
```

唯一的屬性清單 允許您在組織中加入使用者的唯一屬性名稱清單。例如，如果您加入了指定電子郵件位址的唯一屬性名稱，則無法建立兩個具有相同電子郵件位址的使用者。此欄位還可以接受以逗號分隔的清單。清單中的任一屬性名稱均定義唯一性。例如，如果欄位包含屬性名稱清單：

PreferredDomain, AssociatedDomain

而且爲特定使用者將 PreferredDomain 定義爲 http://www.example.com，則對該 URL 而言，此以逗號分隔的整個清單定義是唯一的。將命名屬性 ou 新增至 [唯一的屬性清單] 將不會對預設群組、使用者容器強制執行唯一性。(ou=Groups,ou=People)。

此一唯一性同時針對所有子組織強制執行。

4 **按一下 [確定]**。

新組織會顯示於 [組織] 清單中。若要編輯您建立組織時定義的任一特性，請按一下您要編輯的組織之名稱、變更其特性，然後按一下 [儲存]。

▼ 刪除組織

1 **勾選將要刪除的組織之名稱旁的核取方塊**。

2 **按一下 [刪除]**。

備註 – 執行刪除時不會顯示警告訊息。組織中的所有項目將被刪除，且無法執行還原。

將組織加入到策略

Access Manager 物件會透過策略的 subject 定義加入策略。當建立或修改策略時，可以將組織、角色、群組及使用者定義爲主旨。一旦定義了主旨，策略即會套用於物件。如需更多資訊，請參閱第 132 頁的 「管理策略」。

容器

當由於物件類別與屬性差異而無法使用組織項目時，會使用容器項目。請切記，Access Manager 容器項目與 Access Manager 組織項目不一定等於 LDAP 物件類別 organizationalUnit 與 organization。它們是抽象的識別項目。理想情況下，將使用組織項目而不是容器項目。

備註 – 容器的顯示是選擇性的。若要檢視容器，您必須在 [配置] > [主控台特性] 下選取 [管理] 服務的 [顯示容器]。

▼ 要建立容器

1. 選取組織或容器的位置連結，新容器將會建立於其中。
2. 按一下 [容器] 標籤。
3. 按一下 [容器] 清單中的 [新建]。
4. 輸入將要建立的容器之名稱。
5. 按一下 [確定]。

▼ 要刪除容器

1. 按一下 [容器] 標籤。
2. 選取要刪除的容器名稱旁邊的核取方塊。
3. 按一下 [刪除]。

備註 – 刪除一個容器將會同時刪除該容器中存在的所有物件。包含所有物件和子容器。

群組容器

群組容器用於管理群組。它僅可包含群組與其他群組容器。群組容器「群組」會動態指定爲所有受管理群組的父系項目。如果需要，可以加入附加群組容器。

備註 – 群組容器的顯示是選擇性的。若要檢視群組容器，您必須從 [配置] > [主控台特性] 的 [認證] 服務中選取 [啓用群組容器]。

▼ 建立群組容器

1. 選取包含新群組容器的組織或群組容器的位置連結。
2. 選取 [群組容器] 標籤。
3. 按一下 [群組容器] 清單中的 [新增]。
4. 在 [名稱] 欄位中輸入值，然後按一下 [確定]。新的群組容器會顯示於 [群組容器] 清單中。

▼ 刪除群組容器

1. **導覽至包含要刪除的群組容器之組織**。
2. **選擇 [群組容器] 標籤**。
3. **選取要刪除的群組容器旁邊的核取方塊**。
4. **按一下 [刪除]**。

群組

群組代表包含一般功能、特性或興趣的使用者集合。通常，此群組並無與之相關聯的權限。群組可以兩個層級存在；於組織內及於其他受管理群組內。存在於其他群組中的群組稱爲子群組。子群組是「實際上」存在於父系群組中的子節點。

Access Manager 還支援 巢式群組，巢式群組是單一群組中包含現有群組的「陳述」。巢式群組與子群組不同，它可存在於 DIT 中任何之處。它們可讓您爲大量使用者快速設置存取權限。

您可建立的群組有兩種：靜態群組與動態群組。您只能以手動方式將使用者加入靜態群組；動態群組則透過篩選器控制使用者的加入。巢式群組與子群組皆可加入這兩種類型的群組。

靜態群組

靜態群組是根據您指定之管理的群組類型所建立的。群組成員是使用 `groupOfNames` 或 `groupOfUniqueNames` 物件類別加入群組項目。

備註 – 依預設，受管理群組類型爲動態。您可在管理服務配置中變更該預設。

動態群組

動態群組是透過使用 LDAP 篩選器所建立。所有項目都會透過器篩選並動態指定給群組。篩選器可尋找項目中的任一屬性，並傳回包含該屬性的項目。例如，如果要根據建立編號建立群組，可以使用篩選器傳回包含建立編號屬性的所有使用者的清單。

備註 – 應使用 Directory Server 將 Access Manager 配置爲可使用 referential integrity 外掛程式。啓用後的參考完整性外掛程式會在刪除或重新命名工作完成後，立即對指定的屬性執行完整性更新。這可確保在整個資料庫中維持相關項目之間的關係。資料庫索引可增強中的搜尋效能。如需有關啓用外掛程式的更多資訊，請參閱「Sun Java System Access Manager 6 2005Q1 Migration Guide」。

▼ 建立靜態群組

1. **瀏覽將於其中建立新群組的組織、組或群組容器。**
2. **按一下 [群組] 清單的 [新建靜態]。**
3. **在 [名稱] 欄位中輸入群組的名稱。按 [下一步]。**
4. **選取 [使用者可以訂閱該群組] 屬性以允許使用者自行訂閱群組。**
5. **按一下 [確定]。**
   建立群組之後，您便可以選取群組的名稱並按一下 [一般] 標籤，來編輯 [使用者可以訂閱至此群組] 屬性。

▼ 加入或移除靜態群組成員

1. **在 [群組] 清單中選取將對其加入成員的群組。**
2. **在 [選取動作] 功能表中選擇要執行的動作。您可以執行的動作如下所示：**

新建使用者	此動作會建立新的使用者並在儲存該使用者資訊時將其加入群組。
加入使用者	此動作將現有使用者加入群組。選取此動作時，您會建立指定所要加入的使用者之搜尋條件。用於建構條件的欄位會使用 ANY 或 ALL 運算子。ALL 會傳回所有指定欄位的使用者。ANY 會傳回任一指定欄位的使用者。如果保留某欄位空白，則該欄位將符合該特定屬性的所有可能項目。 建構了此搜尋條件後，即按一下 [下一步]。從傳回的使用者清單中，選取您要加入的使用者，然後按一下 [完成]。
加入群組	此動作將巢式群組加入目前群組。選擇此動作時，您建立了搜尋條件，包括搜尋範圍、群組名稱 (接受「*」萬用字元)，並且您可以指定使用者是否可以自行訂閱群組。輸入資訊後，即按一下 [下一步]。從傳回的群組清單中，選取您要加入的群組，然後按一下 [完成]。
移除成員	此動作將從群組中移除成員 (包括使用者與群組)，但不會刪除它們。選取您要移除的成員，然後從 [選取動作] 功能表中選取 [移除成員]。
刪除成員	此動作將永久刪除您選取的成員。選取您要刪除的成員，然後選擇 [刪除成員]。

▼ 建立動態群組

1. **瀏覽將於其中建立新群組的組織或群組。**
2. **按一下 [群組] 頁籤。**

3 **按一下 [新建動態]。**

4 **在 [名稱] 欄位中輸入群組的名稱。**

5 **建構 LDAP 搜尋篩選器。**

依預設，Access Manager 顯示基本搜尋篩選器介面。用於建構篩選器的 [基本] 欄位使用 ANY 或 ALL 運算子。ALL 會傳回所有指定欄位的使用者。ANY 會傳回任一指定欄位的使用者。如果保留某欄位空白，則該欄位將符合該特定屬性的所有可能項目。

6 **按一下 [確定] 後，符合搜尋條件的所有使用者會自動加入群組。**

▼ 若要加入或移除動態群組的成員

1 **在 [群組] 清單中，按一下要對其加入成員的群組之名稱。**

2 **在 [選取動作] 功能表中選擇要執行的動作。您可以執行的動作如下所示：**

加入群組　此動作將巢式群組加入目前群組。選擇此動作時，您建立了搜尋條件，包括搜尋範圍、群組名稱 (接受「*」萬用字元)，並且您可以指定使用者是否可以自行訂閱群組。輸入資訊後，即按一下 [下一步]。從傳回的群組清單中，選取您要加入的群組，然後按一下 [完成]。

移除成員　此動作將從群組中移除成員 (包括群組)，但不刪除它們。選取您要移除的成員，然後選擇 [移除成員]。

刪除成員　此動作將永久刪除您選取的成員。選取您要刪除的成員，然後選擇 [刪除成員]。

將群組加入到策略

Access Manager 物件會透過策略的 subject 定義加入策略。當建立或修改策略時，可以將組織、角色、群組及使用者定義爲策略主旨頁面中的主旨。一旦定義了主旨，策略即會套用於物件。如需更多資訊，請參閱第 132 頁的 「管理策略」。

使用者容器

使用者容器是預設的 LDAP 組織單元，爲在組織中建立使用者時，所有使用者的指定位置。可以在組織層級和使用者容器層級找到使用者容器 (作爲子使用者容器)。它們僅可包含其他使用者容器與使用者。如果需要，可以將附加使用者容器加入組織。

備註 – 使用者容器的顯示是選擇性的。若要檢視使用者容器，必須在 [管理服務] 中選取 [啓用使用者容器]。

▼ 建立使用者容器

1. 導覽至要在其中建立新使用者容器的組織或使用者容器。
2. 按一下 [使用者容器] 清單中的 [新建]。
3. 輸入要建立的使用者容器名稱。
4. 按一下 [確定]。

▼ 刪除使用者容器

1. 導覽至包含要刪除的使用者容器之組織或使用者容器。
2. 選取要刪除的使用者容器名稱旁邊的核取方塊。
3. 按一下 [刪除]。

備註 – 刪除一個使用者容器將會同時刪除該使用者容器中存在的所有物件。包含所有使用者和子使用者容器。

使用者

使用者代表個別使用者的識別。透過 Access Manager 識別管理模組，您可以在組織、容器以及群組中建立和刪除使用者；在角色和/或群組中加入或移除使用者。您亦可對使用者指定服務。

備註 – 如果子組織內的使用者是使用與 `amadmin` 相同的使用者 ID 建立的，`amadmin` 的登入會失敗。若發生此問題，管理員應透過 Directory Server 主控台變更使用者的 ID。如此可使管理員登入到預設組織中。此外，認證服務中的 [啓動使用者搜尋] 可以設爲使用者容器，以確保登入時傳回獨特的比對結果。

▼ 建立使用者

1. 導覽至要在其中建立使用者的組織、容器或使用者容器。
2. 按一下 [使用者] 標籤。
3. 按一下使用者清單上的 [新建]。

4 **輸入下列欄位的資料：**

使用者 ID	此欄位採用其將登入 Access Manager 的使用者名稱。此特性可爲非 DN 值。
名字	此欄位中爲使用者的名字。[目前登入] 欄位中的 [名字] 值和 [姓氏] 值可識別使用者。這並非必需填寫的值。
姓氏	此欄位採用使用者的姓氏。[名字] 的值與 [姓氏] 的值會識別使用者身份。
全名	此欄位中爲使用者的全名。
密碼	此欄位中爲 [使用者 ID] 欄位中所指定名稱的密碼。
密碼 (確認)	確認密碼。
使用者狀態	此選項指出是否允許使用者透過 Access Manager 認證。只有作用中的使用者才可以認證。預設值爲**作用中**。

5 **按一下 [確定]**。

▼ 若要編輯使用者設定檔

當尚未被指定管理員角色的使用者進行 Access Manager 認證時，預設的檢視爲使用者自己的 [使用者設定檔]。 此外，具適當權限的管理員可以編輯使用者設定檔。在此檢視中，使用者可以修改其個人設定檔的特定屬性值。[使用者設定檔] 檢視中顯示的屬性可以延伸。如需加入物件與識別的自訂屬性之相關詳細資訊，請參閱「Access Manager Developer's Guide」。

1 **選取要編輯其設定檔的使用者。依預設，會顯示 [一般] 檢視。**

2 **編輯下列欄位：**

名字	此欄位中爲使用者的名字。
姓氏	此欄位採用使用者的姓氏。
全名	此欄位中爲使用者的全名。
密碼	按一下 [編輯] 連結以加入並確認使用者密碼。
電子郵件位址	此欄位中爲使用者的電子郵件位址。
雇員編號	此欄位中爲使用者的員工號碼。
電話號碼	此欄位中爲使用者的電話號碼。
家庭住址	此欄位中爲使用者的家庭住址。
使用者狀態	此選項指出是否允許使用者透過 Access Manager 認證。只有作用中的使用者才可以透過 Access Manager 進行認證。預設值爲作用中。可以從下拉式功能表中選取以下任一選項：。 ■ 作用中 — 使用者可透過 Access Manager 進行認證。

- 非作用中 — 使用者不可透過 Access Manager 進行認證，但目錄中仍會儲存使用者設定檔。

備註 – 將使用者狀態變更爲非作用中僅會影響透過 Access Manager 進行認證的動作。Directory Server 使用 *nsAccountLock* 屬性來決定使用者帳號狀態。針對 Access Manager 認證停用的使用者帳號仍可執行毋須 Access Manager 便可執行的作業。若要使目錄中的使用者帳號成爲非使用中 (不僅僅只針對 Access Manager 認證)，請將 *nsAccountLock* 的值設爲 false。若您網站中經授權的管理員定期會將使用者停用，可考慮將 *nsAccountLock* 屬性加入 Access Manager [使用者設定檔] 頁面。如需詳細資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Developer's Guide」。

帳號過期日期	如果存在該屬性，則當目前日期和時間超過指定的帳號過期日期時，認證服務將不允許登入。此屬性的格式爲 *mm/dd/yyyy hh:mm*。
使用者認證配置	此屬性設定使用者的認證鏈。
使用者別名清單	此欄位定義可以套用於使用者的別名清單。若要使用此屬性中配置的任何別名，必須將 `iplanet-am-user-alias-list` 屬性加入 LDAP 服務的 [使用者項目搜尋屬性] 欄位，來修改 LDAP 服務。
語言環境個人喜好	此欄位指定使用者的語言環境。
成功的 URL	此屬性指定使用者認證成功後將重新導向至的 URL。
失敗的 URL	此屬性指定使用者認證失敗後將重新導向至的 URL。
密碼重設選項	這是用來選取忘記密碼頁面中問題之選項，目的在取得忘記的密碼。
使用者探索資源提供	設定使用者的 [使用者探索] 服務的資源提供。
MSISDN 編號	定義在使用 MSISDN 認證時使用者的 MSISDN 編號。

▼ 新增使用者至角色與群組

1. **按一下 [使用者] 標籤。**
2. **按一下您要修改的使用者名稱。**
3. **選取 [角色] 或 [群組] 標籤。**
4. **選取您希望在其中加入使用者的角色或群組，然後按一下 [新增]。**

5 **按一下 [儲存]。**

備註 – 若要從 [角色] 或 [群組] 移除使用者，請選取角色或群組，然後按一下 [移除]，再按一下 [儲存]。

將使用者加入到策略

Access Manager 物件會透過策略的 subject 定義加入策略。當建立或修改策略時，可以將組織、角色、群組及使用者定義爲策略主旨頁面中的主旨。一旦定義了主旨，策略即會套用於物件。如需更多資訊，請參閱第 132 頁的 「管理策略」。

角色

角色爲類似群組概念的一種 Directory Server 項目機制。群組具有成員；角色也具有成員。角色的成員爲擁有該角色的 LDAP 項目。角色自己的條件已定義爲含屬性的 LDAP 項目，爲項目的識別名稱 (DN) 屬性所辨識。Directory Server 具有數種不同類型的角色，但 Access Manager 只能管理它們的其中之一：受管理角色。

備註 – 其他 Directory Server 角色類型仍可於目錄部署中使用，但無法被 Access Manager 主控台管理。其他 Directory Server 類型則可用於策略的主題定義。如需策略 subjects 的相關詳細資訊，請參閱第 129 頁的 「建立策略」。

使用者可擁有一種或多種角色。例如，可以建立具有階段作業服務屬性和密碼重設服務屬性的承包人角色。新承包人雇員加入公司時，管理員可將該角色指定給他們，而不是在承包人項目中設定各自的屬性。若承包人在工程部門工作，且需要適用於工程員工的服務與存取權，那麼管理員可將承包人指派爲工程角色與承包人角色。

Access Manager 使用角色以套用存取控制指令。首次安裝時，Access Manager 會配置定義管理員權限的存取控制指令 (ACI)。系統會接著在角色 (如組織管理角色和組織 Help Desk 管理角色) 中指定這些 ACI，將這些角色指定給使用者時，會定義使用者的存取權限。

只有在 [管理服務] 中啓用了 [在使用者設定檔頁面上顯示角色] 屬性，使用者才可檢視指定給他們的角色。

備註 – 應使用 Directory Server 將 Access Manager 配置爲可使用 referential integrity 外掛程式。啓用後的參考完整性外掛程式會在刪除或重新命名工作完成後，立即對指定的屬性執行完整性更新。這可確保在整個資料庫中維持相關項目之間的關係。資料庫索引可增強中的搜尋效能。如需有關啓用外掛程式的更多資訊，請參閱「Sun Java System Access Manager 6 2005Q1 Migration Guide」。

角色分兩種類型：

- 靜態 — 若要建立靜態角色，在建立角色階段毋須加入使用者即可。角色建立完成後，便可對其加入特定使用者。這樣可讓您在將使用者加入指定角色時，可進行更多的控制。
- 動態 – 動態角色的建立是透過 LDAP 篩選器的使用完成。建立角色時，所有使用者都會透過篩選器的篩選並指定給角色。篩選器會在項目中尋找任何屬性值對 (例如，`ca=user*`)，並自動指定包含該屬性的使用者給角色。

▼ 建立靜態角色

1 **移至將建立角色的組織**。

2 **按一下 [角色] 標籤**。

配置組織時會建立一組預設角色，它們會顯示於 [角色] 清單中。預設角色爲：

容器說明桌面管理員。容器說明桌面管理員角色對組織單元的所有項目皆有讀取權限，但僅對此容器單元中使用者項目之 `userPassword` 屬性具有寫入權限。

組織說明桌面管理員。組織說明桌面管理員對組織中所有項目皆有讀取權限，對 `userPassword` 屬性則有寫入權限。

備註 – 建立子組織時，請記住管理角色是在子組織中建立的，而不是在父系組織中建立的。

容器管理員。容器管理員角色對 LDAP 組織單元中的所有項目均具有讀取寫入權限。在 Access Manager 中，LDAP 組織單元通常稱爲容器。

組織策略管理員。組織策略管理員具有對所有策略的讀取寫入權限，可以建立、指定、修改和刪除此組織內的所有策略。

使用者管理依預設，新建組織中的任何使用者項目均爲該組織的使用者容器的成員。[使用者管理員] 對組織中的所有使用者項目均具有讀取寫入存取權限。請記住，此角色對包含角色與群組 DN 的屬性「並不」具有讀取寫入權限，因此，它們不能修改角色或群組的屬性，也不能從中移除使用者。

備註 – 可以透過 Access Manager 配置其他容器，使其具有使用者項目、群組項目甚至是其他容器。若要將管理員角色套用於配置組織後建立的容器，將會使用預設的容器管理員角色或容器說明桌面管理員。

群組管理員。建立群組時建立的群組管理員對特定群組的所有成員均具有讀取寫入存取權限，可以建立新的使用者、將使用者指定給其管理的群組以及刪除已建立的使用者。

建立群組時將自動產生群組管理員角色，其具有管理群組的必要權限。不會自動將此角色指定給群組成員。它必須由群組的建立者指定，或由對群組管理員角色有存取權的任何人指定。

頂層管理員。頂層管理員對頂層組織中的所有項目均具有讀取寫入權限。換句話說，此頂層管理員角色具有 Access Manager 應用程式中每個配置主體所擁有的權限。

組織管理員。組織管理員對組織中的所有項目均具有讀取寫入權限。建立群組時將自動產生組織管理員角色，其具有管理組織的必要權限。

3 **按一下 [新建靜態] 按鈕**。

4 **輸入角色的名稱**。

5 **輸入角色的描述**。

6 **從 [類型] 功能表選擇角色類型**。

角色可以爲「管理」角色或「服務」角色。主控台使用角色類型決定在 Access Manager 主控台中啓動使用者的位置。管理角色會通知主控台，該角色的擁有者具有管理權限；服務角色會通知主控台，該擁有者爲一般使用者。

7 **從 [存取權限] 功能表，選擇預設的權限集以套用至該角色。具有這些權限，便可以存取組織中的項目。顯示的預設許可權未依特定順序排列。這些權限為**：

沒有許可權	對角色不設定權限。
組織管理員	組織管理員對配置組織中的所有項目均具有讀取寫入權限。
組織說明桌面管理員	組織說明桌面管理員對已配置組織中所有項目具有讀取權限，並對 `userPassword` 屬性具有寫入權限。
組織策略管理員	組織策略管理員對組織中的所有策略均具有讀取寫入權限。組織策略管理員無法建立同級組織的參考策略。 通常，「無權限 ACI」會指定給「服務」角色，而爲「管理」角色指定任一預設 ACI。

▼ 將使用者加入到靜態角色

1 **按一下要對其加入使用者的角色之名稱**。

2 **在 [成員] 清單中，從 [選取動作] 功能表選取 [加入使用者]**。

3 **輸入搜尋條件的資訊。可以選擇基於一個或多個顯示的欄位搜尋使用者。這些欄位包括**：

符合	可讓您對篩選選取您要包含的欄位。`ALL` 會傳回所有指定欄位的使用者。`ANY` 會傳回任一指定欄位的使用者。
名字	依據其名字搜尋使用者。
使用者 ID	依據使用者 ID 搜尋使用者。
姓氏	依據其姓氏搜尋使用者。

全名　　依據其全名搜尋使用者。

使用者狀態　　依據使用者的狀態 (作用中或非作用中) 搜尋使用者。

4 **按一下 [下一步] 以開始搜尋。會顯示搜尋的結果。**

5 **透過選取使用者名稱旁邊的核取方塊，從傳回的名稱中選擇使用者。**

6 **按一下 [完成]。**
使用者即會指定給角色。

▼ 若要建立動態角色

1 **移至將建立角色的組織。**

2 **按一下 [角色] 標籤。**
配置組織時會建立一組預設角色，它們會顯示於 [角色] 清單中。預設角色爲：

容器說明桌面管理員。容器說明桌面管理員角色對組織單元的所有項目皆有讀取權限，但僅對此容器單元中使用者項目之 `userPassword` 屬性具有寫入權限。

組織說明桌面管理員。組織說明桌面管理員對組織中所有項目皆有讀取權限，對 `userPassword` 屬性則有寫入權限。

備註 – 建立子組織時，請記住管理角色是在子組織中建立的，而不是在父系組織中建立的。

容器管理員。容器管理員角色對 LDAP 組織單元中的所有項目均具有讀取寫入權限。在 Access Manager 中，LDAP 組織單元通常稱爲容器。

組織策略管理員。組織策略管理員具有對所有策略的讀取寫入權限，可以建立、指定、修改和刪除此組織內的所有策略。

使用者管理依預設，新建組織中的任何使用者項目均爲該組織的使用者容器的成員。[使用者管理員] 對組織中的所有使用者項目均具有讀取寫入存取權限。請記住，此角色對包含角色與群組 DN 的屬性「並不」具有讀取寫入權限，因此，它們不能修改角色或群組的屬性，也不能從中移除使用者。

備註 – 可以透過 Access Manager 配置其他容器，使其具有使用者項目、群組項目甚至是其他容器。若要將管理員角色套用於配置組織後建立的容器，將會使用預設的容器管理員角色或容器說明桌面管理員。

群組管理員。建立群組時建立的群組管理員對特定群組的所有成員均具有讀取寫入存取權限，可以建立新的使用者、將使用者指定給其管理的群組以及刪除已建立的使用者。

建立群組時將自動產生群組管理員角色，其具有管理群組的必要權限。不會自動將此角色指定給群組成員。它必須由群組的建立者指定，或由對群組管理員角色有存取權的任何人指定。

頂層管理員。頂層管理員對頂層組織中的所有項目均具有讀取寫入權限。換句話說，此頂層管理員角色具有 Access Manager 應用程式中每個配置主體所擁有的權限。

組織管理員。組織管理員對組織中的所有項目均具有讀取寫入權限。建立群組時將自動產生組織管理員角色，其具有管理組織的必要權限。

3 按一下 [新建動態] 按鈕。

4 輸入角色的名稱。

5 輸入角色的描述。

6 從 [類型] 功能表選擇角色類型。

角色可以爲「管理」角色或「服務」角色。主控台使用角色類型決定在 Access Manager 主控台中啓動使用者的位置。管理角色會通知主控台，該角色的擁有者具有管理權限；服務角色會通知主控台，該擁有者爲一般使用者。

7 從 [存取權限] 功能表，選擇預設的權限集以套用至該角色。具有這些權限，便可以存取組織中的項目。顯示的預設許可權未依特定順序排列。這些權限為：

沒有許可權	對角色不設定權限。
組織管理員	組織管理員對配置組織中的所有項目均具有讀取寫入權限。
組織說明桌面管理員	組織說明桌面管理員對已配置組織中所有項目具有讀取權限，並對 `userPassword` 屬性具有寫入權限。
組織策略管理員	組織策略管理員對組織中的所有策略均具有讀取寫入權限。組織策略管理員無法建立同級組織的參考策略。 通常，「無權限 ACI」會指定給「服務」角色，而爲「管理」角色指定任一預設 ACI。

8 輸入搜尋條件的資訊。這些欄位包括：

符合	允許您在希望篩選所包含的任何欄位中納入運算子。`ALL` 會傳回所有指定欄位的使用者。`ANY` 會傳回任一指定欄位的使用者。
名字	依據其名字搜尋使用者。
使用者 ID	依據使用者 ID 搜尋使用者。
姓氏	依據其姓氏搜尋使用者。
全名	依據其全名搜尋使用者。
使用者狀態	依據使用者的狀態 (作用中或非作用中) 搜尋使用者。

9 **按一下 [確定] 以根據篩選條件開始搜尋。篩選條件所定義的使用者會自動指定給角色。**

▼ 從角色移除使用者

1 **導覽至包含要修改之角色的組織。**
從 [識別管理] 模組的 [檢視] 功能表中選取 [組織]，然後選取 [角色] 標籤。

2 **選取要修改的角色。**

3 **從 [檢視] 功能表選擇 [使用者]。**

4 **選取要移除的每個使用者旁邊的核取方塊。**

5 **按一下 [選取動作] 功能表中的 [移除] 使用者。**
使用者即會從角色中移除。

將角色加入策略

Access Manager 物件會透過策略的 subject 定義加入策略。當建立或修改策略時，可以將組織、角色、群組及使用者定義爲策略主旨頁面中的主旨。一旦定義了主旨，策略即會套用於物件。如需更多資訊，請參閱第 132 頁的 「管理策略」。

◆ ◆ ◆ 第 11 章

11 目前階段作業

本章描述 Access Manager 之階段作業管理功能。階段作業管理模組爲檢視使用者階段作業資訊和管理使用者階段作業提供了解決方案。它追蹤各個階段作業時間並允許管理員終止階段作業。系統管理員應忽視 [平台伺服器] 清單中所列的 [負載平衡器] 伺服器。

目前階段作業介面

[目前階段作業] 模組介面允許具有適當權限的管理員，檢視目前登入至 Access Manager 的任何使用者之階段作業資訊。

階段作業管理

階段作業管理框架顯示目前受管理的 Access Manager 名稱。

階段作業資訊

[階段作業資訊] 視窗顯示目前登入至 Access Manager 的所有使用者，並且顯示每位使用者的階段作業時間。這些顯示欄位包括：

使用者 **ID** 。顯示目前登入使用者的使用者 ID。

剩餘時間 。顯示使用者必須重新認證之前可用的階段作業剩餘時間 (分鐘)。

最長階段作業時間。顯示階段作業過期且必須重新認證之前使用者可登入的最長時間 (分鐘) 。

閒置時間。顯示使用者已閒置的時間 (分鐘)。

最長閒置時間。顯示階段作業必須重新認證之前使用者可閒置的最長時間 (分鐘) 。

時間限制由管理員在階段作業管理服務中定義。

在 [使用者 ID] 欄位中輸入字串，然後按一下 [篩選]，可以顯示某個特定的使用者階段作業或使用者階段作業的特定範圍。允許使用萬用字元。

按一下 [更新] 按鈕，將更新使用者階段作業顯示內容。

終止階段作業

具有適當權限的管理員可以隨時終止使用者階段作業。

▼ 若要終止階段作業

1. **選取您要終止的使用者階段作業。**
2. **按一下 [終止]。**

◆ ◆ ◆ 第 12 章

12 密碼重設服務

Access Manager 提供「密碼重設」服務，可讓使用者重設他們用於存取 Access Manager 所保護的特定服務或應用程式的密碼。「密碼重設」服務屬性由頂層管理員定義，可控制驗證憑證 (以機密提問的形式)、控制新建或現有密碼通知的機制以及設定驗證不正確之使用者的鎖定持續時間。

本章包含下列小節：

註冊密碼重設服務

使用者所屬範圍不需要註冊密碼重設服務。如果使用者所屬組織中不存在密碼重設服務，它將繼承在 [服務配置] 中爲此服務定義的值。

▼ 為不同範圍中的使用者註冊密碼重設

1. **瀏覽至您將為使用者註冊密碼的範圍**。
2. **按一下範圍名稱，然後按一下 [服務] 標籤**。
   若尚未加入範圍，按一下 [新增] 按鈕。
3. **選取 [密碼重設]，然後按一下 [下一步]**。
   將會顯示[密碼重設] 服務屬性。有關屬性定義，請參閱線上說明。
4. **按一下 [完成]**。

配置密碼重設服務

註冊密碼重設服務後，該服務必須由擁有管理員權限的使用者配置。

▼ 若要配置服務

1. **選取要註冊 [密碼重設] 服務的範圍。**
2. **按一下 [服務] 標籤。**
3. **按一下服務清單中的 [密碼重設]。**
4. **會顯示密碼重設屬性，可讓您定義 [密碼重設] 服務的需求。確保已啓用密碼重設服務 (預設為啓用)。至少必須定義以下屬性：**
   - 使用者驗證
     - 機密提問
     - 連結 DN
     - 連結密碼

     [連結 DN] 屬性必須包含擁有重設密碼權限的使用者 (例如說明桌面管理員)。由於 Directory Server 有所限制，因此當連結 DN 爲 `cn=Directory Manager` 時，[密碼重設] 便不起作用。

     其餘屬性均爲選擇性的。如需服務屬性的描述，請參閱線上說明。

     備註 – Access Manager 會自動安裝密碼重設 Web 應用程式，以便產生隨機密碼。但是，您可以寫入自己的外掛程式類別，以產生和通知密碼。請參閱位於以下位置的 Readme.html 檔案，以取得這些外掛程式類別的範例。

     PasswordGenerator:

     ```
     AccessManager-base/SUNWam/samples/console/PasswordGenerator
     ```

     NotifyPassword:

     ```
     AccessManager-base/SUNWam/samples/console/NotifyPassword
     ```

     ---
5. **如果使用者要定義其唯一的個人提問，則選取 [啓用個人提問] 屬性。定義屬性後，按一下 [儲存]。**

密碼重設鎖定

密碼重設服務包含鎖定功能，此功能限制使用者正確回答其機密提問前可以嘗試的次數。鎖定功能透過密碼重設服務屬性來配置。如需服務屬性的描述，請參閱線上說明。密碼重設支援兩種類型的鎖定，記憶體鎖定和實體鎖定。

記憶體鎖定

鎖定是暫時的，只有當 [密碼重設失敗鎖定持續時間] 屬性的值大於 0，且 [啓用密碼重設失敗鎖定] 屬性已啓用時時才有效用。該鎖定將防止使用者透過密碼重設 Web 應用程式重設密碼。此鎖定會持續 [密碼重設失敗鎖定持續時間] 中指定的時間，或直到伺服器重新啓動。如需服務屬性的描述，請參閱線上說明。

實體鎖定

該鎖定爲一種比較永久的鎖定。當 [密碼重設失敗鎖定計數] 屬性的值設爲 0，且 [啓用密碼重設失敗鎖定] 屬性已啓用時，若使用者回答機密提問答案錯誤，其使用者帳號狀態會變更爲非作用中。如需服務屬性的描述，請參閱線上說明。

一般使用者的密碼重設

以下小節描述使用者使用密碼重設服務的情況。

自訂密碼重設

啓用了密碼重設服務且管理員定義了屬性後，使用者即可登入 Access Manager 主控台，以便自訂其機密提問。

▼ 若要自訂密碼重設

1. **在使用者名稱和密碼成功通過認證後，使用者登入主控台。**
2. **在 [使用者設定檔] 頁面中，使用者選取密碼重設選項。系統會顯示 [可用提問回答] 畫面。**
3. **系統會為使用者顯示管理員為服務定義的提問，如：**
   - 您的寵物叫什麼名字？
     - 您最喜愛哪個電視節目？
     - 您母親的婚前姓是什麼？
     - 您最喜歡的飯店是哪家？
4. **使用者可以選取機密提問，最多不超過管理員為範圍定義的最大問題數 (最大問題數在 [密碼重設服務] 中定義)。然後，使用者提供對所選問題的回答。這些問題與回答為重設使用者**

密碼的依據 (請參閱下一小節)。如果管理員選取了 [啓用個人提問] 屬性，系統會提供文字欄位，讓使用者輸入特有的機密提問及其回答。

5 **使用者按一下 [儲存]。**

重設遺忘密碼

如果使用者遺忘密碼，可使用密碼重設網路應用程式隨機產生新密碼，並通知使用者此新密碼。遺忘密碼的典型情形如下：

▼ 重設遺忘密碼

1 **使用者從管理員為他們提供的 URL 登入到密碼重設網路應用程式。例如：**

`http://hostname:port /ampassword` (預設範圍)

或

`http://hostname: port/`*deploy_uri* `/UI/PWResetUserValidation?realm=realmname`，其中 realmname 是範圍的名稱。

備註 – 若父系範圍的 [密碼重設] 服務沒有啓用，但其子範圍的啓用了，使用者必須使用以下語法存取服務：

`http://hostname: port/`*deploy_uri*`/UI/PWResetUserValidation?realm=realmname`

---

2 **使用者輸入使用者 ID。**

3 **系統向使用者顯示在密碼重設服務中定義且在自訂期間被使用者選取的個人提問。如果使用者先前未登入 [使用者設定檔] 頁面且未自訂個人提問，則不會產生密碼。**

使用者正確回答提問後，系統會產生新密碼並使用電子郵件將其傳送給該使用者。無論使用者是否正確回答了提問，系統均會將嘗試通知傳送給該使用者。爲了接收新密碼和嘗試通知，使用者必須在 [使用者設定檔] 頁面中輸入自己的電子郵件位址。

密碼策略

透過強制以下作業，安全密碼策略可以將密碼被容易猜出的風險降到最低：

- 使用者必須依據排程變更密碼。
- 使用者必須提供比較特殊的密碼。
- 數次輸入錯誤密碼後，系統可能會鎖定帳戶。

Directory Server 提供在樹的任一節點設定密碼策略的多種方法，而且存在多種設定策略的方法。如需詳細資訊，請參閱以下 Directory Server 文件：

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6698-10/useracct.html#14386

◆ ◆ ◆ 第 13 章

13 記錄服務

Sun Java™ System Access Manager 7 2005Q4 提供記錄服務，以記錄如使用者作業、流量模式和授權違規等資訊。此外，除錯檔案可幫助管理員排解安裝的疑難。

記錄檔

記錄檔記錄其監視的每個服務的許多事件。管理員應定期查看這些檔案。記錄檔的預設目錄是 `/var/opt/SUNWam/logs` (SPARC 系統) 和 `/var/opt/sun/identity` (Linux 系統)。藉由使用 Access Manager 主控台，可在 [記錄服務] 中配置記錄檔目錄。

有關預設記錄檔類型、記錄何種資訊以及記錄檔格式之詳細清單的資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Technical Overview」中的「How the Logging Feature Works」。

有關 [記錄服務] 的屬性定義，請按一下 Access Manager 主控台中的 [說明] 按鈕以查閱線上說明。

Access Manager 服務記錄

服務記錄檔有兩種類型：存取和錯誤。「存取」記錄檔包含嘗試登入與成功登入的記錄。「錯誤」記錄檔記錄 Access Manager 服務中的錯誤。平面記錄檔附加的副檔名爲 `.error` 或 `.access`。資料庫欄位的名稱是以 `_ERROR` 或 `_ACCESS` 結束 (Oracle 資料庫)，或以 `_error` 或 `_access` 結束 (MySQL 資料庫)。例如，平面檔案記錄主控台事件名爲 `amConsole.access`，而記錄同一事件的資料庫欄位名爲 `AMCONSOLE_ACCESS`。以下各節說明記錄服務所記錄的記錄檔。

階段作業記錄檔

[記錄服務] 記錄以下階段作業服務事件：

- 登入

- 登出
- 階段作業閒置逾時
- 階段作業最長逾時
- 登入失敗
- 階段作業重新啓動
- 階段作業銷毀

階段作業記錄檔的前綴是 amSSO。

主控台記錄檔

Access Manager 主控台記錄檔記錄識別相關物件、策略和服務的建立、刪除與修改，其中包括組織、組織單位、使用者、角色、策略和群組。它也記錄使用者屬性的修改，包括密碼以及新增或移除角色和群組中的使用者。此外，主控台記錄檔也寫入委託和資料存放區作業。主控台記錄檔的前綴是 amConsole。

認證記錄檔

認證元件記錄使用者的登入和登出。認證記錄檔的前綴是 amAuthentication。

聯合記錄檔

「聯合」元件記錄聯合相關事件，例如 (但不限於) 建立「認證網域」和建立「寄存提供者」。聯合記錄檔的前綴是 amFederation。

策略記錄檔

策略元件記錄策略相關事件，包括 (但不限於) 策略管理 (策略的建立、刪除和修改) 和策略評估。策略記錄檔的前綴是 amPolicy。

代理程式記錄檔

策略代理程式記錄檔負責記錄有關允許或拒絕使用者存取之記錄資源的異常。代理程式記錄檔的前綴是 amAgent。amAgent 記錄檔只存在於代理程式伺服器中。在 Access Manager 伺服器上於「認證記錄檔」中記錄代理程式事件。如需有關此功能的更多資訊，請參閱有疑問的策略代理程式的相關文件。

SAML 記錄檔

SAML 元件記錄 SAML 相關事件，包括 (但不限於) 指定和工件的建立或移除、回應和請求的詳細資訊以及 SOAP 錯誤。階段作業記錄檔的前綴是 amSAML。

amAdmin 記錄檔

指令行記錄檔記錄使用指令行工具的作業中發生的事件錯誤。包括 (但不限於) 載入服務模式、建立策略和刪除使用者。指令行記錄檔的前綴是 amAdmin。

記錄功能

[記錄服務] 有數個特定功能，可加以啓用以執行額外的功能。包括啓用「安全記錄」、「指令行記錄」和「遠端記錄」。

安全記錄

此選擇性的功能可將額外安全性加入記錄功能中。啓用「安全記錄」後，可以偵測對安全記錄進行的未授權變更或竄改。使用此功能不需用特殊編碼。「安全記錄」是藉由使用由系統管理員配置的預先註冊憑證來達成。會爲每個記錄檔記錄產生和儲存此「清單分析和憑證 (MAC)」。會定期插入特定「簽名」記錄檔記錄，表示寫入該點之記錄內容的簽名。兩種記錄的組合可確保記錄沒有被竄改。

▼ 啓用安全記錄

1. **以 Logger 名稱建立憑證，然後將其安裝在執行 Access Manager 的部署容器中。詳細資訊請參閱部署容器的文件。**

2. **在 Access Manager 主控台中，開啓 [記錄服務] 配置中的 [安全記錄]，並儲存此變更。管理員亦可修改 [記錄服務] 中其他屬性的預設值。**

   若記錄目錄預設值 (/var/opt/SUMWam/logs) 有所變更，請確定將其權限設爲 0700。若此目錄不存在，記錄服務會建立此目錄，但它會建立權限設爲 0755 的目錄。

   此外，若您指定和預設不同的目錄，必須變更以下參數至新目錄中 Web 容器的 server.policy 檔：

   ```
   permission java.io.FilePermission “/var/opt/SUNWam/logs/*”,”delete,write”
   ```

3. **在包含憑證資料庫密碼的 *AccessManager-base*/SUNWam/config 目錄中建立檔案，並將之命名為 .wtpass。**

備註 – 其檔名和路徑可在 AMConfig.properties 檔中配置。如需更多資訊，請參閱附錄 A中的「憑證資料庫」。

請確定部署容器使用者爲因安全性理由對此檔案有讀取權限的管理員。

---

4 **重新啓動伺服器**。

應清除安全記錄目錄，因爲當啓動安全記錄時，部份易引起誤解的驗證錯誤可能會被寫入 `/var/opt/SUNWam/debug/amLog` 檔案。

若要偵測安全記錄中有無未認證的變更或竄改， 請查看驗證程序寫入 `/var/opt/SUNWam/debug/amLog` 的錯誤訊息。若要手動檢查竄改，請執行 `VerifyArchive` 公用程式。如需更多資訊，請參閱第 19 章。

指令行記錄

`amadmin` 指令行工具可建立、修改和刪除 Directory Server 中的識別物件 (例如組織、使用者、角色)。此工具也可載入、建立和註冊服務範本。[記錄服務] 可啓用 `-t` 選項來記錄這些動作。若啓用 (ACTIVE) `AMConfig.properties` 中的 `com.iplanet.am.logstatus` 特性，則會建立記錄檔記錄。(依預設會啓用此特性。)指令行記錄檔的前綴是 `amAdmin`。如需更多資訊，請參閱第 14 章。

記錄特性

`AMConfig.properties` 檔中有一些特性會影響記錄的輸出：

`com.iplanet.am.logstatus=ACTIVE`	此特性可啓用或停用記錄。預設爲 ACTIVE。
`iplanet-am-logging.`*service*`.level=` *level*	*service* 爲服務的正常除錯檔檔名。*level* 爲 `java.util.logging.Level` 值的其中一個，表示記錄於記錄檔中之詳細資訊的等級。等級可爲 SEVERE、WARNING、INFO、CONFIG、FINE、FINER 和 FINEST。大多數服務所記錄的詳細資訊不會高於 INFO 記錄等級。

遠端記錄

Access Manager 支援遠端記錄。使用安裝 Access Manager SDK 之主機的用戶端應用程式可在部署於遠端機器上的 Access Manager 實例上建立記錄檔記錄。遠端記錄可在以下情況下被啓動：

1. 當 Access Manager 實例的 [記錄服務] 中的記錄 URL 指向遠端實例，且二者之間配置爲信任關係，記錄將寫入遠端 Access Manager 實例。
2. 當 Access Manager SDK 是針對遠端 Access Manager 實例而安裝，且在 SDK 伺服器上執行的用戶端 (或簡單 Java 類別) 使用記錄 API，記錄將寫入遠端 Access Manager 機器。
3. 當記錄 API 是由 Access Manager 代理程式所使用。

▼ 啓用遠端記錄

1 若使用 Sun Java System Web Server，`server.xml` 配置檔中需設定以下環境變數：

- `java.util.logging.manager=com.sun.identity.log.LogManager`
- `java.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties`
- 若使用的 Java™ 2 Platform, Standard Edition 爲 1.4 或更高版本，在指令行中執行以下指令將完成此步驟：

  `java -cp /`*AccessManager-base*`/SUNWam/lib/am_logging.jar:/` *AccessManager-base* `/SUNWam/lib/xercesImpl.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/jaas.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/servlet.jar:/` *AccessManager-base* `/SUNWam/locale:/` *AccessManager-base*`/SUNWam/lib/am_services.jar:/` *AccessManager-base*`/SUNWam/lib/am_sdk.jar:/` *AccessManager-base*`/SUNWam/lib/jss311.jar:/` *AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`
- 若使用的 Java 2 Platform, Standard Edition 版本低於 1.4，在指令行中執行以下指令將完成此步驟：

  `java -Xbootclasspath/a:/`*AccessManager-base* `/SUNWam/lib/jdk_logging.jar -cp /` *AccessManager-base* `/SUNWam/lib/am_logging.jar:/` *AccessManager-base* `/SUNWam/lib/xercesImpl.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/jaas.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/servlet.jar:/` *AccessManager-base* `/SUNWam/locale:/` *AccessManager-base*`/SUNWam/lib/am_services.jar:/` *AccessManager-base*`/SUNWam/lib/am_sdk.jar:/` *AccessManager-base*`/SUNWam/lib/jss311.jar:/` *AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`

2 請確定位於 *AccessManager-base*`/SUNWam/lib` 的 `LogConfig.properties` 中有配置以下參數：

- `iplanet-am-logging-remote-handler=com.sun.identity`。

  `log.handlers.RemoteHandler`
- `iplanet-am-logging-remote-formatter=com.sun`。

  `identity.log.handlers.RemoteFormatter`

- `iplanet-am-logging-remote-buffer-size=1`

  遠端記錄支援緩衝，以記錄檔記錄的數目爲基準。此值定義了記錄緩衝區大小，以記錄的數目爲單位。一旦緩衝區空間已滿，所有在緩衝區中的記錄都會被清空至伺服器。

- `iplanet-am-logging-buffer-time-in-seconds=3600`

  此值定義要呼叫緩衝區清除器執行緒的逾時期間。

- `iplanet-am-logging-time-buffering-status=OFF`

  此值定義是否要啓用記錄緩衝 (和緩衝區清除器執行緒)。依預設此功能爲關閉。

備註 – 每當記錄檔是空白時，安全記錄可能會顯示「驗證失敗」。這是因爲當已建立檔案的數目與歸檔檔案大小相等時，安全記錄會將其歸檔並重新開始。於大部分的實例中，您可忽略此錯誤。一旦記錄的數目與歸檔檔案大小相等時，將不會顯示錯誤。

錯誤和存取記錄檔

存在兩種 Access Manager 記錄檔類型：存取記錄檔和錯誤記錄檔。

存取記錄檔記錄有關 Access Manager 部署的一般稽核資訊。記錄檔可能包含一個事件的單一記錄，例如一次成功的認證。記錄檔可能包含相同事件的多個記錄。例如，當管理員使用主控台變更屬性值時，「記錄服務」在一個記錄中記錄變更嘗試。「記錄服務」同時也會在第二個記錄中記錄執行結果。

錯誤記錄檔記錄發生於應用程式中的錯誤。當錯誤記錄檔中記錄了作業錯誤時，作業嘗試會記錄於存取記錄檔中。

平面記錄檔會附加副檔名 `.error` 或 `.access`。資料庫的欄名稱則以 `_ERROR` 或 `_ACCESS` 結束。例如，記錄主控台事件的平面檔案命名爲 `amConsole.access`，記錄相同事件的資料庫欄命名爲 `AMCONSOLE_ACCESS` 或 `amConsole_access`。

下表提供每個 Access Manager 元件所產生之記錄檔的簡要描述。

表 13–1 Access Manager 元件記錄檔

元件	記錄檔名稱前綴	記錄的資訊
階段作業	`amSSO`	階段作業管理屬性值，如登入時間、登出時間、逾時限制。
管理主控台	`amConsole`	經由管理主控台執行的使用者動作，如識別相關之物件、範圍，及策略的建立、刪除與修改。
認證	`amAuthentication`	使用者登入和登出。

表 13–1 Access Manager 元件記錄檔 (續)

元件	記錄檔名稱前綴	記錄的資訊
識別聯合	amFederation	聯合相關事件，如「認證網域」的建立和「寄存提供者」的建立。聯合記錄檔的前綴是 amFederation。
授權 (策略)	amPolicy	策略相關事件，如策略建立、刪除或修改以及策略評估。
策略代理程式	amAgent	有關爲使用者存取或拒絕使用者存取之資源的異常。amAgent 記錄檔位於安裝策略代理程式的伺服器上。在 Access Manager 主機上於「認證記錄檔」中記錄代理程式事件。
SAML	amSAML	SAML 相關事件，如指定和工件的建立或移除、回應和請求的詳細資訊以及 SOAP 錯誤。
指令行	amAdmin	使用指令行工具的作業中發生的事件錯誤。範例爲：載入服務模式、建立策略和刪除使用者。

如需 Access Manager 記錄檔清單與描述，請參閱附錄 C。

除錯檔

除錯檔並非 [記錄服務] 的功能。它們是使用獨立於記錄 API 的其他 API 寫入。除錯檔儲存在 /var/opt/SUNWam/debug。此位置 (以及除錯資訊的等級) 可在 AMConfig.properties 檔中配置，此檔位於 *AccessManager-base*/SUNWam/lib/ 目錄中。如需更多有關除錯特性的資訊，請參閱附錄 A。

除錯等級

除錯檔可記錄的資訊分爲幾個等級。除錯等級是以 AMConfig.properties 的 com.iplanet.services.debug.level 特性設定。

1. Off— 不記錄除錯資訊。
2. Error— 此等級用於生產。生產時，除錯檔中應無錯誤。
3. Warning— 目前並不建議使用此等級。
4. Message— 此等級利用代碼追蹤對可能的問題發出警示。大多數 Access Manager 模組使用此等級傳送除錯訊息。

備註 – [Warning] 與 [Message] 等級不可用於生產中。這樣會嚴重降低效能並產生大量的除錯訊息。

除錯輸出檔

除非模組寫入除錯檔，否則不會建立除錯檔。因此，在預設**錯誤**模式下不會產生除錯檔。登入時若除錯等級設爲**訊息**，則建立的除錯檔包括：

- amAuth
- amAuthConfig
- amAuthContextLocal
- amAuthLDAP
- amCallback
- amClientDetection
- amConsole
- amFileLookup
- amJSS
- amLog
- amLoginModule
- amLoginViewBean
- amNaming
- amProfile
- amSDK
- amSSOProvider
- amSessionEncodeURL
- amThreadManager

最常使用的檔案是 `amSDK`、`amProfile` 和所有適用於認證的檔案。所擷取的資訊包括日期、時間和訊息類型 ([錯誤]、[警告]、[訊息])。

使用除錯檔

依預設，除錯等級設爲**錯誤**。當管理員要進行下列作業時，除錯檔十分有用：

- 寫入自訂認證模組。
- 使用 Access Manager SDK 寫入自訂應用程式。`amProfile` 和 `amSDK` 除錯檔會擷取此資訊。
- 使用主控台或 SDK 對存取權限進行疑難排解。`amProfile` 與 `amSDK` 除錯檔也會擷取此資訊。
- 疑難排解 SSL。
- 疑難排解 LDAP 認證模組。`amAuthLDAP` 除錯檔會擷取此資訊。

應將我們以後可能會收到的疑難排解指南與除錯檔配合使用。例如，當 SSL 失敗時，某些人可能會開啓除錯訊息並尋找 `amJSS` 除錯檔中的任何特定憑證錯誤。

多重 Access Manager 實例和除錯檔

Access Manager 包含 `ammultiserverinstall` 程序檔，可用於配置數個伺服器實例。若多重伺服器實例配置爲使用不同除錯目錄，則各個實例都必須有讀取和寫入除錯目錄的權限。

第 IV 部分

指令行參照

這是「指令行參照」，「Sun Java System Access Manager 7 2005Q4 管理指南」的第四部分。

描述於本部分的所有指令行工具皆可於下列預設位置中取得：

```
AccessManager-base/SUNWam/bin (Solairs)

AccessManager-base/identity/bin (Linux)
```

本部分包含以下章節：

◆ ◆ ◆ 第 14 章

amadmin 指令行工具

本章提供 amadmin 指令行工具的資訊。

amadmin 指令行工具可執行檔

指令行工具可執行檔 amadmin 的主要用途是將 XML 服務檔載入資料存放區，以及在 DIT 上執行批次管理作業。您可在 AccessManager-base/SUNWam/bin 中找到 amadmin，並用於：

- 載入 XML 服務檔案 - 管理員將使用 XML 服務檔案格式 (在 sms.dtd 中定義) 的服務載入 Access Manager 中。必須使用 amadmin 載入所有服務；不能透過 Access Manager 主控台匯入這些服務。

備註 – XML 服務檔案以 XML 資料之靜態 *blobs* 格式儲存於資料存放區中，可爲 Access Manager 所參照。Directory Server 僅能夠識別 LDAP，並不使用該資訊。

- 對 DIT 執行識別物件的批次更新 - 管理員可使用 amadmin.dtd 中定義的批次處理 XML 檔案格式對 Directory Server DIT 執行批次更新。例如，如果管理員希望建立 10 個組織、1000 個使用者和 100 個群組，可以將這些請求放在一個或多個批次處理 XML 檔案中，然後使用 amadmin 載入這些檔案，從而一次達到上述目的。

備註 – amadmin 僅支援 Access Manager 主控台支援的部分功能，並不能取代主控台。建議將主控台用於小型管理工作，而將 amadmin 用於較大型的管理工作。

---

amadmin 語法

要使用 amadmin，必須遵循許多結構上的規則。使用該工具的一般語法如下：

- amadmin -u | --runasdn *dnname* -w | --password *password* [-l | --locale *localename*] [[-v | --verbose] | [-d |--debug]] -t | --data *xmlfile1* [*xmlfile2* ...]

- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -s | --schema` *xmlfile1* `[`*xmlfile2* `...]`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -r | --deleteService` *serviceName1* `[`*serviceName2* `...]`
- amadmin -u | --runasdn *dnname* -w | --password *password* or -f | --password file *passwordfile* [-c | --continue] [-l | --locale *localename*] [[-v | --verbose] | [-d | --debug]] -m | --session *servername pattern*
- `amadmin -h | --help`
- `amadmin -n | --version`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `or - f |--passwordfile` *passwordfile* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d] |--debug]] -a |--addAttributes` *serviceName schemaType xmlfile*`[`*xmlfile2* `] ...`

備註 – 必須如語法中所示，準確輸入兩個連字符號。

amadmin 選項

以下是 `amadmin` 指令行參數選項的定義：

--runasdn (-u)

`--runasdn` 用於爲 LDAP 伺服器認證使用者。此引數的值等於經授權執行 `amadmin` 的使用者之識別名稱 (DN)；例如

`--runasdn uid=amAdmin,ou=People,o=iplanet.com,o=isp`。

DN 亦可透過在網域之間插入空格並爲整個 DN 加上雙引號來進行格式化，例如：`--runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp"`。

--password (-w)

`--password` 是強制性選項，其值等於使用 `--runasdn` 選項指定的 DN 之密碼。

--locale (-l)

`--locale` 是值等於語言環境名稱的選項。此選項可用於自訂訊息語言。如果沒有提供語言環境，系統會使用預設語言環境 `en_US`。

--continue (-c)

--continue 是在即使出現錯誤的情況下仍將繼續處理 XML 檔案的選項。例如，如果要同時載入三個 XML 檔案，並且載入第一個 XML 檔案失敗，而 `amadmin` 將繼續載入其餘檔案。continue 選項只能套用到個別請求。

--session (-m)

--session (-m) 是管理階段作業或顯示目前階段作業的選項。指定的 --runasdn 必須與 AMConfig.properties 中超級使用者的 DN 相同，或者就是頂層管理員使用者的 ID。

以下範例將顯示特定服務主機名稱的所有階段作業：

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com
-v  -w 12345678 -m http://sun.com:58080
```

以下範例將顯示特定使用者的階段作業：

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v
 -w 12345678 -m http://sun.com:58080 username
```

您可以輸入索引編號來終止相應的階段作業，還可以輸入多重索引編號 (以空格分隔) 來終止相應的多重階段作業。

使用以下選項時：

amadmin -m | --session servername pattern

pattern 可以是萬用字元 (*)。如果此式樣使用萬用字元 (*)，則必須使用圖元字元 (\\) 使其從 shell 退出。

--debug (-d)

--debug 是將訊息寫入 amAdmin 檔案 (於 /var/opt/SUNWam/debug 目錄之下建立) 的選項。這些訊息是技術方面的詳細說明，但不符合 i18n 標準。若要產生 amadmin 作業記錄，將資料庫驅動程式的類別路徑記錄到資料庫中時，需要將其手動加入。例如，在記錄到 amadmin 中的 mysql 時，可加入以下各行：

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar
export CLASSPATH
```

--verbose (-v)

--verbose 是將 amadmin 指令的總體進度列印到螢幕上的選項。它不會將詳細資訊列印到檔案中。輸出到指令行的訊息符合 i18n 標準。

--data (-t)

--data 是以要匯入的批次處理 XML 檔案之名稱作爲值的選項。可以指定一個或多個 XML 檔案。這種 XML 檔案可以建立、刪除和讀取各種目錄物件，還可以註冊和取消註冊服務。

--schema (-s)

--schema 是將 Access Manager 服務的屬性載入 Directory Server 的選項。它以定義服務屬性的 XML 服務檔案作爲引數。此種 XML 服務檔以 sms.dtd 爲基礎。可以指定一個或多個 XML 檔案。

備註 – 必須指定 `--data` 或 `--schema` 選項，具體情況取決於是對 DIT 配置批次更新，還是載入服務模式和配置資料。

--deleteservice (-r)

`--deleteservice` 是用於僅刪除服務及其模式的選項。

--serviceName

`--serviceName` 是值等於在 XML 服務檔案的 `Service name=...` 標籤下定義的服務名稱的選項。這部分會顯示在第 186 頁的 「--serviceName」 中。

範例 14–1 `sampleMailService.xml` 的部分

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

`--help` 是顯示 `amadmin` 指令語法的引數。

--version (-n)

`--version` 是顯示公用程式名稱、產品名稱、產品版本和法律聲明的引數。

在聯合管理中使用 amadmin

這個部份列出用於聯合管理的 amadmin 參數。如需有關聯合管理的更多資訊，請參閱「Access Manager Federation Management Guide」。

載入自由中繼相容 XML 到 Directory Server

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-g|--import <xmlfile>
```

--runasdn (-u)

使用者的 DN

--password (-w)

使用者的密碼。

--passwordfile (-f)

包含使用者密碼的檔案名稱。

--entityname (-e)

實體名稱。例如，`http://www.example.com`。實體必須只屬於一個組織。

--import (-g)

包含中介資料資訊的 XML 檔案名稱。這個檔案必須附屬在 Liberty 中介資料規格以及 XSD 中。

匯出一個實體到 XML 檔 (無 XML 數位登入)

amadmin -u|--runasdn <user's DN>

```
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-o|--export <filename>
```

--runasdn (-u)

使用者的 DN

--password (-w)

使用者的密碼。

--passwordfile (-f)

包含使用者密碼的檔案名稱。

--entityname (--e)

位於 Directory Server 中的實體名稱

--export (-o)

包含實體 XML 的檔案名稱。XML 必須符合 Liberty 中介資料 XSD。

匯出一個實體到 XML 檔 (含 XML 數位登入)

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-q|--exportwithsig <filename>
```

--runasdn (-u)

使用者的 DN

--password (-w)

使用者的密碼。

--passwordfile (-f)

包含使用者密碼的檔案名稱。

--entityname (--e)

位於 Directory Server 中的實體名稱

--exportwithsig (-o)

包含實體 XML 的檔案名稱。已經數位簽名這個檔案。XML 必須符合 Liberty 中介資料 XSD。

在資源套件中使用 amadmin

下列部分顯示新增、尋找和刪除資源套件的 `amadmin` 語法。

新增資訊套件。

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-b|--addresourcebundle <name-of-resource-bundle>

-i|--resourcebundlefilename <resource-bundle-file-name>

[-R|--resourcelocale] <locale>
```

取得資源字串。

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-z|--getresourcestrings <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

刪除資訊套件。

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-j|--deleteresourcebundle <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

◆ ◆ ◆ 第 15 章

15 ampassword 指令行工具

本章提供有關 amPassword 指令行工具的資訊，包含以下小節：

ampassword 指令行可執行檔

在 SPARC 系統上，Access Manager 的 ampassword 公用程式位於 /opt/SUNWam/bin，在 Linux 系統上位於 /opt/sun/Identity/bin。該公用程式可讓您變更管理員或使用者的 Directory Server 密碼。

▼ 在 SSL 模式中使用 Access Manager 執行 ampassword

1. **修改位於以下目錄中的 serverconfig.xml 檔案：**

   AccessManager-base/SUNWam/config/

2. **將伺服器屬性 port 變更為 Access Manager 正在執行的 SSL 連接埠。**

3. **將屬性 type 變更為 SSL。**

   例如：

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="sun.com" port="636" type="SSL" />
    <User name="User1" type="proxy">
        <DirDN>
                 cn=puser,ou=DSAME Users,dc=iplanet,dc=com
        </DirDN>
        <DirPassword>
                  AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
         </DirPassword>
```

```
</User> ...
```

ampassword 僅變更 Directory Server 中的密碼。您必須手動變更 ServerConfig.xml 及 Access Manager 的所有認證範本中的密碼。

◆ ◆ ◆ 第 16 章

bak2am 指令行工具

本章提供有關 bak2am 指令行工具的資訊，包含以下小節：

bak2am 指令行可執行檔

Access Manager 在 AccessManager-base/SUNWam/bin 下包含一個 bak2am 公用程式。該公用程式可復原透過 am2bak 公用程式備份的 Access Manager 元件。

bak2am 語法

對於 Solaris 作業系統，使用 bak2am 工具的一般語法如下：

```
./bak2am [ -v | --verbose ] -z | --gzip tar.gz-file
./bak2am [ -v | --verbose ] -t | --tar tar-file
./bak2am -h | --help
./bak2am -n | --version
```

對於 Windows 2000 作業系統，使用 bak2am 工具的一般語法如下：

```
bak2am [ -v | --verbose ] -d | --directory directory-name

bak2am -h | --help
bak2am -n | --version
```

備註 – 必須如語法中所示，準確輸入兩個連字符號。

bak2am 選項

--gzip *backup-name*

`--gzip` 指定 `tar.gz` 格式的備份檔案之完整路徑和檔案名稱。依預設，路徑爲 `AccessManager-base/backup`。此選項僅適用於 Solaris。

--tar *backup-name*

`--tar` 指定 `tar` 格式的備份檔案之完整路徑和檔案名稱。依預設，路徑爲 `AccessManager-base/backup`。此選項僅適用於 Solaris。

--verbose

`--verbose` 用來以詳細模式執行備份公用程式。

--directory

`--directory` 指定備份目錄。依預設，路徑爲 `AccessManager-base/backup`。此選項僅適用於 Windows 2000。

--help

`--help` 是顯示 `bak2am` 指令語法的引數。

--version

`--version` 是顯示公用程式名稱、產品名稱、產品版本和法律聲明的引數。

◆ ◆ ◆ 第 17 章

17 am2bak 指令行工具

本章提供有關 am2bak 指令行工具的資訊。

am2bak 指令行可執行檔

Access Manager 在 AccessManager-base/SUNWam/bin 下包含一個 am2bak 公用程式。該公用程式可執行 Access Manager 全部或可選元件的備份。進行記錄備份時必須執行 Directory Server。

am2bak 語法

對於 Solaris 作業系統，使用 am2bak 工具的一般語法如下：

```
./am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ] [
[-c | --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

./am2bak -h | --help

./am2bak -n | --version
```

對於 Windows 2000 作業系統，使用 am2bak 工具的一般語法如下：

```
am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ] [[-c
| --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

am2bak -h | --help

am2bak -n | --version
```

備註 – 必須如語法中所示，準確輸入兩個連字符號。

am2bak 選項

--verbose (-v)

`--verbose` 用來以詳細模式執行備份公用程式。

--backup *backup-name (-k)*

`--backup` *backup-name* 定義備份檔案的名稱。預設爲 `ambak`。

--location (-l)

`--location` 指定備份的目錄位置。預設位置是 `AccessManager-base/backup`。

--config (-c)

`--config` 指定備份僅用於配置檔案。

--debug (-b)

`--debug` 指定備份僅用於除錯檔案。

--log (-g)

`--log` 指定備份僅用於記錄檔。

--cert (-t)

`--cert` 指定備份僅用於憑證資料庫檔案。

--ds (-d)

`--ds` 指定備份僅用於 Directory Server。

--all (-a)

`--all` 指定整個 Access Manager 的完整備份。

--help (-h)

`--help` 是顯示 `am2bak` 指令語法的引數。

--version (-n)

`--version` 是顯示公用程式名稱、產品名稱、產品版本和法律聲明的引數。

▼ 執行備份程序

1 **以超級使用者的身份登入。**
執行該程序檔的使用者必須具有超級使用者存取權限。

2 **如有必要，請執行該程序檔以確保使用的路徑正確。**
該程序檔將備份以下 Solaris™ 作業環境檔案：

- 配置檔案和自訂檔案：
  - `AccessManager-base/SUNWam/config/`
    - `AccessManager-base/SUNWam/locale/`
    - `AccessManager-base/SUNWam/servers/httpacl`
    - `AccessManager-base/SUNWam/lib/*.properties` (Java 特性檔)
    - `AccessManager-base/SUNWam/bin/amserver.` *instance-name*
    - `AccessManager-base/SUNWam/servers/https-` *all_instances*
    - `AccessManager-base/SUNWam/servers/web-apps-` *all_instances*
    - `AccessManager-base/SUNWam/web-apps/services/WEB-INF/config`
    - `AccessManager-base/SUNWam/web-apps/services/config`
    - `AccessManager-base/SUNWam/web-apps/applications/WEB-INF/classes`
    - `AccessManager-base/SUNWam/web-apps/applications/console`
    - `/etc/rc3.d/K55amserver.`*all_instances*
    - `/etc/rc3.d/S55amserver.`*all_instances*
    - `DirectoryServer-base/slapd-` *host* `/config/schema/`
    - `DirectoryServer-base/slapd-` *host* `/config/slapd-collations.conf`
    - `Access Manager/slapd-` *host* `/config/dse.ldif`

  記錄檔和除錯檔：

  - `var/opt/SUNWam/logs` (Access Manager 記錄檔)
  - `var/opt/SUNWam/install` (Access Manager 安裝記錄檔)
  - `var/opt/SUNWam/debug` (Access Manager 除錯檔)

  憑證：

  - `Access Manager/SUNWam/servers/alias`
  - `Access Manager/alias`

    該程序檔還備份以下 Microsoft® Windows 2000 作業系統檔案：

  配置檔案和自訂檔案：

  - `AccessManager-base/web-apps/services/WEB-INF/config/*`
  - `AccessManager-base/locale/*`

- AccessManager-base/web-apps/applications/WEB-INF/classes/*.properties (java 特性檔)
- AccessManager-base/servers/https- *host*/config/jvm12.conf
- AccessManager-base/servers/https- *host*/config/magnus.conf
- AccessManager-base/servers/https- *host*/config/obj.conf
- DirectoryServer-base/slapd-host/config/schema/*.ldif
- DirectoryServer-base/slapd-host/config/slapd-collations.conf
- DirectoryServer-base/slapd-host/config/dse.ldif

記錄檔和除錯檔：

- var/opt/logs (Access Manager 記錄檔)
- var/opt/debug (Access Manager 除錯檔)

憑證：

- AccessManager-base/servers/alias
- AccessManager/alias

◆ ◆ ◆ 第 18 章

18 amserver 指令行工具

本章提供有關 amserver 指令行工具的資訊。本章包含以下小節：

amserver 指令行可執行檔

amserver 指令行可執行檔可分別啓動和停止與 Unix 和 SecurID 認證模組關聯的 amunixd 及 amsercuridd 輔助程式。

amserver 語法

此工具的一般語法如下：

```
./amserver { start | stop }
```

start

start 是啓動輔助程式的指令。

stop

stop 是停止輔助程式的指令。

◆ ◆ ◆ 第 19 章

19 VerifyArchive 指令行工具

本章提供有關 VerifyArchive 指令行工具的相關資訊，包含以下小節：

VerifyArchive 指令行可執行檔

VerifyArchive 的用途是驗證記錄歸檔檔案。記錄歸檔檔案是一組標記了時間的記錄及其相應的鍵值儲存區 (鍵值儲存區包含用於產生和數位簽名用於偵測記錄檔竄改的鍵值)。歸檔檔案的驗證會偵測對歸檔檔案中任何檔案可能的竄改和/或刪除。

VerifyArchive 擷取給定 logName 的所有歸檔檔案集以及屬於每個歸檔檔案集的所有檔案。執行時，VerifyArchive 會搜尋每個記錄檔記錄，尋找竄改。如果偵測到竄改，會列印一個訊息，指出被竄改的檔案和記錄編號。

VerifyArchive 還檢查已從歸檔檔案集中刪除的所有檔案。如果偵測到已刪除的檔案，會列印訊息，說明驗證失敗。如果未偵測到被竄改或刪除的檔案，則會傳回訊息，說明歸檔檔案驗證已成功完成。

備註 – 若您以不具管理員權限的使用者身份執行 amverifyarchive，可能發生錯誤。

VerifyArchive 語法

需要所有的參數選項。語法如下所示：

```
amverifyarchive -l logName -p path -u
uname -w password
```

選項

logName

logName 指要驗證的記錄檔之名稱 (如 amConsole、amAuthentication 等等)。VerifyArchive 會驗證給定 logName 的存取權限與錯誤記錄檔。例如，如果指定 amConsole，檢驗器會驗證 amConsole.access 與 amConsole.error 檔案。或者，可將 logName 指定爲 amConsole.access 或 amConsole.error，只對那些記錄檔進行驗證。

path

path 是儲存記錄檔案的完整目錄路徑。

uname

uname 是 Access Manager 管理員的使用者 ID。

password

password 是 Access Manager 管理員的密碼。

◆ ◆ ◆ 第 20 章

20 amsecuridd 輔助程式

本章提供有關 amsecuiridd 輔助程式的資訊，包含以下小節：

amsecuridd 輔助程式指令行可執行檔

Access Manager SecurID 認證模組透過 Security Dynamic ACE/Client C API 和 amsecruidd 輔助程式來實作，此輔助程式可在 Access Manager SecurID 認證模組和 SecurID Server 之間通訊。SecurID 認證模組透過開啓 localhost:57943 的套接字來呼叫 amsecuridd 常駐程式，以偵聽 SecurID 認證請求。

備註 – 57943 是預設連接埠號。如果此連接埠號已被使用，您可在 SecurID 認證模組的 SecurID 輔助程式認證連接埠屬性中指定不同的連接埠號。此連接埠號在所有組織中必須是唯一的。

因爲到 amsecuridd 的介面是透過 stdin 的純文字，所以只許可本機主機連線。amsecuridd 使用後端的 SecurID 遠端 API (5.x 版本) 加密資料。

amsecuridd 輔助程式偵聽連接埠號 58943 (依預設)，以接收其配置資訊。如果此連接埠已被使用，您可在 AMConfig.properties 檔案 (依預設，位於 AccessManager-base /SUNWam/config/ 中) 的 securidHelper.ports 屬性中變更此連接埠。securidHelp.ports 屬性包含每個 amsecuridd 輔助程式實例之連接埠的清單 (以空格分隔)。儲存 AMConfig.properties 的變更之後，請重新啓動 Access Manager。

備註 – 對於和單獨 ACE/Server (包含不同的 sdconf.rec 檔案) 通訊的每個組織，系統應該執行單獨的 amsecuridd 實例。

---

amsecuridd 語法

語法如下所示：

```
amsecuridd [-v] [-c portnum]
```

amsecuridd 選項

verbose (-v)

開啓詳細模式，並記錄到 `/var/opt/SUNWam/debug/securidd_client.debug` 。

configure portnumber (-c portnm)

配置偵聽連接埠號。預設值爲 58943。

執行 amsecuridd 輔助程式

依預設，`amsecuridd` 位於 *AccessManager-base* `/SUNWam/share/bin`。若要在預設連接埠上執行輔助程式，請輸入以下指令 (無選項)：

```
./amsecuridd
```

若要在非預設連接埠上執行輔助程式，請輸入以下指令：

```
./amsecuridd [-v] [-c portnm]
```

還可透過 `amserver` 指令行公用程式來執行 `amsecuridd`，但它僅可在預設連接埠上執行。

必需的程式庫

爲了執行輔助程式，需要以下程式庫 (大多數程式庫可在作業系統的 `/usr/lib/` 中找到)：

- `libnsl.so.1`
- `libthread.so.1`
- `libc.so.1`
- `libdl.so.1`
- `libmp.so.2`
- `librt.so.1`
- `libaio.so.1`
- `libmd5.so.1`

備註 – 將 `LD_LIBRARY_PATH` 設定爲 *AccessManager-base* `/Sunwam/lib/`，以找到 `libaceclnt.so`。

第 V 部分

附錄

這是「Sun Java System Access Manager 7 2005Q4 管理指南」的第五部分，其包含錯誤碼清單與檔案參照。本節包含以下附錄：

- 附錄 A
- 附錄 B
- 附錄 C
- 附錄 D

◆ ◆ ◆ 附錄 A

AMConfig.properties 檔案

AMConfig.properties 是 Access Manager 的主要配置檔案。您可以在此檔案中配置部分特性，但並非全部特性。本章提供包含於 AMConfig.properties 中之特性的描述、預設特性值以及修改那些可以變更並且不會危害到 Access Manager 安全的值的相關指示。

本章包含下列小節：

- 第 228 頁的 「SMTP」
- 第 228 頁的 「統計服務」

關於 AMConfig.properties 檔案

安裝時，AMConfig.properties 位於下列目錄中：/etc/opt/SUNWam/config。

AMConfig.properties 的格式爲每行一個特性，而且每個特性都有一個對應值。特性和值區分大小寫。以斜線加上星號字元 (/*) 開頭的各行是註釋，應用程式會忽略這些註釋。註釋的最後一行是以星號加上斜線字元 (*/) 結束。

當您修改 AMConfig.properties 中的特性之後，必須重新啓動 Access Manager 才能使變更生效。

Access Manager 主控台

- com.iplanet.am.console.deploymentDescriptor

  值是在安裝期間設定的。範例：/amconsole
- com.iplanet.am.console.host

  值是在安裝期間設定的。範例：*hostName.domain.Name*.com
- com.iplanet.am.console.port

  值是在安裝期間設定的。範例：80
- com.iplanet.am.console.protocol

  值是在安裝期間設定的。範例：http

Access Manager 伺服器安裝

- com.iplanet.am.install.basedir

  這是「唯讀」特性。請勿修改此特性值。

  值是在安裝期間設定的。範例：/opt/SUNWam/web-src/services/WEB-INF
- com.iplanet.am.install.vardir

  這是「唯讀」特性。請勿修改此特性值。

  值是在安裝期間設定的。範例：/var/opt/SUNWam
- com.iplanet.am.installdir

  這是「唯讀」特性。請勿修改此特性值。

  值是在安裝期間設定的。範例：/opt/SUNWam
- com.iplanet.am.jdk.path

值是在安裝期間設定的。範例：/usr/jdk/entsys-j2se

- com.iplanet.am.locale

  值是在安裝期間設定的。範例：en_US

- com.iplanet.am.server.host

  值是在安裝期間設定的。範例：*hostName.domainName*.com

- com.iplanet.am.server.port

  值是在安裝期間設定的。範例：80

- com.iplanet.am.server.protocol

  值是在安裝期間設定的。範例：http

- com.iplanet.am.version

  值是在安裝期間設定的。範例：7 2005Q4

- com.sun.identity.server.fqdnMap[ ]

  當使用者鍵入不正確的 URL 時，請啓用 Access Manager 認證服務以採取修正動作。例如，當使用者指定一個局部的主機名稱或使用一個 IP 位址以存取受保護的資源時，這是有用的。

  此特性的語法代表無效的 FQDN 值對映到其對應的有效值。該特性使用下列形式：com.sun.identity.server.fqdnMap[*invalid-name*]=*valid—name* . 在此範例中，*invalid-name* 是使用者可能使用的無效 FQDN 主機名稱，而 *valid—name* 是篩選器會將使者用者重新導向到的 FQDN 主機名稱。若存在的 FQDN 值重疊且同樣無效，應用程式可能無法存取。對此特性使用無效值，也會造成應用程式無法存取。您可以使用此特性來對映多個主機名稱。當寄存於伺服器上的應用程式可爲多重主機名稱存取時，這是有用的。

  您可以使用此特性來配置 Access Manager，所以不會對特定主機名稱 URL 採取更正動作。例如，當不能採取更正動作時這是很有用的，如針對使用原始 IP 位址來存取應用程式資源之使用者所使用的重新導向。

  您可指定一個對映項目，例如：com.sun.identity.server.fqdnMap[*IP*]=*IP* 。

  您可指定任何數量之該種特性(只要其爲有效的特性並符合上述的要求)。範例：
  com.sun.identity.server.fqdnMap[*isserver*]=*isserver.mydomain.com*
  com.sun.identity.server.fqdnMap[*isserver.mydomain*]=*isserver.mydomain.com*
  com.sun.identity.server.fqdnMap[*IP address*]=*isserver.mydomain.com*

am.util

- com.iplanet.am.util.xml.validating

  預設值爲 no。決定當使用 Access Manager XMLUtils 類別來剖析 XML 文件時，是否需要驗證。只有當值爲 com.iplanet.services.debug 時，此特性才有效。**層級**特性設定爲 warning 或 message。允許的值有 yes 和 no。僅當此特性的值爲 yes，且 com.iplanet.services.debug.level property 設定爲 warning或 message 時，才會開啓 XML 文件驗證。

amSDK

每個 SDK 快取項目會針對某個使用者儲存一組 AMObject 屬性值。

- com.iplanet.am.sdk.cache.maxSize

  預設值爲 10000。當啓用快取時，指定 SDK 快取的大小。使用一個大於 0 的整數，否則將會使用預設大小 (10000 個使用者)。

- com.iplanet.am.sdk.userEntryProcessingImpl

  此特性指定實作 com.iplanet.am.sdk.AMUserEntryProcessed 介面的外掛程式以執行對使用者建立、刪除及修改作業的某些後處理。若使用該特性，則應指定實作上述介面之完全合格的類別名稱。

- com.iplanet.am.sdk.caching.enabled

  設定此爲 true 可啓用快取，而設定此爲 false 則停用快取。預設值爲 false。

Application Server 安裝

- com.iplanet.am.iASConfig

  值是在安裝期間設定的。範例：APPSERVERDEPLOYMENT

  此特性用於決定 Access Manager 是否在 iPlanet 應用程式伺服器上執行。

認證

- com.sun.identity.auth.cookieName

  預設值爲 AMAuthCookie。指定認證服務所使用的 cookie 名稱以於認證程序期間設定階段作業處理器 ID。一旦完成了此程序 (成功或失敗)，將清除或移除此 cookie。

- com.sun.identity.authentication.ocsp.responder.nickname

  值是在安裝期間設定的。憑證授權機構 (CA) 對該回應程式的暱稱授予憑證。範例：Certificate Manager - sun。如果設定，在 Web 伺服器的憑證資料庫中必須出現該 CA 憑證。

- com.sun.identity.authentication.ocsp.responder.url

  值是在安裝期間設定的。範例： http://ocsp.sun.com/ocsp

  指定此實例的全域 OCSP 回應程式 URL。如果已設定 OCSP 回應程式 URL，則必須同時設定 OCSP 回應程式別名。否則，兩者都會被忽略。若兩者皆未設定，顯現於使用者憑證的 OCSP 回應程式 URL 將爲 OCSP 驗證所使用。若 OCSP 回應程式 URL 未顯現於使用者憑證中，則將不執行 OCSP 驗證。

- com.sun.identity.authentication.ocspCheck

  預設值爲 true。啓用或停用 OCSP 檢查的全域參數。若此值爲 false，則無法使用憑證認證模組類型中的 OCSP 特性。。

- com.sun.identity.authentication.special.users

  值是在安裝期間設定的。範例：cn=dsameuser,ou=DSAME Users,o=AMRoot|cn=amService-UrlAccessAgent,ou=DSAME Users,o=AMRoot

  對此 Access Manager 認證元件識別指定的使用者。用戶端 API 使用此使用者利用完整使用者 DN 以對 Access Manager 伺服器認證遠端應用程式。使用者將總是在本機目錄伺服器上進行認證。此特殊使用者 DN 的多重值可以管道字元 (|) 來分隔。僅限於認證元件可以使用此特性。

- com.sun.identity.authentication.super.user

  值是在安裝期間設定的。範例：uid=amAdmin,ou=People,o=AMRoot

  識別此 Access Manager 實例的超級使用者。此使用者必須使用 LDAP 來登入，且必須使用完整的 DN。始終會針對本機 Directory Server 來認證使用者。

- com.sun.identity.authentication.uniqueCookieDomain

  用來爲以上 cookie 名稱設定 cookie 網域。必須設定此 Cookie 網域，使其涵蓋安裝在網路中的所有 CDC (跨網域控制器) 服務實例。例如，若 Access Manager 的所有實例皆於網域 example.com 中，則爲 .example.com。

- com.sun.identity.authentication.uniqueCookieName

  預設值爲 sunIdentityServerAuthNServer。指定針對階段作業 Cookie 劫持執行 Access Manager 時，將 cookie 名稱設定爲 Access Manager 伺服器主機 URL。

- com.iplanet.am.auth.ldap.createUserAttrList

  指定使用者屬性的清單，當認證服務配置成動態建立使用者時，在 LDAP 認證期間可以由外部 Directory Server 擷取清單中包含的值。在本機 Directory Server 中建立的新使用者，會具有從外部 Directory Server 擷取到的屬性值。

  範例：*attribute1*、*attribute2*、*attribute3*

憑證資料庫

當 iPlanet Web 伺服器配置爲使用 SSL 時，請設定這些特性以初始化 JSS Socket Factory (JSS 通訊端工廠)。

- com.iplanet.am.admin.cli.certdb.dir

  值是在安裝期間設定的。範例：/opt/SUNWwbsvr/alias

  指定憑證資料庫路徑。

- com.iplanet.am.admin.cli.certdb.passfile

  值是在安裝期間設定的。範例：/etc/opt/SUNWam/config/.wtpass

  指定憑證資料庫密碼檔案。

- com.iplanet.am.admin.cli.certdb.prefix

  值是在安裝期間設定的。範例：https-*hostName.domainName*.com-*hostName*-

  指定憑證資料庫前綴。

Cookie

- com.iplanet.am.cookie.encode

  此特性可讓 Access Manager 對 cookie 值進行 URLencode，其可將字元轉換爲 HTTP 可以理解的字元。

  值是在安裝期間設定的。範例：false

- com.iplanet.am.cookie.name

  預設值爲 iPlanetDirectoryPro。認證服務所使用的 Cookie 名稱來設定有效的階段作業控制器 ID。此 cookie 名稱值是用來擷取有效的階段作業資訊。

- com.iplanet.am.cookie.secure

  當使用一個如 HTTP(s) 的安全通訊協定時，允許以一個安全模式設定 Access Manager cookie，其中瀏覽器將僅傳回 cookie。

  預設值爲 false。

- com.iplanet.am.console.remote

  值是在安裝期間設定的。範例：false

  決定主控台是安裝在遠端機器上，或安裝在本機機器上並由認證控制台使用。

- com.iplanet.am.pcookie.name

  指定永久 cookie 的 cookie 名稱。永久性 cookie 於瀏覽器視窗關閉後仍然繼續存在。此可使使用者以新的瀏覽器階段作業登入而不需重新認證。預設值爲 DProPCookie。

- com.sun.identity.cookieRewritingInPath

  預設值爲 true。當配置 Access Manager 以無 cookie 模式執行時，此特性爲認證服務所讀取。該特性指定需要使用以下形式將 cookie 重寫爲 URL 中的額外路徑資訊：protocol://server:port/uri;*cookiename*= cookieValue?queryString。若未指定特性，則將 cookie 寫入爲查詢字串的一部分。

- com.sun.identity.enableUniqueSSOTokenCookie

  預設值爲 false。指出當值設定爲 true 時，針對階段作業 Cookie 劫持會執行 Access Manager。

除錯

- com.iplanet.services.debug.directory

  指定將建立除錯檔案的輸出目錄。值是在安裝期間設定的。範例：/var/opt/SUNWam/debug

- com.iplanet.services.debug.level

  指定除錯層級。預設值爲 error。可能的值有：

off	不建立任何除錯檔案。
error	僅記錄錯誤訊息。

`warning` 僅記錄警告訊息。

`message` 記錄錯誤、警告及資訊性訊息。

Directory Server 安裝

- `com.iplanet.am.defaultOrg`
  值是在安裝時設定的。範例：`o=AMRoot`
  指定 Access Manager 資訊樹中的最高層範圍或組織。
- `com.iplanet.am.directory.host`
  值是在安裝期間設定的。範例：*DirectoryServerHost.domainName*.com
  指定 Directory Server 的完整合格主機名稱。
- `com.iplanet.am.directory.port`
  值是在安裝期間設定的。範例：`389`
  指定 Directory Server 連接埠號。
- `com.iplanet.am.directory.ssl.enabled`
  預設值爲 `false`。指出是否已啓用 Security Socket Layer (SSL)。
- `com.iplanet.am.domaincomponent`
  值是在安裝期間設定的。範例：`o=AMRoot`
  指定 Access Manager 資訊樹的網域元件 (dc) 屬性。
- `com.iplanet.am.rootsuffix`
  值是在安裝期間設定的。範例：`o=AMRoot`

事件連線

- `com.iplanet.am.event.connection.delay.between.retries`
  預設值爲 3000。指定重試以重新建立事件服務連線的延遲 (以毫秒爲單位)。
- `com.iplanet.am.event.connection.ldap.error.codes.retries`
  預設值爲 `80,81,91`。指定將觸發重試以重新建立 [事件服務] 連線的 LDAP 異常錯誤碼。
- `com.iplanet.am.event.connection.num.retries`
  預設值爲 `3`。指定成功地重新建立 [事件服務] 連線的嘗試次數。
- `com.sun.am.event.connection.idle.timeout`
  預設值爲 `0`。指定將會重新啓動永久性搜尋之前的分鐘數。

當策略代理程式與 Directory Server 之間有負載平衡器或防火牆時會使用此特性，而當發生 TCP **閒置逾時**時則會中斷永久性搜尋。此特性值應低於負載平衡器或防火牆 TCP 逾時。這可確保在連線中斷之前，重新啓動永久性搜尋。數值爲 `0` 指出將不會重新啓動搜尋。只有已逾時的連線才會重設。

全域服務管理

- `com.iplanet.am.service.secret`

  值是在安裝期間設定的。範例：`AQICPX9e1cxSxB2RSy1WG1+O4msWpt/6djZl`
- `com.iplanet.am.services.deploymentDescriptor`

  值是在安裝期間設定的。範例：`/amserver`
- `com.iplanet.services.comm.server.pllrequest.maxContentLength`

  預設值爲 `16384` 或 16k。指定 Access Manager 可接受之 `HttpRequest` 的最大內容長度。
- `com.iplanet.services.configpath`

  值是在安裝期間設定的。範例：`/etc/opt/SUNWam/config`

輔助常駐程式

- `com.iplanet.am.daemons`

  預設值爲 `unix securid`。描述
- `securidHelper.ports`

  預設值爲 `58943`。此特性採用以空格分隔的清單，並用於 SecurID 認證模組和說明程式。
- `unixHelper.ipaddrs`

  值是在安裝期間設定的。當開啓輔助程式時，指定一份將爲 `amserver` 程序檔所讀取並傳送至 UNIX 輔助程式的 IP 位址清單。此特性可以包含 IPv4 格式的可信任 IP 位址清單 (以空格分隔)。
- `unixHelper.port`

  預設值爲 `58946`。用於 UNIX 認證模組類型。

識別聯合

- `com.sun.identity.federation.alliance.cache.enabled`

  預設值爲 `true`。若爲 `true`，則將於內部快取聯合中介資料。
- `com.sun.identity.federation.fedCookieName`

  預設值爲 `fedCookie`。指定聯合服務 cookie 的名稱。

- com.sun.identity.federation.proxyfinder

  預設值爲 com.sun.identity.federation.services.FSIDPProxyImpl。定義實作，以尋找欲被代理的偏好身份提供者。

- com.sun.identity.federation.services.signingOn

  預設值爲 false。針對 Liberty 請求與回應，指定簽名驗證的層級。

true	當傳送時會簽署 Liberty 請求與回應，而接收時則會驗證 Liberty 請求與回應的簽名有效性。
false	傳送和接收的 Liberty 請求與回應將不會驗證簽名。
optional	只有當聯合設定檔要求時，才會簽署或驗證 Liberty 請求與回應。

- com.sun.identity.password.deploymentDescriptor

  值是在安裝期間設定的。範例：/ampassword

- com.sun.identity.policy.Policy.policy_evaluation_weights

  預設值爲 10:10:10。指出評估策略主旨、規則和條件的比例處理成本。此值指出所評估策略之主旨、規則和條件的影響順序。此值是使用三個整數來表示，分別代表主旨、規則和條件。此值是以冒號分隔 (:) 來指出評估策略主旨、規則和條件的比例處理成本。

- com.sun.identity.session.application.maxCacheTime

  預設值爲 3。指定應用程式階段作業之快取時間的最大分鐘數。依預設，除非啓用此特性，否則快取不會過期。

- com.sun.identity.sm.ldap.enableProxy

  預設值爲 false。指定用於連線的代理伺服器。若後端儲存支援 LDAPProxy，請設定爲 true。若爲 true，會使用代理伺服器來連線。若爲 false，則不會使用代理程式來連線。

- com.sun.identity.webcontainer

  值是在安裝期間設定的。範例：WEB_CONTAINER

  指定 Web 容器名稱。雖然 servlet 或 JSP 不依賴於 Web 容器，Access Manager 使用 servlet 2.3 API request.setCharacterEncoding() 以正確地對內送的非英文字元解碼。如果 Access Manager 部署在 Sun Java System Web 伺服器 6.1 上，這些 API 將不會運作。Access Manager 使用 gx_charset 機制在 Sun Java System Web 伺服器 6.1 版與 S1AS7.0 版中將內送的資料正確地解碼。可能的值有 BEA6.1、BEA 8.1、IBM5.1 或 IAS7.0。若 Web 容器是 Sun Java System Web Server，則不會置換標記。

JSS 代理程式

這些特性識別 SSL ApprovalCallback 的值。如果已啓用 checkSubjectAltName 或 resolveIPAddress 功能，您必須以 com.iplanet.am.admin.cli.certdb.dir 目錄中的前綴值 com.iplanet.am.admin.cli.certdb.prefix 來建立 cert7.db 和 key3.db。然後重新啓動 Access Manager。

- com.iplanet.am.jssproxy.checkSubjectAltName

預設值爲 false。當啓用時，伺服器憑證包括「主旨替代名稱」(SubjectAltName) 副檔名，且 Access Manager 檢查副檔名中所有名稱項目。若 SubjectAltName 副檔名中的一個名稱與伺服器 FQDN 相同，則 Access Manager 會繼續 SSL 訊號交換模式。若要啓用此特性，將其設定爲信任 FQDN 的逗號分隔清單。例
如：com.iplanet.am.jssproxy.checkSubjectAltName=
amserv1.example.com,amserv2.example.com

- com.iplanet.am.jssproxy.resolveIPAddress

  預設值爲 false。

- com.iplanet.am.jssproxy.trustAllServerCerts

  預設值爲 false。若啓用 (true)， Access Manager 會忽略所有與憑證相關的問題 (如名稱衝突)，繼續 SSL 訊號交換模式。若要防止可能的安全性風險，僅爲測試目的啓用此特性或當企業網路受到嚴謹的控制時。若可能發生安全性風險 (例如，若一個伺服器於不同的網路上連接一個伺服器)，則請避免啓用此特性。

- com.iplanet.am.jssproxy.SSLTrustHostList 若設定了此特性，Access Manager 會檢查正存取伺服器主機上的平台伺服器清單。若平台伺服器清單中兩個伺服器的伺服器 FQDN 相符，Access Manager 會繼續 SSL 訊號交換模式。使用下列語法以設定特性：

  com.iplanet.am.jssproxy.SSLTrustHostList = *fqdn_am_server1* ,*fqdn_am_server2*, *fqdn_am_server3*

- com.sun.identity.jss.donotInstallAtHighestPriority

  預設值爲 false。決定是否以最高優先權將 JSS 新增到 JCE。如果數位簽名與加密應該使用其他 JCE 提供者，請設定爲 true。

連線

- com.iplanet.am.ldap.connection.delay.between.retries

  預設爲 1000。指出重試之間的毫秒數。

- com.iplanet.am.ldap.connection.ldap.error.codes.retries

  預設值爲 80,81,91。指定將觸發重試以重新建立 LDAP 連線的 LDAPException 錯誤碼。

- com.iplanet.am.ldap.connection.num.retries

  預設值爲 3。指定成功地重新建立 LDAP 連線的嘗試次數。

Liberty 聯盟互動

- com.sun.identity.liberty.interaction.htmlStyleSheetLocation

  值是在安裝期間設定的。範例： /opt/SUNWam/lib/is-html.xsl

  指定描繪 HTML 中互動式頁面的樣式表路徑。

- com.sun.identity.liberty.interaction.wmlStyleSheetLocation

值是在安裝期間設定的。範例： `/opt/SUNWam/lib/is-wml.xsl`

指定於 WML 中提供互動頁面之樣式表的路徑。

- `com.sun.identity.liberty.interaction.wscSpecifiedInteractionChoice`

  預設值爲 `interactIfNeeded`。指定 Web 服務用戶是否參與互動。允許的值爲：

`interactIfNeeded`	若有需要，僅互動。也可用於指定無效值時。
`doNotInteract`	沒有互動。
`doNotInteractForData`	無資料互動。

- `com.sun.identity.liberty.interaction.wscSpecifiedMaxInteractionTime`

  預設值爲 `80`。Web 服務用戶在可接受之互動期間的喜好設定。值以秒來表示。如果未指定值或指定非整數值時，會使用預設值。

- `com.sun.identity.liberty.interaction.wscWillEnforceHttpsCheck`

  預設值爲 `yes`。指定 Web 服務用戶是否強制要求，使用 HTTPS 將請求重新導向到 URL。有效值爲 `yes` 和 `no`。大小寫會忽略。Liberty 規格需要值爲 `yes`。如果未指定任何值，則會使用預設值。

- `com.sun.identity.liberty.interaction.wscWillInlcudeUserInteractionHeader`

  預設值爲 `yes`。如果未指定任何值，則會使用預設值。指出 Web 服務用戶是否包括 `userInteractionHeader`。允許的值有 `yes` 和 `no`。大小寫會忽略。

- `com.sun.identity.liberty.interaction.wscWillRedirect`

  預設值爲 `yes`。指出 Web 服務用戶是否對互動重新導向使用者。有效值爲 `yes` 和 `no`。若未指定值，則使用預設值。

- `com.sun.identity.liberty.interaction.wspRedirectHandler`

  值是在安裝期間設定的。範例：
  `http://`*hostName.domainName*`.com:`*portNumber*`/amserver/WSPRedirectHandler`

  指定 URL `WSPRedirectHandlerServlet` 用來處理根據使用者代理程式重新導向的 Liberty WSF WSP 資源所有者互動。這應該在執行 Liberty 服務提供者的相同 JVM 上執行。

- `com.sun.identity.liberty.interaction.wspRedirectTime`

  預設爲 `30`。Web 服務提供者之互動的預期期間。以秒來表示。如果未指定值，或若值是非整數時，會使用預設值。

- `com.sun.identity.liberty.interaction.wspWillEnforceHttpsCheck`

  預設值爲 `yes`。如果未指定任何值，則會使用預設值。指出 Web 服務用戶是否會強制要求 `returnToURL` 使用 HTTPS。有效值爲 `yes` 和 `no`。(不區分大小寫) Liberty 規格要求此值爲 `yes`。

- `com.sun.identity.liberty.interaction.`

  `wspWillEnforceReturnToHostEqualsRequestHost`

  Liberty 規格需要值爲 `yes`。指出 Web 服務用戶是否強制 `returnToHost` 和 `requestHost` 是相同的。有效值爲 `yes` 和 `no`。

- com.sun.identity.liberty.interaction.wspWillRedirect

  預設爲 yes。如果未指定任何值，則會使用預設值。指出 Web 服務提供者是否會將使用者重新導向以進行互動。有效值爲 yes 和 no。大小寫會忽略。

- com.sun.identity.liberty.interaction.wspWillRedirectForData

  預設值爲 yes。如果未指定任何值，則會使用預設值。指出 Web 服務提供者是否會將使用者重新導向以進行資料互動。有效值爲 yes 和 no。大小寫會忽略。

- com.sun.identity.liberty.ws.interaction.enable

  預設值爲 false。

- com.sun.identity.liberty.ws.jaxb.namespacePrefixMappingList

  預設值爲

  ```
  =S=http://schemas.xmlsoap.org/soap/envelope/|sb=urn:liberty:sb:2003-08

  |pp=urn:liberty:id-sis-pp:2003-08|ispp=http://www.sun.com/identity/

  liberty/pp|is=urn:liberty:is:2003-08
  ```

  。指定將 JAXB 目錄樹狀結構調整爲 DOM 樹狀結構時，使用的名稱空間前綴對映。語法爲 prefix=namespace|prefix=namespace|...

- com.sun.identity.liberty.ws.jaxb.packageList

  指定建構 JAXBContext 時，所使用的 JAXB 套裝模組清單。每個套裝軟體必須以冒號 (:) 分隔。

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  預設值爲 com.sun.identity.liberty.ws.security.AMSecurityTokenProviderDescription。

- com.sun.identity.liberty.ws.soap.certalias

  值是在安裝期間設定的。將使用於 SSL 連線以爲 Liberty SOAP 連結所用的用戶端憑證別名。

- com.sun.identity.liberty.ws.soap.messageIDCacheCleanupInterval

  預設值爲 60000。指定開始快取清除事件之前要經過的毫秒數。儲存於快取中的每個訊息會以其 messageID 來避免訊息重複。當訊息的目前時間減去收到的時間超過 staleTimeLimit 值時，會從快取中移除該訊息。

- com.sun.identity.liberty.ws.soap.staleTimeLimit

  預設值爲 300000。確定訊息是否過時，因此不再可信。如果訊息的時間戳記早於目前戳記指定的毫秒數，訊息就被視爲超過時效。

- com.sun.identity.liberty.ws.soap.supportedActors

  預設值爲 http://schemas.xmlsoap.org/soap/actor/next。指定受支援的 SOAP 行動程式。每個行動程式必須以管道字元 (|) 來分隔。

- com.sun.identity.liberty.ws.ta.certalias

值是在安裝期間設定的。指定用於簽署 SAML 或 SAML 之可信任授權單位的憑證別名。回應訊息的 BEARER 記號。

- `com.sun.identity.liberty.ws.wsc.certalias`

  值是在安裝期間設定的。指定欲設憑證別名以用於核發此 Web 服務用戶端的 Web 服務安全性記號。

- `com.sun.identity.liberty.ws.ta.certalias`

  值是在安裝期間設定的。指定用於簽署 SAML 或 SAML 之可信任授權單位的憑證別名。回應訊息的 BEARER 記號。

- `com.sun.identity.liberty.ws.trustedca.certaliases`

  值是在安裝期間設定的。

  指定可信任 CA 的憑證別名。內送請求的 SAML 或 SAML BEARER 記號。必須由此清單中的可信任 CA 簽署訊息。語法爲
  cert alias 1`[:`*issuer 1*`]|`*cert alias 2*`[:`*issuer 2*`]|....`。
  範例： `myalias1:myissuer1|myalias2|myalias3:myissuer3`。
  當記號在簽名內沒有 `KeyInfo` 時，會使用值**發行者**。該記號核發者必須於此清單中，且對應憑證別名將用來驗證簽名。如果有 `KeyInfo`，按鍵必須包含符合 `KeyInfo` 的憑證別名，且憑證別名必須在此清單中。

- `com.sun.identity.liberty.ws.security.TokenProviderImpl`

  值是在安裝期間設定的。指定安全性記號提供者的實作。

- `com.sun.identity.saml.removeassertion`

  預設值爲 `true`。若解除參照的指定應由快取中移除，則指出旗標。套用至與工件相關所建立的指定並解除參照。

記錄服務

- `com.iplanet.am.logstatus`

  指定記錄是否開啓 (`ACTIVE`) 或關閉 (`INACTIVE`)。該值於安裝期間設定爲 `ACTIVE`。

您可新增至 AMConfig.properties 的記錄特性

藉由對 `AMConfig.properties` 檔案新增特性，您可配置包含於特定記錄檔案中資料的詳細程度。請使用以下格式：

`iplanet-am-logging.`*logfileName* `.level=`*java.util.logging.Level*，其中 *logfileName* 是 Access Manager 服務 (請參閱表 1) 記錄檔的名稱，而 *java.util.logging.Level* 是允許的屬性值。Access Manager 中的記錄層級爲 INFO 。SAML 和識別聯合服務亦以更詳細的程度來記錄 (FINE、FINER、FINEST)。範例：

```
iplanet-am-logging.amSSO.access.level=FINER
```

亦可關閉對特定記錄檔的記錄。範例：

```
iplanet-am-logging.amConsole.access.evel=OFF
```

表 A–1 Access Manager 記錄檔

記錄檔名稱	已記錄的記錄
amAdmin.access	成功的 amadmin 指令行事件
amAdmin.error	amadmin 指令行錯誤事件
amAuthLog.access	Access Manager 策略代理程式相關的事件。請參閱本表之後的說明。
amAuthentication.access	成功的認證事件
amAuthentication.error	認證失敗
amConsole.access	控制台事件
amConsole.error	控制台錯誤事件。
amFederation.access	成功的聯合事件。
amFederation.error	聯合錯誤事件。
amPolicy.access	儲存策略允許事件
amPolicy.error	儲存策略拒絕事件
amSAML.access	成功的 SAML 事件
amSAML.error	SAME 錯誤事件
amLiberty.access	成功的 Liberty 事件
amLiberty.error	Liberty 錯誤事件
amSSO.access	單次登入建立與破壞
amSSO.error	單次登入錯誤事件

備註 – amAuthLog 檔名可由 AMAgent.properties 中的策略代理程式特性決定。若爲 Web 策略代理程式，特性爲 com.sun.am.policy.agents.config.remote。log。若爲 J2EE 策略代理程式，特性爲 com.sun.identity.agents.config.remote.logfile。預設爲 amAuthLog.*host.domain.port*，其中 *host.domain* 是執行策略代理程式 Web 伺服器主機之完全合格的主機名稱，而 *port* 是該伺服器的連接埠號。若您部署了多重「策略代理程式」，您可擁有該檔案的多重實例。特性 com.sun.identity.agents.config.audit。accesstype (針對 Web 和 J2EE 代理程式兩者) 決定遠端記錄的資料。所記錄的資料可包括策略允許、策略拒絕、允許與拒絕兩者或者不包括允許也不包括拒絕。

命名服務

- com.iplanet.am.naming.failover.url

  Access Manager 7.0 中不再使用該特性。

- com.iplanet.am.naming.url

  值是在安裝期間設定的。範例：http://*hostName.domainName*.com:*portNumber*/amserver/namingservice

  指定要使用的命名服務 URL。

通知服務

使用下列各鍵來配置通知執行緒池。

- com.iplanet.am.notification.threadpool.size

  預設值爲 10。指定執行緒的總數來定義池的大小。

- com.iplanet.am.notification.threadpool.threshold

  預設值爲 100。指定最大作業佇列長度。

  當通知作業進入時，會被送到作業佇列進行處理。如果佇列達到最大長度，後續的內送請求會隨同 ThreadPoolException 一併拒絕，直到佇列有空間爲止。

- com.iplanet.am.notification.url

  值是在安裝期間設定的。範例：http://*hostName.domainName*.com:*portNumber*/amserver/notificationservice

策略代理程式

- com.iplanet.am.policy.agents.url.deploymentDescriptor

  值是在安裝期間設定的。範例： AGENT_DEPLOY_URI

- com.sun.identity.agents.app.username

  預設值爲 UrlAccessAgent。指定應用程式認證模組要使用的使用者名稱。

- com.sun.identity.agents.cache.size

  預設值爲 1000。指定資源結果快取的大小。在安裝策略代理程式的伺服器上建立快取。

- com.sun.identity.agents.header.attributes

  預設值爲 cn,ou,o,mail,employeenumber,c。指定要由策略評估程式傳回的策略特性。使用格式 a[,...]。於此範例中，a 是可於資料儲存庫中取得的特性。

- com.sun.identity.agents.logging.level

  預設值爲 NONE。控制策略用戶端 API 記錄層級的顆粒性。預設值爲 NONE。可能的數值爲：

ALLOW　記錄**允許存取**請求。

DENY　記錄**拒絕存取**請求。

BOTH　記錄**允許存取**和**拒絕存取**兩種請求。

NONE　沒有記錄任何請求情。

- com.sun.identity.agents.notification.enabled

  預設值爲 false。啓用或停用策略用戶端 API 的通知。

- com.sun.identity.agents.notification.url

  爲策略用戶端 SDK 所使用以註冊策略變更通知。此特性的錯誤配置將造成策略通知的停用。

- com.sun.identity.agents.polling.interval

  預設值爲 3。指定輪詢間隔，這是會從用戶端 API 快取中卸除項目之前的分鐘數。

- com.sun.identity.agents.resource.caseSensitive

  預設值爲 false。描述

  指定在策略評估期間，開啓或關閉區分大小寫。

- com.sun.identity.agents.true.value

  指定策略動作的眞實值。若應用程式不需要存取 PolicyEvaluator.isAllowed 方法，則可忽略此值。此值表示應如何解釋 Access Manager 的策略決定。預設值爲**允許**。

- com.sun.identity.agents.resource.comparator.class

  預設值爲 com.sun.identity.policy.plugins.URLResourceName

  指定資源比較類別名稱。可用的實作類別
  有：com.sun.identity.policy.plugins.PrefixResourceName 和
  com.sun.identity.policy.plugins.URLResourceName。

- com.sun.identity.agents.resource.delimiter

  預設值爲反斜線 (/)。指定資源名稱的分割元。

- com.sun.identity.agents.resource.wildcard

  預設值爲 *。指定資源名稱的萬用字元。

- com.sun.identity.agents.server.log.file.name

  預設值爲 amRemotePolicyLog。指定用來將訊息記錄到 Access Manager 的記錄檔名稱。僅需要檔案名稱。檔案目錄是由其他 Access manager 配置設定所決定的。

- com.sun.identity.agents.use.wildcard

  預設值爲 true。指出是否使用資源名稱比較的萬用字元。

策略用戶端 API

- com.sun.identity.policy.client.booleanActionValues

  iPlanetAMWebAgentService|POST|allow|deny

  預設值爲 iPlanetAMWebAgentService|GET|allow|deny:。

  指定策略動作名稱的布林動作值。使用以下格式 serviceName|actionName|trueValue|falseValue。動作名稱值爲分號 (:) 所分隔。

- com.sun.identity.policy.client.cacheMode

  預設值爲 self。指定用戶端策略評估程式的快取模式。有效值爲 subtree 與 self。如果設定爲 subtree，策略評估程式會針對實際請求資源之根目錄的所有資源，從伺服器取得策略決策。如果設定爲 self，策略評估程式僅會針對實際請求的資源，從伺服器取得策略決策。

- com.sun.identity.policy.client.clockSkew

  調整策略用戶端機器與策略伺服器之間的時間差異。如果此特性不存在，且策略代理程式的時間與策略伺服器的時間不同，則策略決策偶爾會發生錯誤。您必須執行時間同步服務，以使策略伺服器與策略用戶端上的時間儘可能保持接近。無論有否執行時間同步服務，使用此特性來調整微小的時間差異。　時間偏斜 (以秒爲單位) = 代理程式時間 - 伺服器時間。在策略伺服器上對特性加入註釋。取消對行的註釋，並在策略用戶端機器上或執行策略代理程式的機器上設定適當的代理程式-伺服器時間偏斜值 (以秒爲單位)。

- com.sun.identity.policy.client.resourceComparators=

  serviceType=iPlanetAMWebAgentService|class=

  指定不同服務名稱要使用的 ResourceComparators。由 Access Manager 控制台複製值。移至 [**配置服務**] > [PolicyConfiguration] > [**全域**: ResourceComparator]。從 Access Manager 鏈結多個值，使用冒號 (:) 做爲分割元。

- com.sun.identity.policy.plugins.URLResourceName|wildcard

  預設值爲 *|delimiter=/|caseSensitive=trueDescription

設定檔服務

- com.iplanet.am.profile.host

  Access Manager 7 中不再使用該特性。僅爲確保向下相容性而提供。值是在安裝期間設定的。範例：*hostName.domainName*.com

- com.iplanet.am.profile.port

  Access Manager 7 中不再使用該特性。僅爲確保向下相容性而提供。值是在安裝期間設定的。範例：80

複製

使用下列各鍵來配置複製設定。

- com.iplanet.am.replica.delay.between.retries

  預設值爲 1000。指定重試之間的毫秒數。

- com.iplanet.am.replica.num.retries

  預設值爲 0。指定要重試的次數。

SAML 服務

- com.sun.identity.saml.assertion.version

  預設值爲 1.1。指定使用的預設 SAML 版本。可能的值爲 1.0 或 1.1。

- com.sun.identity.saml.checkcert

  預設值爲 on。針對鍵值儲存區中的憑證，用來檢查內嵌於 KeyInfo 之憑證的旗標。鍵值儲存區中的憑證由 com.sun.identity.saml.xmlsig.keystore 特性指定。可能的數值爲：on|off。如果旗標爲「on」，*鍵值儲存區中必須出現憑證*以用於 XML 簽名驗證。如果旗標爲「off」，則略過*存在檢查*。/

  on　鍵值儲存區中必須出現憑證，以用於 XML 簽名驗證。

  off　略過檢查是否存在。

- com.sun.identity.saml.protocol.version

  預設值爲 1.1。指定使用的預設 SAML 版本。可能的值爲 1.0 或 1.1。

- com.sun.identity.saml.removeassertion

- com.sun.identity.saml.request.maxContentLength

  預設值爲 16384。指定將用於 SAML 之 HTTP **請求**的最大內容長度。

- com.sun.identity.saml.xmlsig.certalias

  預設值爲 test。描述

- com.sun.identity.saml.xmlsig.keypass

  值是在安裝期間設定的。範例：/etc/opt/SUNWam/config/.keypass

  指定 SAML XML 鍵密碼檔案的路徑。

- com.sun.identity.saml.xmlsig.keystore

  值是在安裝期間設定的。範例：/etc/opt/SUNWam/config/keystore.jks

  指定 SAML XML 鍵值儲存區密碼檔案的路徑。

- com.sun.identity.saml.xmlsig.storepass

  值是在安裝期間設定的。範例：/etc/opt/SUNWam/config/.storepass

指定 SAML XML 鍵儲存密碼檔案的路徑。

安全性

- com.iplanet.security.encryptor

  預設值爲 com.iplanet.services.util.JSSEncryption。指定加密類別實作。可用的類別有：com.iplanet.services.util.JCEEncryption 和 com.iplanet.services.util.JSSEncryption.

- com.iplanet.security.SecureRandomFactoryImpl

  預設值爲 com.iplanet.am.util.JSSSecureRandomFactoryImpl。指定 SecureRandomFactory 的工廠類別名稱。可用的實作類別有：com.iplanet.am.util.JSSSecureRandomFactoryImpl 會使用 JSS 和 com.iplanet.am.util.SecureRandomFactoryImpl 會使用純 Java。

- com.iplanet.security.SSLSocketFactoryImpl

  預設值爲 com.iplanet.services.ldap.JSSSocketFactory。指定 LDAPSocketFactory 的工廠類別名稱。可用的類別有： com.iplanet.services.ldap.JSSSocketFactory 會使用 JSS 和 netscape.ldap.factory.JSSESocketFactory 會使用純 Java。

- com.sun.identity.security.checkcaller

  預設值爲 false。啓用或停用 Java 安全性管理員檢查 Access Manager 的權限。預設爲停用。如果啓用，應適當變更部署 Access Manager 的容器之 Java 策略檔案。以此方式，就可用信任的 Access Manager JAR 檔案來執行機密作業。如需詳細資訊，請參閱 com.sun.identity.security 的 Java API Reference (Javadoc) 項目。

- am.encryption.pwd

  值是在安裝期間設定的。範例：dSB9LkwPCSoXfIKHVMhIt3bKgibtsggd

  指定用來對密碼加密與解密的鍵值。

階段作業服務

- com.iplanet.am.clientIPCheckEnabled

  預設值爲 false。指定是否在所有 SSOToken 建立或驗證時，檢查用戶端的 IP 位址。

- com.iplanet.am.session.client.polling.enable

  此爲「唯讀」特性。請勿修改此特性值。

  預設值爲 false。啓用用戶端階段作業輪詢。請注意階段作業輪詢模式與階段作業通知模式是相斥的。若啓用輪詢模式，階段作業通知將自動關閉，反之亦然。

- com.iplanet.am.session.client.polling.period

  預設值爲 180。指定輪詢期間的秒數。

- com.iplanet.am.session.httpSession.enabled

  預設值爲 true。啓用或停用 USING httpSession。

- com.iplanet.am.session.invalidsessionmaxtime

  預設值爲 10。若已建立階段作業且使用者並未登入，指定無效的階段作業將由階段作業表移除之後的分鐘數。此值應一律大於認證模組特性檔案中的逾時值。

- com.iplanet.am.session.maxSessions

  預設值爲 5000。指定允許的最大同步運作階段作業數。

  如果最大同步運作階段作業數超過此數字，登入會送出 [最大階段作業] 錯誤訊息。

- com.iplanet.am.session.purgedelay

  預設值爲 60。指定清除階段作業要延遲的分鐘數。

  這是階段作業逾時之後的延伸時間週期，在此期間階段作業會繼續存在於階段作業伺服器中。用戶端應用程式使用此特性，透過 SSO API 來檢查階段作業是否逾時。此延伸時間週期結束之後，此階段作業會被銷毀。如果使用者登出或 Access Manager 元件明確地銷毀階段作業，此階段作業不會在延伸期間持續。於此擴充期間，此階段作業是 INVALID 狀態。

- com.sun.am.session.caseInsensitiveDN

  預設值爲 true。比較代理程式 DN。若值爲 false，則比較區分大小寫。

- com.sun.am.session.enableHostLookUp

  預設值爲 false。在階段作業記錄期間，啓用或停用主機查詢。

SMTP

- com.iplanet.am.smtphost

  預設值爲 localhost。指定郵件伺服器主機。

- com.iplanet.am.smtpport

  預設值爲 25。指定郵件伺服器通訊埠。

統計服務

- com.iplanet.am.stats.interval

  預設值爲 60。指定統計記錄之間要經過的分鐘數。最小爲 5 秒，以避免 CPU 飽和。Access Manager 假設任何小於 5 秒的值皆爲 5 秒。

- com.iplanet.services.stats.directory

  值是在安裝期間設定的。範例：/var/opt/SUNWam/stats 指定建立除錯檔案的目錄。

- com.iplanet.services.stats.state

預設值爲 `file`。指定統計記錄的位置。可能的數值爲：

`off` 不記錄任何統計。

`file` 會將統計寫入指定目錄下的檔案。

`console` 會將統計寫入 Web 伺服器記錄檔。

◆ ◆ ◆ 附錄 B

serverconfig.xml 檔案

serverconfig.xml 檔案提供有關以 Directory Server 做爲資料存放區之 Sun Java™ System Access Manager 的配置資訊。本章說明該檔案的元素以及如何針對容錯移轉對其進行配置、如何具有多重實例、如何取消部署主控台以及如何從伺服器移除主控台檔案。包含以下小節：

簡介

serverconfig.xml 檔案位於 */ AccessManager-base* /SUNWam/config/ums。它包含 Identity SDK 建立 LDAP 連線池連至 Directory Server 時所用的參數。產品中的其他功能不使用此檔案。這個檔案中定義了兩個使用者：user1 爲 Directory Server 代理使用者，user2 爲 Directory Server 管理員。

代理使用者

代理使用者可以具備任何使用者的權限 (例如，組織管理員或一般使用者)。以連結至代理使用者之連線建立連線池。Access Manager 以 cn=puser,ou=DSAME Users,dc=example,dc=com 之 DN 建立代理使用者。此使用者用於所有針對 Directory Server 的查詢。它利用了已在 Directory Server 中配置的代理使用者 ACI，因此可在必要時代表使用者執行動作。 它會保持一條開啓的連線，透過該連線傳遞所有的查詢 (服務配置、組織資訊的擷取等等)。代理使用者密碼一律會加密。第 231 頁的「代理使用者」說明加密的密碼在 serverconfig.xml 中的位置。

範例 B–1 serverconfig.xml 中的代理使用者

```
<User name="User1" type="proxy">
<DirDN>
cn=puser,ou=DSAME Users,dc=example,dc=com
```

範例 B–1 serverconfig.xml 中的代理使用者 *(續)*

```
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

管理員使用者

dsameuser 用於連結，當 Access Manager SDK 在未連結至特定使用者的 Directory Server 上執行作業時使用 (例如，擷取服務配置資訊)。第 231 頁的「代理使用者」會代表 dsameuser 執行這些作業，但是連結必須先驗證 dsameuser 憑證。安裝時，Access Manager 會建立 cn=dsameuser,ou=DSAME Users,dc=example,dc=com。第 231 頁的「代理使用者」說明可在 serverconfig.xml 中的何處找到加密的 dsameuser 密碼。

範例 B–2 serverconfig.xml 中的管理員使用者

```
<User name="User2" type="admin">
<DirDN>
cn=dsameuser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

server-config 定義類型文件

server-config.dtd 定義 serverconfig.xml 的結構。它位於 *AccessManager-base* /SUNWam/dtd。本節定義 DTD 的主要元素。第 234 頁的「MiscConfig 元素」是 serverconfig.xml 檔案的範例。

iPlanetDataAccessLayer 元素

iPlanetDataAccessLayer 是根元素。它允許爲每個 XML 檔案定義多個伺服器群組。其直接子元素爲 第 233 頁的「ServerGroup 元素」。它並未包含任何屬性。

ServerGroup 元素

ServerGroup 定義到一或多個 Directory Server 的指標。它們可以是主伺服器或副本伺服器。符合 *ServerGroup* 標準的子元素包括 第 233 頁的 「Server 元素」、第 233 頁的 「User 元素」、第 234 頁的 「BaseDN 元素」與 第 234 頁的 「MiscConfig 元素」。*ServerGroup* 的 XML 屬性是該伺服器群組的名稱，而 *minConnPool* 和 *maxConnPool* 則定義可爲 LDAP 連線池開啓的最小 (1) 和最大 (10) 連線數。不支援定義多個 ServerGroup 元素。

備註 – Access Manager 使用連線池存取 Directory Server。當 Access Manager 開啓後且尚未關閉時，所有連線都是開啓的。可以重複使用這些連線。

Server 元素

Server 定義特定 Directory Server 實例。它並未包含任何子元素。對伺服器、主機名稱、執行 Directory Server 的連接埠號、必須開啓的 LDAP 連線類型 (簡單或 SSL) 而言，*Server* 的必要 XML 屬性名稱都是使用者友善的。

備註 – 如需使用 Server 元素之自動容錯移轉的範例，請參閱第 235 頁的 「容錯移轉或多主節點配置」。

User 元素

User 包含的子元素定義爲 Directory Server 實例配置的使用者。符合 *User* 標準的子元素包括 *DirDN* 和 *DirPassword*。其必要的 XML 屬性爲使用者的名稱，以及使用者的類型。*type* 的值可用於確定使用者的權限和爲 Directory Server 實例開啓的連線類型。選項包括：

- auth—定義驗證到 Directory Server 的使用者。
- proxy—定義 Directory Server 代理使用者。請參閱第 231 頁的 「代理使用者」以取得更多資訊。
- rebind—定義具有可用來重新連結之憑證的使用者。
- admin—定義具有 Directory Server 管理權限的使用者。請參閱第 232 頁的 「管理員使用者」以取得更多資訊。

DirDN 元素

DirDN 包含所定義使用者的 LDAP 辨別名稱。

DirPassword 元素

DirPassword 包含所定義使用者的已加密密碼。

注意 – 在部署過程中保持密碼與加密金鑰的一致性是很重要的。例如，此元素中定義的密碼亦會儲存在 Directory Server 中。如果變更了任一處的密碼，則必須在兩個地方都進行更新。此外，這個密碼是加密的。如果變更了 `am.encryption.pwd` 特性中定義的加密金鑰，則必須使用 `ampassword --encrypt` *password* 來重新加密 `serverconfig.xml` 中所有的密碼。

BaseDN 元素

BaseDN 定義伺服器群組的基本辨別名稱。它並未包含任何子元素與 XML 屬性。

MiscConfig 元素

MiscConfig 是定義任何 LDAP JDK 功能的預留位置，例如快取大小。它並未包含任何子元素。其必要的 XML 屬性是該功能的名稱及其定義值。

範例 B–3 serverconfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
 Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

 Use is subject to license terms.

-->
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
                <Server name="Server1" host="
               ishost.domain_name" port="389"
type="SIMPLE" />
                <User name="User1" type="proxy">
                        <DirDN>
                                cn=puser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <User name="User2" type="admin">
                        <DirDN>
                                cn=dsameuser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
```

範例 B–3 serverconfig.xml *(續)*

```
                </User>
                <BaseDN>
                        dc=example,dc=com
                </BaseDN>
        </ServerGroup>
</iPlanetDataAccessLayer>
```

容錯移轉或多主節點配置

Access Manager 允許自動容錯移轉至任何在 `serverconfig.xml` 中定義爲第 233 頁的「ServerGroup 元素」和第 233 頁的「Server 元素」之 Directory Server。可以爲容錯移轉或多主節點配置多部伺服器。如果第一部配置的伺服器關閉，則第二部配置的伺服器會接管。第 235 頁的「容錯移轉或多主節點配置」說明具有自動容錯移轉配置的 `serverconfig.xml`。

範例 B–4 在 serverconfig.xml 中配置容錯移轉

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<!--
PROPRIETARY/CONFIDENTIAL. Use of this product is subject to license terms.
Copyright 2002 Sun Microsystems, Inc. All rights reserved.
-->
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1" maxConnPool="10">
          <Server name="Server1" host="
            amhost1.domain_name" port="389" type="SIMPLE" />
          <Server name="Server2" host="
            amhost2.domain_name" port="389" type="SIMPLE" />
          <Server name="Server3" host="
            amhost3.domain_name" port="390" type="SIMPLE" />
          <User name="User1" type="proxy">
               <DirDN>
                    cn=puser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <User name="User2" type="admin">
               <DirDN>
                    cn=dsameuser,ou=DSAME Users,dc=example,dc=com
```

範例 B–4 在 serverconfig.xml 中配置容錯移轉 *(續)*

```
                </DirDN>
                <DirPassword>
                     AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
                </DirPassword>
           </User>
           <BaseDN>
                o=isp
           </BaseDN>
      </ServerGroup>
</iPlanetDataAccessLayer>
```

◆ ◆ ◆ 附錄 C

記錄檔參照

此附錄列出每個 Access Manager 功能區域之可能的記錄檔。本附錄中的表格說明下列記錄檔案項目：

- ID — 記錄識別號碼。
- 記錄層級 — 訊息的記錄層級特性。
- 描述 — 記錄訊息的描述。
- 日期 — 訊息保存的日期類型。
- 觸發器 — 記錄檔訊息的理由。
- 動作 — 您可取得更多資訊的動作。

記錄檔的定義與位置將於「Sun Java System Access Manager 7 2005Q4 Technical Overview」中描述。

表 C–1 amAdmin 指令行公用程式的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	使用者登入不成功。	使用者 ID	使用者登入不成功。	
2 TEST	INFO	已收到 ADMINEXCEPTION。	元素名稱錯誤訊息	當處理 Admin 請求時已收到 ADMINEXCEPTION。	檢查 amAdmin 除錯檔以取得更多資訊。
3	INFO	階段作業已銷毀	使用者的名稱	階段作業已銷毀。	
11	INFO	服務模式已載入	模式名稱	成功地載入服務模式。	
12	INFO	已刪除服務	服務名稱	成功地刪除服務。	
13	INFO	已新增特性	特性名稱	成功地新增特性。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
21	INFO	該特性並無策略	服務名稱	已指定刪除策略規則旗標，但服務並無策略。	
22	INFO	找不到服務的策略模式	服務名稱	已指定刪除策略規則旗標，但無法找到服務的策略模式	
23	INFO	刪除服務策略	服務名稱	以指定的刪除策略規則旗標刪除服務。	
24	INFO	刪除服務策略完成	服務名稱	以指定的刪除策略規則旗標刪除服務。	
25	INFO	建立於組織中的策略	策略名稱組織 *DN*	建立於組織 DN 中的策略	
26	INFO	由組織刪除的策略	策略名稱組織 *DN*	由組織 DN 刪除的策略	
31	INFO	將語言環境的資源束新增至 Directory Server。	資源束名稱資源語言環境	成功地將語言環境的資源束儲存於 Directory Server 之中。	
32	INFO	將預設資源束新增至 Directory Server。	資源束名稱	成功地將預設資源束儲存於 Directory Server 之中。	
33	INFO	已從 Directory Server 中刪除的語言環境資源束。	資源束名稱資源語言環境	已成功地從 Directory Server 中刪除的語言環境資源束。	
34	INFO	已從 Directory Server 中刪除的預設資源束。	資源束名稱	已成功地從 Directory Server 中刪除的預設資源束。	
41	INFO	已修改之服務的服務模式	服務的名稱	成功地修改服務的服務模式。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
42	INFO	服務的已刪除服務子模式。	子模式名稱服務名稱	成功地刪除服務的服務子模式。	
43	INFO	服務的已新增服務子模式。	服務的名稱	成功地對服務新增服務子模式。	
44	INFO	對服務新增子配置。	子配置名稱服務名稱	成功地對服務新增服務子配置。	
45	INFO	服務之已修改子配置	子配置名稱服務名稱	成功地修改服務的服務子配置。	
46	INFO	服務的已刪除子配置。	子配置名稱服務名稱	成功地刪除服務的服務子配置。	
47	INFO	刪除服務的所有服務配置。	服務的名稱	成功地刪除服務的所有服務配置。	
91	INFO	修改組織中的服務子配置	子配置名稱服務名稱組織 *DN*	成功地修改組織中的服務子配置。	
92	INFO	新增組織中的服務子配置	子配置名稱服務名稱組織 *DN*	成功地新增組織中的服務子配置。	
93	INFO	刪除組織中的服務子配置	子配置名稱服務名稱組織 *DN*	成功地刪除組織中的服務子配置。	
94	INFO	於組織中建立的遠端提供者	提供者名稱組織 *DN*	成功地於組織中建立遠端提供者。	
95	INFO	於組織中修改的遠端提供者	提供者名稱組織 *DN*	成功地於組織中修改遠端提供者。	
96	INFO	於組織中修改的寄存提供者	提供者名稱組織 *DN*	成功地於組織中修改寄存提供者。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
97	INFO	於組織中建立的寄存提供者	提供者名稱組織 *DN*	成功地於組織中建立寄存提供者。	如需更多資訊，請於識別儲存庫記錄下進行查詢。
98	INFO	於組織中刪除的遠端提供者	提供者名稱組織 *DN*	成功地於組織中刪除遠端提供者。	
99	INFO	於組織中建立認證網域	信任圈名稱組織 *DN*	成功地建立組織中的認證網域。	
100	INFO	於組織中刪除認證網域。	信任圈名稱組織 *DN*	成功地刪除組織中的認證網域。	
101	INFO	於組織中修改認證網域。	信任圈名稱組織 *DN*	成功地修改組織中的認證網域。	
102	INFO	嘗試修改服務範本	服務範本的 DN	已嘗試修改服務範本	
103	INFO	已修改的服務範本	服務範本的 DN	成功地修改服務範本。	
104	INFO	嘗試移除服務範本	服務範本的 DN	已嘗試移除服務範本。	
105	INFO	已移除的服務範本	服務範本的 DN	成功地移除服務範本。	
106	INFO	嘗試新增服務範本	服務範本的 DN	已嘗試新增服務範本。	
107	INFO	已新增的服務範本	服務範本的 DN	成功地新增服務範本。	
108	INFO	嘗試對群組新增巢式群組	要新增的群組名稱包含群組的 *DN*	已嘗試對群組新增巢式群組。	
109	INFO	對群組新增巢式群組	要新增的群組名稱包含群組的 *DN*	成功地對群組新增巢式群組。	
110	INFO	嘗試對群組或角色新增使用者	使用者名稱目標群組或角色	已嘗試對群組或角色新增使用者。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
111	INFO	對群組或角色新增使用者	使用者名稱目標群組或角色	成功地對群組或角色新增使用者。	
112	INFO	嘗試建立實體。	實體的 DN	已嘗試建立實體。	
113	INFO	已建立實體。	實體的本土化名稱實體的 *DN*	已建立實體。	
114	INFO	嘗試建立角色	角色 DN	已嘗試建立角色。	
115	INFO	建立的角色	角色名稱	已建立的角色。	
116	INFO	嘗試建立群組容器	群組容器名稱	已嘗試建立群組容器。	
117	INFO	建立群組容器	群組容器名稱	已建立的群組容器。	
118	INFO	嘗試建立群組。	群組名稱	嘗試建立群組。	
119	INFO	建立群組。	群組名稱	已建立群組。	
120	INFO	嘗試建立使用者容器。	使用者容器的 DN	已嘗試建立使用者容器。	
121	INFO	建立使用者容器。	使用者容器的 DN	已建立的使用者容器。	
122	INFO	嘗試於組織或角色中建立服務範本	服務範本名稱組織或角色的名稱	已嘗試於組織或角色中建立服務範本。	
123	INFO	於組織或角色中建立服務範本	服務範本名稱組織或角色的名稱	組織或角色中之已建立的服務範本。	
124	INFO	嘗試建立容器	容器名稱	已嘗試建立容器。	
125	INFO	建立容器	容器名稱	已建立的容器。	
126	INFO	嘗試建立使用者。	使用者的名稱	已嘗試建立使用者。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
127	INFO	建立使用者。	使用者的名稱	已建立的使用者。	
128	INFO	嘗試刪除實體。	實體的 DN	已嘗試刪除實體。	
129	INFO	刪除實體。	實體的本土化名稱實體的 *DN*	已刪除的實體。	
130	INFO	嘗試刪除使用者容器	使用者容器的 DN	已嘗試刪除使用者容器。	
131	INFO	刪除使用者容器	使用者容器的 DN	已刪除的使用者容器。	
132	INFO	嘗試刪除角色	角色名稱	已嘗試刪除角色。	
133	INFO	刪除角色	角色名稱	已刪除的角色。	
134	INFO	嘗試刪除組織中的服務範本	服務範本名稱組織名稱	已嘗試刪除組織中的服務範本。	
135	INFO	刪除組織中的服務範本	服務範本名稱組織名稱	組織中已刪除的服務範本。	
136	INFO	嘗試刪除容器。	容器名稱	已嘗試刪除容器。	
137	INFO	刪除容器。	容器名稱	已刪除的容器。	
138	INFO	嘗試修改實體	實體的本土化名稱實體的 *DN*	已嘗試修改實體。	
139	INFO	修改實體	實體的本土化名稱實體的 *DN*	已修改的實體。	
140	INFO	嘗試修改使用者容器。	使用者容器的 DN	已嘗試修改使用者容器。	
141	INFO	修改使用者容器。	使用者容器的 DN	已修改的使用者容器。	
142	INFO	嘗試修改容器。	容器名稱	已嘗試修改容器。	
143	INFO	修改容器。	容器名稱	已修改的容器。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
144	INFO	嘗試於組織下註冊服務。	服務名稱組織名稱	已嘗試於組織下註冊服務	
145	INFO	於組織下註冊服務。	服務名稱組織名稱	組織下之已註冊服務	
146	INFO	嘗試於組織下解除註冊服務。	服務名稱組織名稱	已嘗試於組織下解除註冊服務	
147	INFO	於組織下解除註冊服務。	服務名稱組織名稱	組織下的未註冊服務。	
148	INFO	嘗試修改群組。	群組名稱	已嘗試修改群組	
149	INFO	修改群組。	群組名稱	已修改的群組	
150	INFO	嘗試由群組移除巢式群組。	巢式群組名稱群組名稱	已嘗試由群組移除巢式群組。	
151	INFO	從群組移除巢式群組。	巢式群組名稱群組名稱	從群組移除的巢式群組。	
152	INFO	嘗試刪除群組	群組名稱	已嘗試刪除群組。	
153	INFO	刪除群組	群組名稱	已刪除的群組。	
154	INFO	嘗試由一個角色移除一個使用者	使用者名稱角色名稱	已嘗試由一個角色移除一個使用者。	
155	INFO	由一個角色移除一個使用者	使用者名稱角色名稱	已由一個角色移除一個使用者。	
156	INFO	嘗試由一個群組移除一個使用者	使用者名稱群組名稱	已嘗試由一個群組移除一個使用者。	
157	INFO	由一個群組移除一個使用者	使用者名稱群組名稱	已由一個群組移除一個使用者。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
201	INFO	嘗試對範圍中的識別新增識別	要新增的識別名稱要新增的識別類型要新增至的識別名稱要新增至的識別類型範圍名稱	已嘗試對範圍中的識別新增識別。	
202	INFO	對範圍中的識別新增識別	要新增的識別名稱要新增的識別類型要新增至的識別名稱要新增至的識別類型範圍名稱	已對範圍中的識別新增識別。	
203	INFO	嘗試對範圍中的識別指定服務。	服務名稱識別名稱識別類型範圍名稱	已嘗試對範圍中的識別指定服務。	
204	INFO	對範圍中的識別指定服務。	服務名稱識別名稱識別類型範圍名稱	已對範圍中的識別指定服務。	
205	INFO	嘗試建立範圍中一種類型的識別。	識別類型範圍名稱	已嘗試建立範圍中一種類型的識別。	
206	INFO	建立範圍中一種類型的識別。	識別類型範圍名稱	已建立範圍中一種類型的識別。	
207	INFO	嘗試建立範圍中一種類型的識別。	識別名稱識別類型範圍名稱	已嘗試建立範圍中一種類型的識別。	
208	INFO	建立範圍中一種類型的識別。	識別名稱識別類型範圍名稱	已建立範圍中一種類型的識別。	
209	INFO	嘗試刪除範圍中一種類型的識別	識別名稱識別類型範圍名稱	已嘗試刪除範圍中一種類型的識別。	
210	INFO	刪除範圍中一種類型的識別。	識別名稱識別類型範圍名稱	已刪除範圍中一種類型的識別。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
211	INFO	嘗試對範圍中的識別修改服務	服務名稱識別類型識別名稱範圍名稱	已嘗試對範圍中的識別修改服務。	
212	INFO	對範圍中的識別修改服務	服務名稱識別類型識別名稱範圍名稱	已對範圍中的識別修改服務。	
213	INFO	嘗試由範圍中的識別移除識別。	要移除的識別名稱要移除的識別類型要移除識別名稱之處要移除識別類型之處範圍名稱	已嘗試由範圍中的識別移除識別。	
214	INFO	由範圍的識別移除識別	要移除的識別名稱要移除的識別類型要移除識別名稱之處要移除識別類型之處範圍名稱	已由範圍的識別移除識別。	
215	INFO	嘗試對範圍中的識別設定服務特性	服務名稱識別類型識別名稱範圍名稱	已嘗試對範圍中的識別設定服務特性	
216	INFO	設定範圍中識別的服務特性	服務名稱識別類型識別名稱範圍名稱	設定範圍中識別的服務特性。	
217	INFO	嘗試由範圍中的識別取消指定服務	服務名稱識別類型識別名稱範圍名稱	已嘗試由範圍中的識別取消指定服務。	
218	INFO	從範圍中的識別取消指定服務	服務名稱識別類型識別名稱範圍名稱	已從範圍中的識別取消指定服務。	
219	INFO	嘗試建立組織	組織名稱	已嘗試建立一個組織。	
220	INFO	建立組織	組織名稱	已建立一個組織。	
221	INFO	嘗試刪除子組織。	子組織名稱	嘗試刪除子組織。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
222	INFO	刪除子組織。	子組織名稱	刪除的子組織。	
223	INFO	嘗試修改角色	角色名稱	已嘗試修改角色。	
224	INFO	修改角色	角色名稱	已修改的角色。	
225	INFO	嘗試修改子組織。	子組織名稱	嘗試修改子組織。	
226	INFO	修改子組織。	子組織名稱	修改的子組織。	
227	INFO	嘗試刪除使用者。	使用者的名稱	已嘗試刪除使用者。	
228	INFO	刪除使用者。	使用者的名稱	已刪除的使用者。	
229	INFO	嘗試修改使用者。	使用者的名稱	已嘗試修改使用者。	
230	INFO	修改使用者。	使用者的名稱	已修改的使用者。	
231	INFO	嘗試對範圍中的服務特性新增值。	特性名稱服務名稱範圍名稱	已嘗試對範圍中的服務特性新增值。	
232	INFO	對範圍中的服務特性新增值。	特性名稱服務名稱範圍名稱	已對範圍中的服務特性新增值。	
233	INFO	嘗試對範圍指定服務	服務名稱範圍名稱	已嘗試對範圍指定服務。	
234	INFO	對範圍指定服務	服務名稱範圍名稱	已對範圍指定服務。	
235	INFO	嘗試建立範圍。	已建立範圍的名稱父系範圍名稱	已嘗試建立範圍。	
236	INFO	建立一個範圍	已建立範圍的名稱父系範圍名稱	已建立一個範圍。	
237	INFO	刪除範圍。	是否遞迴已刪除的範圍名稱	已刪除的範圍。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
238	INFO	刪除範圍。	是否遞迴已刪除的範圍名稱	已刪除的範圍。	
239	INFO	嘗試修改範圍中的服務。	服務名稱範圍名稱	已嘗試修改範圍中的服務。	
240	INFO	修改範圍中的服務。	服務名稱範圍名稱	已修改範圍中的服務。	
241	INFO	嘗試由範圍中的服務移除一個特性	特性名稱服務名稱範圍名稱	已嘗試由範圍中的服務移除一個特性。	
242	INFO	由範圍中的服務移除一個特性	特性名稱服務名稱範圍名稱	已由範圍中的服務移除一個特性。	
243	INFO	嘗試由範圍中的服務特性移除值。	特性名稱服務名稱範圍名稱	已嘗試由範圍中的服務特性移除值。	
244	INFO	由範圍中的服務特性移除值	特性名稱服務名稱範圍名稱	已由範圍中的服務特性移除值。	
245	INFO	嘗試設定範圍中服務的特性。	服務名稱範圍名稱	已嘗試設定範圍中服務的特性。	
246	INFO	設定範圍中服務的特性。	服務名稱範圍名稱	設定範圍中服務的特性。	
247	INFO	嘗試由範圍取消指定服務。	服務名稱範圍名稱	已嘗試由範圍取消指定服務。	
248	INFO	由範圍取消指定服務。	服務名稱範圍名稱	已由範圍取消指定服務。	
249	INFO	嘗試對組織配置指定服務	服務名稱範圍名稱	已嘗試對組織配置指定服務。	
250	INFO	對組織配置指定服務	服務名稱範圍名稱	已對組織配置指定服務。	

表 C–1 amAdmin 指令行公用程式的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
251	INFO	對組織配置指定服務尚未完成	服務名稱範圍名稱	已對組織配置指定服務，但該服務並非組織配置之可指定服務的其中之一。	
252	INFO	對範圍指定服務尚未完成	服務名稱範圍名稱	對範圍指定服務，但該服務並非範圍之可指定服務的其中之一。	
253	INFO	嘗試由組織配置解除指定服務。	服務名稱範圍名稱	已嘗試由組織配置解除指定服務。	
254	INFO	由組織配置解除指定服務。	服務名稱範圍名稱	已由組織配置解除指定服務。	
255	INFO	解除指定不在組織配置中或範圍中的服務。	服務名稱範圍名稱	已請求解除指定不在組織配置中或範圍中的服務。	
256	INFO	嘗試修改組織配置中的服務。	服務名稱範圍名稱	已嘗試修改組織配置中的服務。	
257	INFO	修改組織配置中的服務。	服務名稱範圍名稱	已修改組織配置中的服務。	
258	INFO	修改不在組織配置中或範圍中的服務。	服務名稱範圍名稱	已嘗試修改不在組織配置中或範圍中的服務。	

表 C–2 認證的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
100	INFO	認證成功	訊息	以有效的憑證認證使用者	
101	INFO	基於使用者的認證成功	訊息認證類型使用者名稱	以有效的憑證認證使用者	

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
102	INFO	基於角色的認證成功	訊息認證類型 角色名稱	以有效的憑證認證屬於角色的使用者	
103	INFO	基於服務的認證成功	訊息認證類型 服務名稱	對範圍下之已配置的服務使用有效的憑證認證使用者	
104	INFO	基於認證層級的認證成功	訊息認證類型 認證層級值	對具有認證層級值大於或等於指定的認證層級之一或多個認證模組使用有效的憑證認證使用者	
105	INFO	基於模組的認證成功	訊息認證類型 模組名稱	對範圍下之認證模組使用有效的憑證認證使用者	
200	INFO	認證失敗	錯誤訊息	表示不正確/無效的憑證使用者鎖定/不在作用中	對必要的認證模組輸入正確/有效的憑證
201	INFO	認證失敗	錯誤訊息	已輸入無效的憑證。	輸入正確的密碼。
202	INFO	認證失敗	錯誤訊息	已命名的配置 (認證鏈接) 不存在。	爲此組織建立並配置一個已命名的配置。
203	INFO	認證失敗	錯誤訊息	並未找到該使用者的使用者設定檔。	使用者並未存在於配置的資料儲存外掛程式中，因此請正確地配置該範圍/組織的資料儲存外掛程式。
204	INFO	認證失敗	錯誤訊息	該使用者不在作用中。	啓動使用者。
205	INFO	認證失敗	錯誤訊息	已超過失敗嘗試的最大數量。鎖定使用者。	請連絡系統管理員。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
206	INFO	認證失敗	錯誤訊息	使用者帳號已過期。	請連絡系統管理員。
207	INFO	認證失敗	錯誤訊息	登入逾時。	重試登入。
208	INFO	認證失敗	錯誤訊息	認證模組遭到拒絕。	配置此模組或使用其他模組。
209	INFO	認證失敗	錯誤訊息	已達到最大可允許階段作業數的限度。	登出階段作業或增加限度。
210	INFO	認證失敗	錯誤訊息	組織/範圍不存在。	使用有效的組織/範圍。
211	INFO	認證失敗	錯誤訊息	組織/範圍不在作用中。	啓動組織/範圍。
212	INFO	認證失敗	錯誤訊息	無法建立階段作業。	請確保已配置階段作業服務，且並未達到最大階段作業數。
213	INFO	基於使用者的認證失敗	錯誤訊息認證類型使用者名稱	未對使用者配置認證配置 (一或多個認證模組鏈)。表示不正確/無效的憑證使用者鎖定/不在作用中	對使用者配置認證配置 (一或多個認證模組鏈)。對所需的認證模組輸入正確/有效的憑證
214	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證已輸入無效的憑證。	輸入正確的密碼。
215	INFO	認證失敗	錯誤訊息認證類型使用者名稱	此使用者的已命名的配置 (認證鏈接) 不存在	爲此使用者建立並配置一個已命名的配置。
216	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證並未找到該使用者的使用者設定檔。	使用者並未存在於配置的資料儲存外掛程式中，因此請正確地配置該範圍/組織的資料儲存外掛程式。
217	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證該使用者不在作用中。	啓動使用者。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
218	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證已超過失敗嘗試的最大數量。使用者已被鎖定。	請連絡系統管理員。
219	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證使用者帳號已過期。	請連絡系統管理員。
220	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證登入逾時。	重試登入。
221	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證認證模組遭到拒絕。	配置此模組或使用其他模組。
222	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證已達到最大可允許階段作業數的限度。	登出階段作業或增加限度。
223	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證組織/範圍不存在。	使用有效的組織/範圍。
224	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證組織/範圍不在作用中。	啓動組織/範圍。
225	INFO	認證失敗	錯誤訊息認證類型使用者名稱	基於使用者的認證無法建立階段作業。	請確保已配置階段作業服務，且並未達到最大階段作業數。
226	INFO	基於角色的認證失敗	錯誤訊息認證類型角色名稱	未對使用者配置認證配置 (一或多個認證模組鏈)。表示不正確/無效的憑證使用者不屬於此角色使用者鎖定/不在作用中	對角色配置認證配置 (一或多個認證模組鏈)。對所需的認證模組輸入正確/有效的憑證對認證的使用者指定此角色

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
227	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證已輸入無效的憑證。	輸入正確的密碼。
228	INFO	認證失敗	錯誤訊息認證類型角色名稱	此角色的已命名的配置 (認證鏈接) 不存在。	爲此角色建立並配置一個已命名的配置。
229	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證並未找到該使用者的使用者設定檔。	使用者並未存在於配置的資料儲存外掛程式中，因此請正確地配置該範圍/組織的資料儲存外掛程式。
230	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證該使用者不在作用中。	啓動使用者。
231	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證已超過失敗嘗試的最大數量。使用者已被鎖定。	請連絡系統管理員。
232	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證使用者帳號已過期。	請連絡系統管理員。
233	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證登入逾時。	重試登入。
234	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證認證模組遭到拒絕。	配置此模組或使用其他模組。
235	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證已達到最大可允許階段作業數的限度。	登出階段作業或增加限度。
236	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證組織/範圍不存在。	使用有效的組織/範圍。
237	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證組織/範圍不在作用中。	啓動組織/範圍。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
238	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證無法建立階段作業。	請確保已配置階段作業服務，且並未達到最大階段作業數。
239	INFO	認證失敗	錯誤訊息認證類型角色名稱	基於角色的認證使用者不屬於這個角色。	對這個角色新增使用者。
240	INFO	基於服務的認證失敗	錯誤訊息認證類型服務名稱	未對服務配置認證配置 (一或多個認證模組鏈)。表示不正確/無效的憑證使用者鎖定/不在作用中	對服務配置認證配置 (一或多個認證模組鏈)。對所需的認證模組輸入正確/有效的憑證
241	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證已輸入無效的憑證。	輸入正確的密碼。
242	INFO	認證失敗	錯誤訊息認證類型服務名稱	以此服務名稱的已命名的配置 (認證鏈接) 不存在。	建立並配置一個以命名的配置。
243	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證並未找到該使用者的使用者設定檔。	使用者並未存在於配置的資料儲存外掛程式中，因此請正確地配置該範圍/組織的資料儲存外掛程式。
244	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證該使用者不在作用中。	啓動使用者。
245	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證已超過失敗嘗試的最大數量。使用者已被鎖定。	請連絡系統管理員。
246	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證使用者帳號已過期。	請連絡系統管理員。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
247	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證登入逾時。	重試登入。
248	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證認證模組遭到拒絕。	配置此模組或使用其他模組。
249	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證服務不存在。	請僅使用有效的服務。
250	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證已達到最大可允許階段作業數的限度。	登出階段作業或增加限度。
251	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證組織/範圍不存在。	使用有效的組織/範圍。
252	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證組織/範圍不在作用中。	啓動組織/範圍。
253	INFO	認證失敗	錯誤訊息認證類型服務名稱	基於服務的認證無法建立階段作業。	請確保已配置階段作業服務，且並未達到最大階段作業數。
254	INFO	基於認證層級的認證失敗	錯誤訊息認證類型認證層級值	並無具有認證層級值大於或等於所指定認證層級的認證模組 對具有認證層級值大於或等於指定的認證層級之一或多個認證模組顯示不正確/無效的憑證 使用者鎖定/不在作用中	配置一或多個具有認證層級值大於或等於所需之認證層級的認證模組 對一或多個具有認證層級值大於或等於所指定認證層級的認證模組輸入正確/有效的憑證
255	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證已輸入無效的憑證。	輸入正確的密碼。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
256	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證無可用的認證配置。	建立一個認證配置。
257	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證並未找到該使用者的使用者設定檔。	使用者並未存在於配置的資料儲存外掛程式中，因此請正確地配置該範圍/組織的資料儲存外掛程式。
258	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證該使用者不在作用中。	啓動使用者。
259	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證已超過失敗嘗試的最大數量。使用者已被鎖定。	請連絡系統管理員。
260	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證使用者帳號已過期。	請連絡系統管理員。
261	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證登入逾時。	重試登入。
262	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證認證模組遭到拒絕。	配置此模組或使用其他模組。
263	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證認證層級無效。	請指定有效的認證層級。
264	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證已達到最大可允許階段作業數的限度。	登出階段作業或增加限度。
265	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證組織/範圍不存在。	使用有效的組織/範圍。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
266	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證組織/範圍不在作用中。	啓動組織/範圍。
267	INFO	認證失敗	錯誤訊息認證類型認證層級值	基於認證層級的認證無法建立階段作業。	請確保已配置階段作業服務，且並未達到最大階段作業數。
268	INFO	基於模組的認證失敗	錯誤訊息認證類型模組名稱	未在範圍之下註冊/配置模組存在不正確/無效的憑證 使用者已被鎖定/不在作用中	於範圍之下註冊/配置認證模組對認證模組輸入正確的/有效的憑證
269	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證已輸入無效的憑證。	輸入正確的密碼。
270	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證並未找到該使用者的使用者設定檔。	使用者並未存在於配置的資料儲存外掛程式中，因此請正確地配置該範圍/組織的資料儲存外掛程式。
271	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證該使用者不在作用中。	啓動使用者。
272	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證已超過失敗嘗試的最大數量。使用者已被鎖定。	請連絡系統管理員。
273	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證使用者帳號已過期。	請連絡系統管理員。
274	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證登入逾時。	重試登入。
275	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證認證模組遭到拒絕。	配置此模組或使用其他模組。

表 C–2 認證的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
276	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證已達到最大可允許階段作業數的限度。	登出階段作業或增加限度。
277	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證組織/範圍不存在。	使用有效的組織/範圍。
278	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證組織/範圍不在作用中。	啓動組織/範圍。
279	INFO	認證失敗	錯誤訊息認證類型模組名稱	基於模組的認證無法建立階段作業。	請確保已配置階段作業服務，且並未達到最大階段作業數。
300	INFO	使用者登出成功	訊息	使用者已登出	
301	INFO	使用者由基於使用者的認證登出成功	訊息認證類型使用者名稱	使用者已登出	
302	INFO	使用者由基於角色的認證登出成功	訊息認證類型角色名稱	屬於此角色的使用者已登出	
303	INFO	使用者由基於服務的認證登出成功	訊息認證類型服務名稱	使用者登出範圍之下的一個已配置服務	
304	INFO	使用者由基於認證層級的認證登出成功	訊息認證類型認證層級值	使用者登出一或多個具有認證層級值大於或等於所指定認證層級的認證模組	
305	INFO	使用者由基於模組的認證登出成功	訊息認證類型模組名稱	使用者登出範圍之下的認證模組	

表 C–3 Access Manager 主控台的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	嘗試建立識別	識別名稱識別類型範圍名稱	按一下 [範圍建立] 頁中的 [建立] 按鈕。	
2	INFO	識別建立成功。	識別名稱識別類型範圍名稱	按一下 [範圍建立] 頁中的 [建立] 按鈕。	
3	SEVERE	識別建立失敗	識別名稱識別類型範圍名稱錯誤訊息	無法於範圍之下建立識別。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
4	SEVERE	識別建立失敗	識別名稱識別類型範圍名稱錯誤訊息	由於資料存放區錯誤，因此無法於範圍之下建立識別。	如需更多資訊，請於資料存放區記錄下進行查詢。
11	INFO	嘗試搜尋識別	基底範圍識別類型搜尋式樣搜尋大小限制搜尋時間限制	按一下識別搜尋檢視中的 [搜尋] 按鈕。	
12	INFO	搜尋識別成功	基底範圍識別類型搜尋式樣搜尋大小限制搜尋時間限制	按一下識別搜尋檢視中的 [搜尋] 按鈕。	
13	SEVERE	搜尋識別失敗	識別名稱識別類型範圍名稱錯誤訊息	無法執行範圍下之識別的搜尋作業。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
14	SEVERE	搜尋識別失敗	識別名稱識別類型範圍名稱錯誤訊息	由於資料存放區錯誤，因此無法執行範圍下之識別的搜尋作業。	如需更多資訊，請於資料存放區記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
21	INFO	嘗試讀取識別的特性值	識別名稱特性名稱	檢視 [識別設定檔檢視]。	
22	INFO	識別的特性值讀取成功	識別名稱特性名稱	檢視 [識別設定檔檢視]。	
23	SEVERE	識別的特性值讀取失敗	識別名稱特性名稱錯誤訊息	無法讀取識別的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
24	SEVERE	識別的特性值讀取失敗	識別名稱特性名稱錯誤訊息	由於資料存放區錯誤，因此無法讀取識別的特性值。	如需更多資訊，請於資料存放區記錄下進行查詢。
25	SEVERE	識別的特性值讀取失敗	識別名稱特性名稱錯誤訊息	由於異常服務管理員 API，因此無法讀取識別的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
31	INFO	嘗試修改識別的特性值	識別名稱特性名稱	按一下識別設定檔檢視中的 [儲存] 按鈕。	
32	INFO	識別的特性值修改成功	識別名稱特性名稱	按一下識別設定檔檢視中的 [儲存] 按鈕。	
33	SEVERE	識別的特性值修改失敗	識別名稱特性名稱錯誤訊息	無法修改識別的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
34	SEVERE	識別的特性值修改失敗	識別名稱特性名稱錯誤訊息	由於資料存放區錯誤，因此無法修改識別的特性值。	如需更多資訊，請於資料存放區記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
41	INFO	嘗試刪除識別	範圍名稱將要刪除的識別名稱	按一下識別搜尋檢視中的 [刪除] 按鈕。	
42	INFO	識別刪除成功	範圍名稱將要刪除的識別名稱	按一下識別搜尋檢視中的 [刪除] 按鈕。	
43	SEVERE	識別刪除失敗	範圍名稱將要刪除的識別名稱錯誤訊息	無法刪除識別。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
44	SEVERE	識別刪除失敗	範圍名稱將要刪除的識別名稱錯誤訊息	由於資料存放區錯誤，因此無法刪除識別。	如需更多資訊，請於資料存放區記錄下進行查詢。
51	INFO	嘗試讀取識別的成員身份資訊	識別名稱成員身份類型	檢視是識別的成員身份頁。	
52	INFO	讀取識別的成員身份資訊成功	識別名稱成員身份類型	檢視是識別的成員身份頁。	
53	SEVERE	讀取識別的成員身份資訊失敗。	識別名稱成員身份識別類型錯誤訊息	無法讀取識別的成員身份資訊。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
54	SEVERE	讀取識別的成員身份資訊失敗。	識別名稱成員身份識別類型錯誤訊息	由於資料存放區錯誤，因此無法讀取識別的成員身份資訊。	如需更多資訊，請於資料存放區記錄下進行查詢。
61	INFO	嘗試讀取識別的成員資訊	識別名稱成員識別類型	檢視識別的成員頁面。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
62	INFO	讀取識別的成員資訊成功	識別名稱成員識別類型	檢視識別的成員頁面。	
63	SEVERE	讀取識別的成員資訊失敗。	識別名稱成員識別類型錯誤訊息	無法讀取識別的成員資訊。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
64	SEVERE	讀取識別的成員資訊失敗。	識別名稱成員識別類型錯誤訊息	由於資料存放區錯誤，因此無法讀取識別的成員資訊。	如需更多資訊，請於資料存放區記錄下進行查詢。
71	INFO	嘗試對識別新增成員	識別名稱將要新增的識別名稱。	選取要新增至識別的成員。	
72	INFO	對識別新增成員成功	識別名稱新增的識別名稱。	選取要新增至識別的成員。	
73	SEVERE	對識別新增成員失敗。	識別名稱將要新增的識別名稱。錯誤訊息	無法對識別新增成員。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
74	SEVERE	對識別新增成員失敗。	識別名稱將要新增的識別名稱。錯誤訊息	由於資料存放區錯誤，因此無法對識別新增成員。	如需更多資訊，請於資料存放區記錄下進行查詢。
81	INFO	嘗試由識別移除成員	識別名稱將要移除的識別名稱。	選取將要由識別移除的成員。	
82	INFO	由識別移除的成員成功。	識別名稱移除的識別名稱。	選取將要由識別移除的成員。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
83	SEVERE	對識別移除成員失敗。	識別名稱將要移除的識別名稱。錯誤訊息	無法由識別移除成員。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
84	SEVERE	由識別移除成員失敗。	識別名稱將要移除的識別名稱。錯誤訊息	由於資料存放區錯誤，因此無法對識別移除成員。	如需更多資訊，請於資料存放區記錄下進行查詢。
91	INFO	嘗試讀取識別之所指定的服務名稱	識別名稱	按一下識別之 [服務指定檢視] 中的 [新增] 按鈕。	
92	INFO	讀取識別之所指定的服務名稱成功	識別名稱	按一下識別之 [服務指定檢視] 中的 [新增] 按鈕。	
93	SEVERE	讀取識別之所指定的服務名稱失敗	識別名稱錯誤訊息	無法讀取識別之所指定的服務名稱。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
94	SEVERE	讀取識別之所指定的服務名稱失敗	識別名稱錯誤訊息	由於資料存放區錯誤，因此無法讀取識別之已指定服務名稱。	如需更多資訊，請於資料存放區記錄下進行查詢。
101	INFO	嘗試讀取識別之可指定的服務名稱	識別名稱	檢視識別的服務頁面。	
102	INFO	讀取識別之可指定的服務名稱成功	識別名稱	檢視識別的服務頁面。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
103	SEVERE	讀取識別之可指定的服務名稱失敗。	識別名稱錯誤訊息	無法讀取識別之可指定的服務名稱。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
104	SEVERE	讀取識別之可指定的服務名稱失敗。	識別名稱錯誤訊息	由於資料存放區錯誤，因此無法讀取識別之可指定的服務名稱。	如需更多資訊，請於資料存放區記錄下進行查詢。
111	INFO	嘗試對識別指定服務	識別名稱服務名稱	按一下識別之 [服務檢視] 的 [新增] 按鈕。	
112	INFO	識別的服務指定成功	識別名稱服務名稱	按一下識別之 [服務檢視] 的 [新增] 按鈕。	
113	SEVERE	識別的服務指定失敗。	識別名稱服務名稱錯誤訊息	無法對識別指定服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
114	SEVERE	識別的服務指定失敗。	識別名稱服務名稱錯誤訊息	由於資料存放區錯誤，因此無法對識別指定成員。	如需更多資訊，請於資料存放區記錄下進行查詢。
121	INFO	嘗試由識別解除指定服務	識別名稱服務名稱	按一下識別之 [服務檢視] 中的 [移除] 按鈕。	
122	INFO	對識別解除指定服務成功	識別名稱服務名稱	按一下識別之 [服務檢視] 中的 [移除] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
123	SEVERE	由識別解除指定服務失敗。	識別名稱服務名稱錯誤訊息	無法由識別解除指定服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
124	SEVERE	由識別解除指定服務失敗。	識別名稱服務名稱錯誤訊息	由於資料存放區錯誤，因此無法由識別解除指定服務。	如需更多資訊，請於資料存放區記錄下進行查詢。
131	INFO	嘗試讀取識別的服務特性值	識別名稱服務名稱	檢視識別的服務設定檔檢視。	
132	INFO	識別的服務特性值讀取成功	識別名稱服務名稱	檢視識別的服務設定檔檢視。	
133	SEVERE	識別的服務特性值讀取失敗。	識別名稱服務名稱錯誤訊息	無法讀取識別的服務特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
134	SEVERE	識別的服務特性值讀取失敗。	識別名稱服務名稱錯誤訊息	由於資料存放區錯誤，因此無法讀取識別的服務特性值。	如需更多資訊，請於資料存放區記錄下進行查詢。
141	INFO	嘗試將服務特性值寫入識別	識別名稱服務名稱	按一下識別之 [服務設定檔檢視] 中的 [儲存] 按鈕。	
142	INFO	對識別服務特性值寫入成功	識別名稱服務名稱	按一下識別之 [服務設定檔檢視] 中的 [儲存] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
143	SEVERE	對識別的服務特性值寫入失敗。	識別名稱服務名稱錯誤訊息	無法將服務特性值寫入識別。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
144	SEVERE	對識別的服務特性值寫入失敗。	識別名稱服務名稱錯誤訊息	由於資料存放區錯誤，因此無法將服務特性值寫入識別。	如需更多資訊，請於資料存放區記錄下進行查詢。
201	INFO	嘗試讀取所有全域服務預設特性值	服務的名稱	檢視一個服務的全域配置檢視。	
202	INFO	讀取所有全域服務預設特性值成功	服務的名稱	檢視一個服務的全域配置檢視。	
203	INFO	嘗試讀取全域服務預設特性值	服務名稱特性名稱	檢視一個服務的全域配置檢視。	
204	INFO	讀取全域服務預設特性值成功	服務名稱特性名稱	檢視一個服務的全域配置檢視。	
205	INFO	全域服務預設特性值讀取失敗	服務名稱特性名稱	檢視一個服務的全域配置檢視。	如需更多資訊，請於服務管理記錄下進行查詢。
211	INFO	嘗試寫入全域服務預設特性值	服務名稱特性名稱	按一下服務之 [全域配置檢視] 中的 [儲存] 按鈕。	
212	INFO	全域服務預設特性值寫入成功	服務名稱特性名稱	按一下服務之 [全域配置檢視] 中的 [儲存] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
213	SEVERE	全域服務預設特性值寫入失敗。	服務名稱特性名稱錯誤訊息	無法寫入全域服務預設特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
214	SEVERE	全域服務預設特性值寫入失敗。	服務名稱特性名稱錯誤訊息	由於服務管理錯誤，因此無法寫入服務預設特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
221	INFO	嘗試取得子配置名稱	服務名稱基底全域子配置名稱	檢視一個其服務具有子模式的全域服務檢視。	
222	INFO	全域子配置名稱讀取成功	服務名稱基底全域子配置名稱	檢視一個其服務具有子模式的全域服務檢視。	
223	SEVERE	全域子配置名稱讀取失敗。	服務名稱基底全域子配置名稱錯誤訊息	無法取得全域子配置名稱。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
224	SEVERE	全域子配置名稱讀取失敗。	服務名稱基底全域子配置名稱錯誤訊息	由於服務管理錯誤，無法取得全域子配置名稱。	如需更多資訊，請於服務管理記錄下進行查詢。
231	INFO	嘗試刪除子配置	服務名稱基底全域子配置名稱將要刪除之子配置名稱	按一下全域服務設定檔檢視中的 [刪除選取的] 按鈕。	
232	INFO	子配置刪除成功	服務名稱基底全域子配置名稱將要刪除之子配置名稱	按一下全域服務設定檔檢視中的 [刪除選取的] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
233	SEVERE	子配置刪除失敗。	服務名稱基底全域子配置名稱將要刪除的子配置名稱錯誤訊息	無法刪除子配置。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
234	SEVERE	子配置刪除失敗。	服務名稱基底全域子配置名稱將要刪除的子配置名稱錯誤訊息	由於服務管理錯誤，無法刪除子配置。	如需更多資訊，請於服務管理記錄下進行查詢。
241	INFO	嘗試建立子配置	服務名稱基底全域子配置名稱將要建立的子配置名稱將要建立的子模式名稱	按一下建立子配置檢視中的 [新增] 按鈕。	
242	INFO	子配置建立成功	服務名稱基底全域子配置名稱將要建立的子配置名稱將要建立的子模式名稱	按一下建立子配置檢視中的 [新增] 按鈕。	
243	SEVERE	子配置建立失敗。	服務名稱基底全域子配置名稱將要建立的子配置名稱將要建立的子模式名稱錯誤訊息	無法建立子配置。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
244	SEVERE	子配置建立失敗。	服務名稱基底全域子配置名稱將要建立的子配置名稱將要建立的子模式名稱錯誤訊息	由於服務管理錯誤，無法建立子配置。	如需更多資訊，請於服務管理記錄下進行查詢。
251	INFO	子配置特性值讀取成功	服務名稱子配置名稱	檢視子配置設定檔檢視。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
261	INFO	嘗試寫入子配置特性值	服務名稱子配置名稱	按一下子配置設定檔檢視中的 [儲存] 按鈕。	
262	INFO	子配置特性值寫入成功	服務名稱子配置名稱	按一下子配置設定檔檢視中的 [儲存] 按鈕。	
263	SEVERE	子配置特性值寫入失敗。	服務名稱子配置名稱錯誤訊息	無法寫入子配置特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
264	SEVERE	子配置特性值寫入失敗。	服務名稱子配置名稱錯誤訊息	由於服務管理錯誤，因此無法寫入子配置特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
301	INFO	嘗試取得範圍下的策略名稱。	範圍名稱	檢視策略主頁。	
302	INFO	取得範圍下的策略名稱成功	範圍名稱	檢視策略主頁。	
303	SEVERE	取得範圍下的策略名稱失敗。	範圍名稱錯誤訊息	無法取得範圍下的策略名稱。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於策略記錄下進行查詢。
304	SEVERE	取得範圍下的策略名稱失敗。	範圍名稱錯誤訊息	由於策略 SDK 相關的錯誤，因此無法取得範圍下的策略名稱。	如需更多資訊，請於策略記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
311	INFO	嘗試建立範圍下的策略。	範圍名稱策略名稱	按一下策略建立頁中的 [新建] 按鈕。	
312	INFO	策略建立成功	範圍名稱策略名稱	按一下策略建立頁中的 [新建] 按鈕。	
313	SEVERE	策略建立失敗。	範圍名稱策略名稱錯誤訊息	無法建立範圍下的策略。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於策略記錄下進行查詢。
314	SEVERE	策略建立失敗。	範圍名稱策略名稱錯誤訊息	由於策略 SDK 相關的錯誤，因此無法建立範圍下的策略。	如需更多資訊，請於策略記錄下進行查詢。
321	INFO	嘗試修改策略。	範圍名稱策略名稱	按一下策略設定檔頁中的 [儲存] 按鈕。	
322	INFO	策略修改成功	範圍名稱策略名稱	按一下策略設定檔頁中的 [儲存] 按鈕。	
323	SEVERE	策略修改失敗。	範圍名稱策略名稱錯誤訊息	無法修改範圍下的策略。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於策略記錄下進行查詢。
324	SEVERE	策略修改失敗。	範圍名稱策略名稱錯誤訊息	由於策略 SDK 相關的錯誤，因此無法修改策略。	如需更多資訊，請於策略記錄下進行查詢。
331	INFO	嘗試刪除策略。	範圍名稱策略名稱	按一下策略主頁中的 [刪除] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
332	INFO	策略刪除成功	範圍名稱策略名稱	按一下策略主頁中的 [刪除] 按鈕。	
333	SEVERE	策略刪除失敗。	範圍名稱策略名稱錯誤訊息	無法刪除策略。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於策略記錄下進行查詢。
334	SEVERE	策略刪除失敗。	範圍名稱策略名稱錯誤訊息	由於策略 SDK 相關的錯誤，因此無法刪除策略。	如需更多資訊，請於策略記錄下進行查詢。
401	INFO	嘗試取得範圍名稱	父系範圍名稱	檢視範圍主頁。	
402	INFO	成功取得範圍名稱。	父系範圍名稱	檢視範圍主頁。	
403	SEVERE	取得範圍名稱失敗。	父系範圍名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得範圍名稱。	如需更多資訊，請於服務管理記錄下進行查詢。
411	INFO	嘗試建立範圍。	父系範圍名稱新的範圍名稱	按一下建立範圍頁中的 [新建] 按鈕。	
412	INFO	範圍建立成功。	父系範圍名稱新的範圍名稱	按一下建立範圍頁中的 [新建] 按鈕。	
413	SEVERE	範圍建立失敗。	父系範圍名稱新的範圍名稱錯誤訊息	由於服務管理 SDK 異常，因此無法建立新的範圍。	如需更多資訊，請於服務管理記錄下進行查詢。
421	INFO	嘗試刪除範圍	父系範圍名稱要刪除的範圍名稱	按一下範圍主頁中的 [刪除] 按鈕。	
422	INFO	範圍刪除成功。	父系範圍名稱要刪除的範圍名稱	按一下範圍主頁中的 [刪除] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
423	SEVERE	範圍刪除失敗。	父系範圍名稱 要刪除的範圍名稱 錯誤訊息	由於服務管理 SDK 異常，因此無法刪除範圍。	如需更多資訊，請於服務管理記錄下進行查詢。
431	INFO	嘗試取得範圍的特性值	範圍名稱	檢視範圍設定檔頁。	
432	INFO	取得範圍的特性值成功。	範圍名稱	檢視範圍設定檔頁。	
433	SEVERE	取得範圍的特性值失敗。	範圍名稱 錯誤訊息	由於服務管理 SDK 異常，因此無法取得範圍的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
441	INFO	嘗試修改範圍設定檔	範圍名稱	按一下範圍設定檔頁中的 [儲存] 按鈕。	
442	INFO	範圍設定檔修改成功。	範圍名稱	按一下範圍設定檔頁中的 [儲存] 按鈕。	
443	SEVERE	範圍設定檔修改失敗。	範圍名稱 錯誤訊息	由於服務管理 SDK 異常，因此無法修改範圍設定檔。	如需更多資訊，請於服務管理記錄下進行查詢。
501	INFO	嘗試於範圍下取得委託主旨	範圍名稱 搜尋樣式	檢視委託主頁。	
502	INFO	於範圍下取得委託主旨成功。	範圍名稱 搜尋樣式	檢視委託主頁。	
503	SEVERE	於範圍下取得委託主旨失敗。	範圍名稱 搜尋式樣 錯誤訊息	無法取得委託主旨。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於委託管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
504	SEVERE	於範圍下取得委託主旨失敗。	範圍名稱搜尋式樣錯誤訊息	由於委託管理 SDK 相關的錯誤，因此無法取得委託主旨。	如需更多資訊，請於委託管理記錄下進行查詢。
511	INFO	嘗試取得委託主旨的權限。	範圍名稱委託主旨的 *ID*	檢視委託主旨設定檔頁面。	
512	INFO	取得委託主旨的權限成功。	範圍名稱委託主旨的 *ID*	檢視委託主旨設定檔頁面。	
513	SEVERE	取得委託主旨的權限失敗。	範圍名稱委託主旨的 *ID* 錯誤訊息	無法取得委託主旨的權限。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於委託管理記錄下進行查詢。
514	SEVERE	取得委託主旨的權限失敗。	範圍名稱委託主旨的 *ID* 錯誤訊息	由於委託管理 SDK 相關的錯誤，因此無法取得委託主旨的權限。	如需更多資訊，請於委託管理記錄下進行查詢。
521	INFO	嘗試修改委託權限	範圍名稱委託權限 *ID* 主旨的 *ID*	按一下委託主旨設定檔頁中的 [儲存] 按鈕。	
522	INFO	委託權限修改成功。	範圍名稱委託權限 *ID* 主旨的 *ID*	按一下委託主旨設定檔頁中的 [儲存] 按鈕。	
523	SEVERE	委託權限修改失敗。	範圍名稱委託權限 *ID* 主旨的 *ID* 錯誤訊息	無法修改委託權限。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於委託管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
524	SEVERE	委託權限修改失敗。	範圍名稱委託權限 *ID* 主旨的 *ID* 錯誤訊息	由於委託管理 SDK 相關的錯誤，因此無法修改委託權限。	如需更多資訊，請於委託管理記錄下進行查詢。
601	INFO	嘗試取得資料存放區名稱	範圍名稱	檢視資料存放區主頁。	
602	INFO	取得資料存放區名稱成功。	範圍名稱	檢視資料存放區主頁。	
603	SEVERE	取得資料存放區名稱失敗。	範圍名稱錯誤訊息	無法取得資料存放區名稱。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
604	SEVERE	取得資料存放區名稱失敗。	範圍名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得資料存放區名稱。	如需更多資訊，請於服務管理記錄下進行查詢。
611	INFO	嘗試取得識別儲存庫的特性值	範圍名稱識別儲存庫名稱	檢視資料存放區設定檔頁面。	
612	INFO	取得資料存放區的特性值成功。	範圍名稱識別儲存庫名稱	檢視資料存放區設定檔頁面。	
613	SEVERE	取得資料存放區的特性值失敗。	範圍名稱識別儲存庫名稱錯誤訊息	無法取得識別儲存庫的特性值其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
614	SEVERE	取得資料存放區的特性值失敗。	範圍名稱識別儲存庫名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得資料存放區的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
621	INFO	嘗試建立識別儲存庫	範圍名稱識別儲存庫名稱識別儲存庫類型	按一下資料存放區建立頁中的 [新建] 按鈕。	
622	INFO	資料存放區建立成功。	範圍名稱識別儲存庫名稱識別儲存庫類型	按一下資料存放區建立頁中的 [新建] 按鈕。	
623	SEVERE	資料存放區建立失敗。	範圍名稱識別儲存庫名稱識別儲存庫類型錯誤訊息	無法建立識別儲存庫。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
624	SEVERE	資料存放區建立失敗。	範圍名稱識別儲存庫名稱識別儲存庫類型錯誤訊息	由於服務管理 SDK 異常，因此無法建立資料存放區。	如需更多資訊，請於服務管理記錄下進行查詢。
631	INFO	嘗試刪除識別儲存庫	範圍名稱識別儲存庫名稱	按一下資料存放區主頁中的 [刪除] 按鈕。	
632	INFO	資料存放區刪除成功。	範圍名稱識別儲存庫名稱	按一下資料存放區主頁中的 [刪除] 按鈕。	
633	SEVERE	資料存放區刪除失敗。	範圍名稱識別儲存庫名稱錯誤訊息	無法刪除識別儲存庫。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
634	SEVERE	刪除資料存放區失敗。	範圍名稱識別儲存庫名稱錯誤訊息	由於服務管理 SDK 異常，因此無法刪除資料存放區。	如需更多資訊，請於服務管理記錄下進行查詢。
641	INFO	嘗試修改識別儲存庫	範圍名稱識別儲存庫名稱	按一下資料存放區設定檔頁中的 [儲存] 按鈕。	
642	INFO	資料存放區修改成功。	範圍名稱識別儲存庫名稱	按一下資料存放區設定檔頁中的 [儲存] 按鈕。	
643	SEVERE	資料存放區修改失敗。	範圍名稱識別儲存庫名稱錯誤訊息	無法修改識別儲存庫。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
644	SEVERE	修改資料存放區失敗。	範圍名稱識別儲存庫名稱錯誤訊息	由於服務管理 SDK 異常，因此無法修改資料存放區。	如需更多資訊，請於服務管理記錄下進行查詢。
701	INFO	嘗試取得已指定的範圍服務	範圍名稱	檢視範圍服務主頁。	
702	INFO	取得已指定的範圍服務成功。	範圍名稱	檢視範圍服務主頁。	
703	SEVERE	取得已指定的範圍服務失敗。	範圍名稱錯誤訊息	由於認證配置異常，因此無法取得已指定的範圍服務。	如需更多資訊，請於認證記錄下進行查詢。
704	SEVERE	取得已指定的範圍服務失敗。	範圍名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得已指定的範圍服務。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
705	SEVERE	取得已指定的範圍服務失敗。	範圍名稱錯誤訊息	由於資料存放區 SDK 異常，因此無法取得已指定的範圍服務。	如需更多資訊，請於服務管理記錄下進行查詢。
706	SEVERE	取得已指定的範圍服務失敗。	範圍名稱錯誤訊息	無法取得已指定的範圍服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
711	INFO	嘗試取得可指定的範圍服務	範圍名稱	檢視範圍服務主頁。	
712	INFO	取得可指定的範圍服務成功。	範圍名稱	檢視範圍服務主頁。	
713	SEVERE	取得可指定的範圍服務失敗。	範圍名稱錯誤訊息	由於認證配置異常，因此無法取得可指定的範圍服務。	如需更多資訊，請於認證記錄下進行查詢。
714	SEVERE	取得可指定的範圍服務失敗。	範圍名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得可指定的範圍服務。	如需更多資訊，請於服務管理記錄下進行查詢。
715	SEVERE	取得可指定的範圍服務失敗。	範圍名稱錯誤訊息	由於 ID 儲存庫管理 SDK 異常，因此無法取得可指定的範圍服務。	如需更多資訊，請於 ID 儲存庫管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
716	SEVERE	取得可指定的範圍服務失敗。	範圍名稱錯誤訊息	無法取得可指定的範圍服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
721	INFO	嘗試由範圍取消指定服務。	範圍名稱服務名稱	按一下範圍服務頁中的 [取消指定] 按鈕。	
722	INFO	由範圍取消指定服務成功。	範圍名稱服務名稱	按一下範圍服務頁中的 [取消指定] 按鈕。	
723	SEVERE	由範圍取消指定服務失敗。	範圍名稱服務名稱錯誤訊息	由於服務管理 SDK 異常，因此無法由範圍取消指定服務。	如需更多資訊，請於服務管理記錄下進行查詢。
725	SEVERE	由範圍取消指定服務失敗。	範圍名稱服務名稱錯誤訊息	無法由範圍取消指定服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區管理記錄下進行查詢。
724	SEVERE	由範圍取消指定服務失敗。	範圍名稱服務名稱錯誤訊息	由於資料存放區管理 SDK 異常，因此無法由範圍取消指定服務。	如需更多資訊，請於資料存放區管理記錄下進行查詢。
731	INFO	嘗試對範圍指定服務	範圍名稱服務名稱	按一下範圍服務頁中的 [指定] 按鈕。	
732	INFO	對範圍的服務指定成功。	範圍名稱服務名稱	按一下範圍服務頁中的 [指定] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
733	SEVERE	對範圍的服務指定失敗。	範圍名稱服務名稱錯誤訊息	由於服務管理 SDK 異常，因此無法對範圍指定服務。	如需更多資訊，請於服務管理記錄下進行查詢。
734	SEVERE	對範圍的服務指定失敗。	範圍名稱服務名稱錯誤訊息	無法對範圍指定服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
735	SEVERE	對範圍的服務指定失敗。	範圍名稱服務名稱錯誤訊息	由於資料存放區 SDK 異常，因此無法對範圍指定服務。	如需更多資訊，請於服務管理記錄下進行查詢。
741	INFO	嘗試取得範圍中的服務特性值	範圍名稱服務名稱特性模式名稱	檢視範圍服務設定檔頁面。	
742	INFO	取得範圍下的服務特性值成功。	範圍名稱服務名稱特性模式名稱	檢視範圍服務設定檔頁面。	
743	SEVERE	取得範圍下的服務特性值失敗。	範圍名稱服務名稱特性模式名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得服務的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
744	INFO	取得範圍下的服務特性值失敗。	範圍名稱服務名稱特性模式名稱錯誤訊息	由於資料存放區 SDK 異常，因此無法取得服務的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
745	SEVERE	取得範圍下的服務特性值失敗。	範圍名稱服務名稱特性模式名稱錯誤訊息	無法取得服務的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
751	INFO	嘗試修改範圍中的服務特性值	範圍名稱服務名稱	按一下範圍服務設定檔頁中的 [儲存] 按鈕。	
752	INFO	於範圍下的服務特性值修改成功。	範圍名稱服務名稱	按一下範圍服務設定檔頁中的 [儲存] 按鈕。	
753	SEVERE	於範圍下的服務特性值修改失敗。	範圍名稱服務名稱錯誤訊息	由於服務管理 SDK 異常，因此無法修改服務的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
754	SEVERE	於範圍下的服務特性值修改失敗。	範圍名稱服務名稱錯誤訊息	由於資料存放區錯誤，因此無法修改服務的特性值。	如需更多資訊，請於資料存放區記錄下進行查詢。
755	SEVERE	於範圍下的服務特性值修改失敗。	範圍名稱服務名稱錯誤訊息	無法修改服務的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於資料存放區記錄下進行查詢。
801	INFO	嘗試取得認證類型		檢視認證設定檔頁。	
802	INFO	認證類型取得成功。		檢視認證設定檔頁。	
803	SEVERE	認證類型取得失敗。	錯誤訊息	由於認證配置 SDK 異常，因此無法取得認證類型。	如需更多資訊，請於認證管理記錄下進行查詢。
811	INFO	嘗試於範圍之下取得認證實例	範圍名稱	檢視認證設定檔頁。	
812	INFO	於範圍之下的認證實例取得成功。	範圍名稱	檢視認證設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
813	SEVERE	於範圍之下的認證實例取得失敗。	範圍名稱錯誤訊息	由於認證配置 SDK 異常，因此無法取得認證實例。	如需更多資訊，請於認證管理記錄下進行查詢。
821	INFO	嘗試於範圍之下移除認證實例	範圍名稱認證實例名稱	檢視認證設定檔頁。	
822	INFO	於範圍之下的認證實例移除成功。	範圍名稱認證實例名稱	檢視認證設定檔頁。	
823	SEVERE	於範圍之下的認證實例移除失敗。	範圍名稱認證實例名稱錯誤訊息	由於認證配置 SDK 異常，因此無法移除認證實例。	如需更多資訊，請於認證管理記錄下進行查詢。
831	INFO	嘗試於範圍之下建立認證實例	範圍名稱認證實例名稱認證實例類型	按一下認證建立頁中的 [新建] 按鈕。	
832	INFO	於範圍之下的認證實例建立成功。	範圍名稱認證實例名稱認證實例類型	按一下認證建立頁中的 [新建] 按鈕。	
833	SEVERE	於範圍之下的認證實例建立失敗。	範圍名稱認證實例名稱認證實例類型錯誤訊息	由於認證配置 SDK 異常，因此無法建立認證實例。	如需更多資訊，請於認證配置記錄下進行查詢。
841	INFO	嘗試修改認證實例	範圍名稱認證服務名稱	按一下認證設定檔頁中的 [儲存] 按鈕。	
842	INFO	認證實例的修改成功。	範圍名稱認證服務名稱	按一下認證設定檔頁中的 [儲存] 按鈕。	
843	SEVERE	認證實例的修改失敗。	範圍名稱認證服務名稱錯誤訊息	由於服務管理 SDK 異常，因此無法修改認證實例。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
844	SEVERE	認證實例的修改失敗。	範圍名稱認證服務名稱錯誤訊息	無法修改認證實例。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
851	INFO	嘗試取得認證實例設定檔	範圍名稱認證實例名稱	檢視認證實例設定檔頁。	
852	INFO	認證實例設定檔的取得成功。	範圍名稱認證實例名稱	檢視認證實例設定檔頁。	
853	SEVERE	認證實例設定檔的取得失敗。	範圍名稱認證實例名稱錯誤訊息	由於認證配置 SDK 異常，因此無法取得認證實例設定檔。	如需更多資訊，請於認證管理記錄下進行查詢。
861	INFO	嘗試修改認證實例設定檔	範圍名稱認證實例名稱	按一下認證實例設定檔頁中的 [儲存] 按鈕。	
862	INFO	認證實例設定檔的修改成功。	範圍名稱認證實例名稱	按一下認證實例設定檔頁中的 [儲存] 按鈕。	
863	SEVERE	認證實例設定檔的修改失敗。	範圍名稱認證實例名稱錯誤訊息	由於認證配置 SDK 異常，因此無法修改認證實例設定檔。	如需更多資訊，請於認證管理記錄下進行查詢。
864	SEVERE	認證實例設定檔的修改失敗。	範圍名稱認證實例名稱錯誤訊息	由於服務管理 SDK 異常，因此無法修改認證實例設定檔。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
864	SEVERE	認證實例設定檔的修改失敗。	範圍名稱認證實例名稱錯誤訊息	無法修改認證實例設定檔。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
871	INFO	嘗試於範圍之下取得認證設定檔	範圍名稱	檢視範圍頁面下的認證設定檔。	
872	INFO	於範圍之下認證設定檔取得成功。	範圍名稱	檢視範圍頁面下的認證設定檔。	
873	SEVERE	於範圍之下認證設定檔取得失敗。	範圍名稱錯誤訊息	由於服務管理 SDK 異常，因此無法於範圍之下取得認證設定檔。	如需更多資訊，請於服務管理記錄下進行查詢。
881	INFO	嘗試取得認證配置設定檔	範圍名稱認證配置名稱	檢視認證配置設定檔頁。	
882	INFO	取得認證配置設定檔成功。	範圍名稱認證配置名稱	檢視認證配置設定檔頁。	
883	SEVERE	取得認證配置設定檔失敗。	範圍名稱認證配置名稱錯誤訊息	無法取得認證配置設定檔。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
884	SEVERE	取得認證配置設定檔失敗。	範圍名稱認證配置名稱錯誤訊息	由於服務管理 SDK 異常，因此無法取得認證配置設定檔。	如需更多資訊，請於服務管理記錄下進行查詢。
885	SEVERE	取得認證配置設定檔失敗。	範圍名稱認證配置名稱錯誤訊息	由於認證配置 SDK 異常，因此無法取得認證配置設定檔。	如需更多資訊，請於認證配置記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
891	INFO	嘗試修改認證配置設定檔	範圍名稱認證配置名稱	按一下認證配置設定檔頁中的 [儲存] 按鈕。	
892	INFO	認證配置設定檔的修改成功。	範圍名稱認證配置名稱	按一下認證配置設定檔頁中的 [儲存] 按鈕。	
893	SEVERE	認證配置設定檔的修改失敗。	範圍名稱認證配置名稱錯誤訊息	無法修改認證配置設定檔。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
894	SEVERE	認證配置設定檔的修改失敗。	範圍名稱認證配置名稱錯誤訊息	由於服務管理 SDK 異常，因此無法修改認證配置設定檔。	如需更多資訊，請於服務管理記錄下進行查詢。
895	SEVERE	認證配置設定檔的修改失敗。	範圍名稱認證配置名稱錯誤訊息	由於認證配置 SDK 異常，因此無法修改認證配置設定檔。	如需更多資訊，請於認證配置記錄下進行查詢。
901	INFO	嘗試建立認證配置	範圍名稱認證配置名稱	按一下認證配置建立頁中的 [新建] 按鈕。	
902	INFO	認證配置的建立成功。	範圍名稱認證配置名稱	按一下認證配置建立頁中的 [新建] 按鈕。	
903	SEVERE	認證配置的建立失敗。	範圍名稱認證配置名稱錯誤訊息	無法建立認證配置。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
904	SEVERE	認證配置的建立失敗。	範圍名稱認證配置名稱錯誤訊息	由於服務管理 SDK 異常，因此無法建立認證配置。	如需更多資訊，請於服務管理記錄下進行查詢。
905	SEVERE	認證配置的建立失敗。	範圍名稱認證配置名稱錯誤訊息	由於認證配置 SDK 異常，因此無法建立認證配置。	如需更多資訊，請於認證配置記錄下進行查詢。
1001	INFO	嘗試取得實體描述元名稱。	搜尋式樣	檢視實體描述元主頁。	
1002	INFO	取得實體描述元名稱成功。	搜尋式樣	檢視實體描述元主頁。	
1003	SEVERE	取得實體描述元名稱失敗。	搜尋式樣錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得實體描述元名稱。	如需更多資訊，請於聯合記錄下進行查詢。
1011	INFO	嘗試建立實體描述元。	描述元名稱描述元類型	按一下實體描述元建立頁中的 [新建] 按鈕。	
1012	INFO	建立實體描述元成功	描述元名稱描述元類型	按一下實體描述元建立頁中的 [新建] 按鈕。	
1013	SEVERE	建立實體描述元失敗。	描述元名稱描述元類型錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法建立實體描述元。	如需更多資訊，請於聯合記錄下進行查詢。
10211	INFO	嘗試刪除實體描述元。	描述元名稱	按一下實體描述元主頁中的 [刪除] 按鈕。	
1022	INFO	刪除實體描述元成功	描述元名稱	按一下實體描述元主頁中的 [刪除] 按鈕。	
1023	SEVERE	刪除實體描述元失敗。	描述元名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法刪除實體描述元。	如需更多資訊，請於聯合記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
1031	INFO	嘗試取得一個附屬提供者實體描述元的特性值。	描述元名稱	檢視附屬提供者實體描述元設定檔頁。	
1032	INFO	取得一個附屬提供者實體描述元的特性值成功。	描述元名稱	檢視附屬提供者實體描述元設定檔頁。	
1033	SEVERE	取得一個附屬提供者實體描述元的特性值失敗。	描述元名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得一個附屬提供者實體描述元的特性值。	如需更多資訊，請於聯合記錄下進行查詢。
1041	INFO	嘗試修改一個附屬提供者實體描述元。	描述元名稱	按一下附屬提供者實體描述元設定檔頁的 [儲存] 按鈕。	
1042	INFO	附屬提供者實體描述元的修改成功。	描述元名稱	按一下附屬提供者實體描述元設定檔頁的 [儲存] 按鈕。	
1043	SEVERE	附屬提供者實體描述元的修改失敗。	描述元名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法修改附屬提供者實體描述元。	如需更多資訊，請於聯合記錄下進行查詢。
1044	SEVERE	附屬提供者實體描述元的修改失敗。	描述元名稱錯誤訊息	由於一或多個特性值之不正確的數字格式，因此無法修改附屬提供者實體描述元。	如需更多資訊，請於聯合記錄下進行查詢。
1051	INFO	嘗試取得一個實體描述元的特性值。	描述元名稱	檢視實體描述元設定檔頁。	
1052	INFO	取得實體描述元的特性值成功。	描述元名稱	檢視實體描述元設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
1053	SEVERE	取得實體描述元的特性值失敗。	描述元名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得一個實體描述元的特性值。	如需更多資訊，請於聯合記錄下進行查詢。
1061	INFO	嘗試修改實體描述元。	描述元名稱	按一下實體描述元設定檔頁的 [儲存] 按鈕。	
1062	INFO	實體描述元修改成功。	描述元名稱	按一下實體描述元設定檔頁的 [儲存] 按鈕。	
1063	SEVERE	實體描述元修改失敗。	描述元名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法修改實體描述元。	如需更多資訊，請於聯合記錄下進行查詢。
1101	INFO	嘗試取得認證網域名稱。	搜尋式樣	檢視認證網域主頁。	
1102	INFO	取得認證網域名稱成功。	搜尋式樣	檢視認證網域主頁。	
1103	SEVERE	取得認證網域名稱失敗。	搜尋式樣錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得認證網域名稱。	如需更多資訊，請於聯合記錄下進行查詢。
1111	INFO	嘗試建立認證網域	認證網域名稱	按一下認證網域建立頁中的 [新建] 按鈕。	
1112	INFO	認證網域建立成功。	認證網域名稱	按一下認證網域建立頁中的 [新建] 按鈕。	
1113	SEVERE	認證網域建立失敗。	認證網域名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法建立認證網域。	如需更多資訊，請於聯合記錄下進行查詢。
1121	INFO	嘗試刪除認證網域	認證網域名稱	按一下認證網域主頁中的 [建立] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
1122	INFO	認證網域刪除成功。	認證網域名稱	按一下認證網域主頁中的 [建立] 按鈕。	
1123	SEVERE	認證網域刪除失敗。	認證網域名稱 錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法刪除認證網域。	如需更多資訊，請於聯合記錄下進行查詢。
1131	INFO	嘗試取得認證網域特性值	認證網域名稱	檢視認證網域設定檔頁。	
1132	INFO	取得認證網域特性值成功。	認證網域名稱	檢視認證網域設定檔頁。	
1133	SEVERE	取得認證網域特性值失敗。	認證網域名稱 錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得認證網域特性值。	如需更多資訊，請於聯合記錄下進行查詢。
1141	INFO	嘗試修改認證網域	認證網域名稱	按一下認證網域設定檔頁中的 [儲存] 按鈕。	
1142	INFO	修改認證網域成功。	認證網域名稱	按一下認證網域設定檔頁中的 [儲存] 按鈕。	
1143	SEVERE	修改認證網域失敗。	認證網域名稱 錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法修改認證網域。	如需更多資訊，請於聯合記錄下進行查詢。
1151	INFO	嘗試取得所有提供者名稱		檢視認證網域設定檔頁。	
1152	INFO	取得所有提供者名稱成功。		檢視認證網域設定檔頁。	
1153	SEVERE	取得所有提供者名稱失敗。	錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得所有提供者名稱。	如需更多資訊，請於聯合記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
1161	INFO	嘗試取得認證網域下的提供者名稱	認證網域名稱	檢視認證網域設定檔頁。	
1162	INFO	取得認證網域下的提供者名稱成功。	認證網域名稱	檢視認證網域設定檔頁。	
1163	SEVERE	取得認證網域下的提供者名稱失敗。	認證網域名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得認證網域下的提供者名稱。	如需更多資訊，請於聯合記錄下進行查詢。
1171	INFO	嘗試對認證網域新增提供者	認證網域名稱提供者名稱	按一下提供者指定頁中的 [儲存] 按鈕。	
1172	INFO	對認證網域新增提供者成功。	認證網域名稱提供者名稱	按一下提供者指定頁中的 [儲存] 按鈕。	
1173	SEVERE	對認證網域新增提供者失敗。	認證網域名稱提供者名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法對認證網域新增提供者。	如需更多資訊，請於聯合記錄下進行查詢。
1181	INFO	嘗試由認證網域移除提供者	認證網域名稱提供者名稱	按一下提供者指定頁中的 [儲存] 按鈕。	
1182	INFO	由認證網域刪除提供者成功。	認證網域名稱提供者名稱	按一下提供者指定頁中的 [儲存] 按鈕。	
1183	SEVERE	由認證網域刪除提供者失敗。	認證網域名稱提供者名稱錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法由認證網域移除提供者。	如需更多資訊，請於聯合記錄下進行查詢。
1301	INFO	嘗試建立提供者	提供者名稱提供者角色提供者類型	按一下提供者指定頁中的 [儲存] 按鈕。	
1302	INFO	提供者建立成功。	提供者名稱提供者角色提供者類型	按一下提供者指定頁中的 [儲存] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
1303	SEVERE	提供者建立失敗。	提供者名稱提供者角色提供者類型錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法建立提供者。	如需更多資訊，請於聯合記錄下進行查詢。
1303	SEVERE	提供者建立失敗。	提供者名稱提供者角色提供者類型錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法建立提供者。	如需更多資訊，請於聯合記錄下進行查詢。
1304	SEVERE	提供者建立失敗。	提供者名稱提供者角色提供者類型錯誤訊息	因爲管理主控台找不到適當的方法來設定這個提供者的值，因此無法建立提供者。	這是一個 Web 應用程式錯誤。請連絡 Sun 支援以尋求協助。
1311	INFO	嘗試取得提供者的特性值	提供者名稱提供者角色提供者類型	檢視提供者設定檔頁。	
1312	INFO	取得提供者的特性值成功。	提供者名稱提供者角色提供者類型	檢視提供者設定檔頁。	
1321	INFO	嘗試取得提供者的控制器	提供者名稱提供者角色	檢視提供者設定檔頁。	
1322	INFO	取得提供者的控制器成功。	提供者名稱提供者角色	檢視提供者設定檔頁。	
1323	SEVERE	取得提供者的控制器失敗。	提供者名稱提供者角色錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得提供者的控制器。	如需更多資訊，請於聯合記錄下進行查詢。
1331	INFO	嘗試修改提供者。	提供者名稱提供者角色	按一下提供者設定檔頁中的 [儲存] 按鈕。	
1332	INFO	提供者修改成功。	提供者名稱提供者角色	按一下提供者設定檔頁中的 [儲存] 按鈕。	
1333	SEVERE	提供者修改失敗。	提供者名稱提供者角色錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法修改提供者。	如需更多資訊，請於聯合記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
1334	SEVERE	提供者修改失敗。	提供者名稱提供者角色錯誤訊息	因爲管理主控台找不到適當的方法來設定這個提供者的值，因此無法修改提供者。	這是一個 Web 應用程式錯誤。請連絡 Sun 支援以尋求協助。
1341	INFO	嘗試刪除提供者	提供者名稱提供者角色	按一下提供者設定檔頁中的 [刪除提供者] 按鈕。	
1342	INFO	提供者刪除成功。	提供者名稱提供者角色	按一下提供者設定檔頁中的 [刪除提供者] 按鈕。	
1343	SEVERE	提供者刪除失敗。	提供者名稱提供者角色錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法刪除提供者。	如需更多資訊，請於聯合記錄下進行查詢。
1351	INFO	嘗試取得未來的受信任提供者	提供者名稱提供者角色	檢視新增受信任提供者頁。	
1352	INFO	取得未來的受信任提供者成功。	提供者名稱提供者角色	檢視新增受信任提供者頁。	
1353	SEVERE	取得未來的受信任提供者失敗。	提供者名稱提供者角色錯誤訊息	由於聯合 SDK 相關的錯誤，因此無法取得未來的受信任提供者。	如需更多資訊，請於聯合記錄下進行查詢。
2001	INFO	嘗試取得服務模式之模式類型的特性值	服務名稱模式類型名稱特性模式名稱	檢視服務設定檔頁。	
2002	INFO	取得服務模式之模式類型的特性值成功。	服務名稱模式類型名稱特性模式名稱	檢視服務設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
2003	SEVERE	取得服務模式之模式類型的特性值失敗。	服務名稱模式類型名稱特性模式名稱錯誤訊息	無法取得服務模式之模式類型的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
2004	SEVERE	取得服務模式之模式類型的特性值失敗。	服務名稱模式類型名稱特性模式名稱錯誤訊息	由於服務管理 SDK 相關的錯誤，因此無法取得服務模式之模式類型的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
2005	INFO	取得服務模式之模式類型的特性值失敗。	服務名稱模式類型名稱特性模式名稱	檢視服務設定檔頁。	不需對此事件採取任何動作。控制台嘗試由服務取得一個模式，但模式不存在。
2011	INFO	嘗試取得服務模式的模式類型之特性模式的特性值	服務名稱模式類型名稱特性模式名稱	檢視服務設定檔頁。	
2012	INFO	取得服務模式的模式類型之特性模式的特性值成功。	服務名稱模式類型名稱特性模式名稱	檢視服務設定檔頁。	
2013	SEVERE	取得服務模式的模式類型之特性模式的特性值失敗。	服務名稱模式類型名稱特性模式名稱錯誤訊息	無法取得服務模式之模式類型的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
2014	SEVERE	取得服務模式的模式類型之特性模式的特性值失敗。	服務名稱模式類型名稱特性模式名稱錯誤訊息	由於服務管理 SDK 相關的錯誤，因此無法取得服務模式之模式類型的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
2021	INFO	嘗試修改服務模式的模式類型之特性模式的特性值	服務名稱模式類型名稱特性模式名稱	按一下服務設定檔頁中的 [儲存] 按鈕。	
2022	INFO	修改服務模式的模式類型之特性模式的特性值成功。	服務名稱模式類型名稱特性模式名稱	按一下服務設定檔頁中的 [儲存] 按鈕。	
2023	SEVERE	修改服務模式的模式類型之特性模式的特性值失敗。	服務名稱模式類型名稱特性模式名稱錯誤訊息	無法修改服務模式之模式類型的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於服務管理記錄下進行查詢。
2024	SEVERE	修改服務模式的模式類型之特性模式的特性值失敗。	服務名稱模式類型名稱特性模式名稱錯誤訊息	由於服務管理 SDK 相關的錯誤，因此無法修改服務模式之模式類型的特性值。	如需更多資訊，請於服務管理記錄下進行查詢。
2501	INFO	嘗試取得用戶端偵測服務的裝置名稱	設定檔名稱樣式名稱搜尋式樣	檢視用戶端設定檔頁。	
2502	INFO	取得用戶端偵測服務的裝置名稱成功。	設定檔名稱樣式名稱搜尋式樣	檢視用戶端設定檔頁。	
2511	INFO	嘗試刪除用戶端偵測服務中的用戶端	用戶端類型	按一下用戶端類型以刪除超連結頁面。	
2512	INFO	用戶端偵測服務中的用戶端刪除成功。	用戶端類型	按一下用戶端類型以刪除超連結頁面。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
2513	SEVERE	用戶端偵測服務中的用戶端刪除失敗。	用戶端類型錯誤訊息	由於用戶端偵測 SDK 相關的錯誤，因此無法刪除用戶端。	如需更多資訊，請於用戶端偵測管理記錄下進行查詢。
2521	INFO	嘗試建立用戶端偵測服務中的用戶端	用戶端類型	按一下用戶端建立頁中的 [新建] 按鈕。	
2522	INFO	用戶端偵測服務中的用戶端建立成功。	用戶端類型	按一下用戶端建立頁中的 [新建] 按鈕。	
2523	SEVERE	用戶端偵測服務中的用戶端建立失敗。	用戶端類型錯誤訊息	由於用戶端偵測 SDK 相關的錯誤，因此無法建立用戶端。	如需更多資訊，請於用戶端偵測管理記錄下進行查詢。
2524	INFO	用戶端偵測服務中的用戶端建立失敗。	用戶端類型錯誤訊息	由於用戶端類型無效，因此無法建立用戶端。	於建立之前，請再次檢查用戶端類型。
2531	INFO	嘗試建立用戶端偵測服務中的用戶端設定檔	用戶端類型分類	檢視用戶端設定檔頁。	
2532	INFO	用戶端偵測服務中的用戶端設定檔取得成功。	用戶端類型分類	檢視用戶端設定檔頁。	
2541	INFO	嘗試修改用戶端偵測服務中的用戶端設定檔	用戶端類型	按一下用戶端設定檔頁中的 [儲存] 按鈕。	
2542	INFO	用戶端偵測服務中的用戶端設定檔修改成功。	用戶端類型	按一下用戶端設定檔頁中的 [儲存] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
2543	SEVERE	用戶端偵測服務中的用戶端設定檔修改失敗。	用戶端類型錯誤訊息	由於用戶端偵測 SDK 相關的錯誤，因此無法修改用戶端設定檔。	如需更多資訊，請於用戶端偵測管理記錄下進行查詢。
3001	INFO	嘗試取得目前的階段作業	伺服器名稱搜尋式樣	檢視階段作業主頁。	
3002	INFO	取得目前的階段作業成功。	伺服器名稱搜尋式樣	檢視階段作業主頁。	
3003	SEVERE	取得目前的階段作業失敗。	伺服器名稱範圍名稱錯誤訊息	由於階段作業 SDK 異常，因此伺無法取得目前的階段作業。	如需更多資訊，請於階段作業管理記錄下進行查詢。
3011	INFO	嘗試使階段作業無效	伺服器名稱階段作業 *ID*	按一下階段作業主頁中的 [無效] 按鈕。	
3012	INFO	使階段作業無效成功。	伺服器名稱階段作業 *ID*	按一下階段作業主頁中的 [無效] 按鈕。	
3013	SEVERE	使階段作業無效失敗。	伺服器名稱階段作業 *ID* 錯誤訊息	由於階段作業 SDK 異常，因此伺無法使階段作業無效。	如需更多資訊，請於階段作業管理記錄下進行查詢。
10001	INFO	嘗試由組織搜尋容器	組織的 DN 搜尋式樣	按一下組織容器頁中的 [搜尋] 按鈕。	
10002	INFO	由組織搜尋容器成功。	組織的 DN 搜尋式樣	按一下組織容器頁中的 [搜尋] 按鈕。	
10003	SEVERE	由組織搜尋容器失敗。	組織的 DN 搜尋式樣錯誤訊息	無法搜尋容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10004	SEVERE	由組織搜尋容器失敗。	組織的 DN 搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10011	INFO	嘗試由一個容器搜尋容器	容器的 DN 搜尋式樣	按一下容器之子容器頁中的 [搜尋] 按鈕。	
10012	INFO	由一個容器搜尋容器成功。	容器的 DN 搜尋式樣	按一下容器之子容器頁中的 [搜尋] 按鈕。	
10013	SEVERE	由一個容器搜尋容器失敗。	容器的 DN 搜尋式樣錯誤訊息	無法搜尋容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10014	SEVERE	由一個容器搜尋容器失敗。	容器的 DN 搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10021	INFO	嘗試於組織下建立容器	組織的 DN 容器名稱	按一下容器建立頁中的 [新建] 按鈕。	
10022	INFO	於組織下建立容器成功。	組織的 DN 容器名稱	按一下容器建立頁中的 [新建] 按鈕。	
10023	SEVERE	於組織下建立容器失敗。	組織的 DN 容器名稱錯誤訊息	無法建立容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10024	SEVERE	於組織下建立容器失敗。	組織的 DN 容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10031	INFO	嘗試於容器下建立容器	容器的 DN 容器名稱	按一下容器建立頁中的 [新建] 按鈕。	
10032	INFO	容器之下建立容器成功。	容器的 DN 容器名稱	按一下容器建立頁中的 [新建] 按鈕。	
10033	SEVERE	容器之下建立容器失敗。	容器的 DN 容器名稱錯誤訊息	無法建立容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10034	SEVERE	容器之下建立容器失敗。	容器的 DN 容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10041	INFO	嘗試對容器取得已指定的服務	容器 DN	檢視容器服務設定檔頁面。	
10042	INFO	對容器取得已指定的服務成功。	容器 DN	檢視容器服務設定檔頁面。	
10043	SEVERE	對容器取得已指定的服務失敗。	容器 DN 錯誤訊息	無法取得對容器的指定服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10044	SEVERE	對容器取得已指定的服務失敗。	容器 DN 錯誤訊息	由於存取管理 SDK 異常，無法對容器取得已指定的服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10101	INFO	嘗試取得組織下的服務範本	組織 DN 服務名稱範本類型	檢視組織服務設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10102	INFO	取得組織下的服務範本成功。	組織 DN 服務名稱範本類型	檢視組織服務設定檔頁。	
10103	SEVERE	取得組織下的服務範本失敗。	組織 DN 服務名稱範本類型錯誤訊息	無法取得服務範本。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10104	SEVERE	取得組織下的服務範本失敗。	組織 DN 服務名稱範本類型錯誤訊息	由於存取管理 SDK 異常，無法取得服務範本。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10111	INFO	嘗試取得容器下的服務範本	容器 DN 服務名稱範本類型	檢視容器服務設定檔頁面。	
10112	INFO	取得容器下的服務範本成功。	容器 DN 服務名稱範本類型	檢視容器服務設定檔頁面。	
10113	SEVERE	取得容器下的服務範本失敗。	容器 DN 服務名稱範本類型錯誤訊息	無法取得服務範本。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10114	SEVERE	取得容器下的服務範本失敗。	容器 DN 服務名稱範本類型錯誤訊息	由於存取管理 SDK 異常，無法取得服務範本。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10121	INFO	嘗試刪除目錄物件	物件名稱	按一下物件主頁中的 [刪除] 按鈕。	
10122	INFO	目錄物件刪除成功。	物件名稱	按一下物件主頁中的 [刪除] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10123	SEVERE	目錄物件刪除失敗。	物件名稱錯誤訊息	無法刪除目錄物。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10124	SEVERE	目錄物件刪除失敗。	物件名稱錯誤訊息	由於存取管理 SDK 異常，無法刪除目錄物件。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10131	INFO	嘗試修改目錄物件	物件 DN	按一下物件設定檔頁。	
10132	INFO	目錄物件修改成功。	物件 DN	按一下物件設定檔頁。	
10133	SEVERE	目錄物件修改失敗。	物件 DN 錯誤訊息	由於存取管理 SDK 異常，無法修改目錄物件。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10141	INFO	嘗試由組織刪除服務範本	組織 DN 服務名稱	按一下組織服務頁中的 [取消指定] 按鈕。	
10142	INFO	由組織刪除服務成功。	組織 DN 服務名稱	按一下組織服務頁中的 [取消指定] 按鈕。	
10143	SEVERE	由組織刪除服務失敗。	組織 DN 服務名稱錯誤訊息	無法刪除服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10144	SEVERE	由組織刪除服務失敗。	組織 DN 服務名稱錯誤訊息	由於存取管理 SDK 異常，無法刪除服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10151	INFO	嘗試由容器刪除服務	容器 DN 服務名稱	按一下容器服務頁中的 [取消指定] 按鈕。	
10152	INFO	由容器刪除服務成功。	容器 DN 服務名稱	按一下容器服務頁中的 [取消指定] 按鈕。	
10153	SEVERE	由容器刪除服務失敗。	容器 DN 服務名稱錯誤訊息	無法刪除服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10154	SEVERE	由容器刪除服務失敗。	容器 DN 服務名稱錯誤訊息	由於存取管理 SDK 異常，無法刪除服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10201	INFO	嘗試搜尋組織下的群組容器	組織 DN 搜尋式樣	按一下組織群組容器頁中的 [搜尋] 按鈕。	
10202	INFO	組織下搜尋群組容器成功。	組織 DN 搜尋式樣	按一下組織群組容器頁中的 [搜尋] 按鈕。	
10203	SEVERE	組織下搜尋群組容器失敗。	組織 DN搜尋式樣錯誤訊息	無法搜尋群組容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10204	SEVERE	組織下搜尋群組容器失敗。	組織 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10211	INFO	嘗試搜尋容器下的群組容器	容器 DN 搜尋式樣	按一下容器之群組容器頁中的 [搜尋] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10212	INFO	容器下搜尋群組容器成功。	容器 DN 搜尋式樣	按一下容器之群組容器頁中的 [搜尋] 按鈕。	
10213	SEVERE	容器下搜尋群組容器失敗。	容器 DN搜尋式樣錯誤訊息	無法搜尋群組容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10214	SEVERE	容器下搜尋群組容器失敗。	容器 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10221	INFO	嘗試搜尋群組容器下的群組容器	群組容器 DN 搜尋式樣	按一下群組容器之群組容器頁中的 [搜尋] 按鈕。	
10222	INFO	群組容器下搜尋群組容器成功。	群組容器 DN 搜尋式樣	按一下群組容器之群組容器頁中的 [搜尋] 按鈕。	
10223	SEVERE	群組容器下搜尋群組容器失敗。	群組容器 DN搜尋式樣錯誤訊息	無法搜尋群組容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10224	SEVERE	群組容器下搜尋群組容器失敗。	群組容器 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10231	INFO	嘗試建立組織中的群組容器	組織 DN群組容器名稱	按一下群組容器建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10232	INFO	組織下建立群組容器成功。	組織 DN群組容器名稱	按一下群組容器建立頁中的 [新建] 按鈕。	
10233	SEVERE	組織下建立群組容器失敗。	組織 DN群組容器名稱錯誤訊息	無法建立群組容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10234	SEVERE	組織下建立群組容器失敗。	組織 DN群組容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10241	INFO	嘗試建立容器中的群組容器	容器 DN群組容器名稱	按一下群組容器建立頁中的 [新建] 按鈕。	
10242	INFO	容器之下建立群組容器成功。	容器 DN群組容器名稱	按一下群組容器建立頁中的 [新建] 按鈕。	
10243	SEVERE	容器之下建立群組容器失敗。	容器 DN群組容器名稱錯誤訊息	無法建立群組容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10244	SEVERE	容器之下建立群組容器失敗。	容器 DN群組容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10251	INFO	嘗試建立群組容器中的群組容器	群組容器 DN 群組容器名稱	按一下群組容器建立頁中的 [新建] 按鈕。	
10252	INFO	群組容器之下建立群組容器成功。	群組容器 DN 群組容器名稱	按一下群組容器建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10253	SEVERE	群組容器之下建立群組容器失敗。	群組容器 DN群組容器名稱錯誤訊息	無法建立群組容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10254	SEVERE	群組容器之下建立群組容器失敗。	群組容器 DN群組容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10301	INFO	嘗試搜尋組織下的群組	組織的 DN 搜尋式樣	按一下組織群組頁中的 [搜尋] 按鈕。	
10302	INFO	組織下搜尋群組成功。	組織的 DN 搜尋式樣	按一下組織群組頁中的 [搜尋] 按鈕。	
10303	SEVERE	組織下搜尋群組失敗。	組織的 DN 搜尋式樣錯誤訊息	無法搜尋群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10304	SEVERE	組織下搜尋群組失敗。	組織的 DN 搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10311	INFO	嘗試搜尋容器下的群組	容器的 DN 搜尋式樣	按一下容器群組頁中的 [搜尋] 按鈕。	
10312	INFO	容器下搜尋群組成功。	容器的 DN 搜尋式樣	按一下容器群組頁中的 [搜尋] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10313	SEVERE	容器下搜尋群組失敗。	容器的 DN 搜尋式樣錯誤訊息	無法搜尋群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10314	SEVERE	容器下搜尋群組失敗。	容器的 DN 搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10321	INFO	嘗試搜尋靜態群組下的群組	靜態群組的 DN 搜尋式樣	按一下靜態群組的群組頁中的 [搜尋] 按鈕。	
10322	INFO	靜態群組下搜尋群組成功。	靜態群組的 DN 搜尋式樣	按一下靜態群組的群組頁中的 [搜尋] 按鈕。	
10323	SEVERE	靜態群組下搜尋群組失敗。	靜態群組的 DN搜尋式樣錯誤訊息	無法搜尋群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10324	SEVERE	靜態群組下搜尋群組失敗。	靜態群組的 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10331	INFO	嘗試搜尋動態群組下的群組	動態群組的 DN 搜尋式樣	按一下動態群組的群組頁中的 [搜尋] 按鈕。	
10332	INFO	動態群組下搜尋群組成功。	動態群組的 DN 搜尋式樣	按一下動態群組的群組頁中的 [搜尋] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10333	SEVERE	動態群組下搜尋群組失敗。	動態群組的 DN搜尋式樣錯誤訊息	無法搜尋群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10334	SEVERE	動態群組下搜尋群組失敗。	動態群組的 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10341	INFO	嘗試搜尋可指定之動態群組下的群組	可指定的動態群組 DN 搜尋式樣	按一下可指定之動態群組的群組頁中的 [搜尋] 按鈕。	
10342	INFO	可指定的動態群組下搜尋群組成功。	可指定的動態群組 DN 搜尋式樣	按一下可指定之動態群組的群組頁中的 [搜尋] 按鈕。	
10343	SEVERE	可指定的動態群組下搜尋群組失敗。	可指定的動態群組 DN搜尋式樣錯誤訊息	無法搜尋群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10344	SEVERE	可指定的動態群組下搜尋群組失敗。	可指定的動態群組 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10351	INFO	嘗試建立組織下的群組	群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10352	INFO	組織下建立群組成功。	群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10353	SEVERE	組織下建立群組失敗。	群組 DN群組名稱錯誤訊息	無法建立群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10354	SEVERE	組織下建立群組失敗。	群組 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10361	INFO	嘗試建立容器下的群組	容器 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10362	INFO	容器下建立群組成功。	容器 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10363	SEVERE	容器下建立群組失敗。	容器 DN群組名稱錯誤訊息	無法建立群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10364	SEVERE	容器下建立群組失敗。	容器 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10371	INFO	嘗試建立群組容器下的群組	群組容器 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10372	INFO	群組容器下建立群組成功。	群組容器 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10373	SEVERE	群組容器下建立群組失敗。	群組容器 DN群組名稱錯誤訊息	無法建立群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10374	SEVERE	群組容器下建立群組失敗。	群組容器 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10381	INFO	嘗試建立動態群組下的群組	動態群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10382	INFO	動態群組下建立群組成功。	動態群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10383	SEVERE	動態群組下建立群組失敗。	動態群組 DN群組名稱錯誤訊息	無法建立群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10384	SEVERE	動態群組下建立群組失敗。	動態群組 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10391	INFO	嘗試建立靜態群組下的群組	靜態群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10392	INFO	靜態群組下建立群組成功。	靜態群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10393	SEVERE	靜態群組下建立群組失敗。	靜態群組 DN群組名稱錯誤訊息	無法建立群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10394	SEVERE	靜態群組下建立群組失敗。	靜態群組 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10401	INFO	嘗試建立可指定之動態群組下的群組	可指定的動態群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10402	INFO	可指定的動態群組下建立群組成功。	可指定的動態群組 DN 群組名稱	按一下群組建立頁中的 [新建] 按鈕。	
10403	SEVERE	可指定的動態群組下建立群組失敗。	可指定的動態群組 DN群組名稱錯誤訊息	無法建立群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10404	SEVERE	可指定的動態群組下建立群組失敗。	可指定的動態群組 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法建立群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10411	INFO	嘗試修改群組	群組 DN	按一下群組設定檔頁中的 [儲存] 按鈕。	
10412	INFO	群組修改成功。	群組 DN	按一下群組設定檔頁中的 [儲存] 按鈕。	
10414	SEVERE	群組修改失敗。	可指定的動態群組 DN群組名稱錯誤訊息	由於存取管理 SDK 異常，無法修改群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10421	INFO	嘗試搜尋群組中的使用者	群組 DN 搜尋式樣	檢視群組使用者頁。	
10422	INFO	搜尋群組中的使用者成功。	群組 DN 搜尋式樣	檢視群組使用者頁。	
10423	SEVERE	搜尋群組中的使用者失敗。	群組 DN搜尋式樣錯誤訊息	無法搜尋使用者。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10424	SEVERE	搜尋群組中的使用者失敗。	群組 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋使用者。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10431	INFO	嘗試取得巢式群組	群組 DN	檢視群組成員頁。	
10432	INFO	取得巢式群組成功。	群組 DN	檢視群組成員頁。	
10433	SEVERE	取得巢式群組失敗。	群組 DN 錯誤訊息	無法取得巢式群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10434	SEVERE	取得巢式群組失敗。	群組 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得巢式群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10441	INFO	嘗試移除巢式群組	群組 DN 巢式群組 *DN*	按一下群組成員頁中的 [移除] 按鈕。	
10442	INFO	移除巢式群組成功。	群組 DN 巢式群組 *DN*	按一下群組成員頁中的 [移除] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10443	SEVERE	移除巢式群組失敗。	群組 DN巢式群組 *DN*錯誤訊息	無法移除巢式群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10444	SEVERE	移除巢式群組失敗。	群組 DN巢式群組 *DN*錯誤訊息	由於存取管理 SDK 異常，無法移除巢式群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10451	INFO	嘗試由群組移除使用者	群組 DN 使用者 *DN*	按一下群組成員頁中的 [移除] 按鈕。	
10452	INFO	由群組移除使用者成功。	群組 DN 使用者 *DN*	按一下群組成員頁中的 [移除] 按鈕。	
10453	SEVERE	由群組移除使用者失敗。	群組 DN 使用者 *DN* 錯誤訊息	無法移除使用者。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10454	SEVERE	由群組移除使用者失敗。	群組 DN 使用者 *DN* 錯誤訊息	由於存取管理 SDK 異常，無法移除使用者。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10501	INFO	嘗試搜尋組織中的使用者容器	組織 DN 搜尋式樣	檢視組織的使用者容器頁。	
10502	INFO	於組織中搜尋使用者容器成功。	組織 DN 搜尋式樣	檢視組織的使用者容器頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10503	SEVERE	於組織中搜尋使用者容器失敗。	組織 DN搜尋式樣錯誤訊息	無法搜尋使用者容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10504	SEVERE	於組織中搜尋使用者容器失敗。	組織 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋使用者容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10511	INFO	嘗試搜尋容器中的使用者容器	容器 DN 搜尋式樣	檢視容器的使用者容器頁。	
10512	INFO	於容器中搜尋使用者容器成功。	容器 DN 搜尋式樣	檢視容器的使用者容器頁。	
10513	SEVERE	於容器中搜尋使用者容器失敗。	容器 DN搜尋式樣錯誤訊息	無法搜尋使用者容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10514	SEVERE	於容器中搜尋使用者容器失敗。	容器 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋使用者容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10521	INFO	嘗試搜尋使用者容器中的使用者容器	使用者容器 DN 搜尋式樣	檢視使用者容器的使用者容器頁。	
10522	INFO	於使用者容器中搜尋使用者容器成功。	使用者容器 DN 搜尋式樣	檢視使用者容器的使用者容器頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10523	SEVERE	於使用者容器中搜尋使用者容器失敗。	使用者容器 DN搜尋式樣錯誤訊息	無法搜尋使用者容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10524	SEVERE	於使用者容器中搜尋使用者容器失敗。	使用者容器 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋使用者容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10531	INFO	嘗試建立組織中的使用者容器	組織 DN使用者容器名稱	按一下使用者容器建立頁中的 [新建] 按鈕。	
10532	INFO	於組織中建立使用者容器成功。	組織 DN使用者容器名稱	按一下使用者容器建立頁中的 [新建] 按鈕。	
10533	SEVERE	於組織中建立使用者容器失敗。	組織 DN使用者容器名稱錯誤訊息	無法建立使用者容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10534	SEVERE	於組織中建立使用者容器失敗。	組織 DN使用者容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立使用者容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10541	INFO	嘗試建立容器中的使用者容器	容器 DN使用者容器名稱	按一下使用者容器建立頁中的 [新建] 按鈕。	
10542	INFO	於容器中建立使用者容器成功。	容器 DN 使用者容器名稱	按一下使用者容器建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10543	SEVERE	於容器中建立使用者容器失敗。	容器 DN使用者容器名稱錯誤訊息	無法建立使用者容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10544	SEVERE	於容器中建立使用者容器失敗。	容器 DN使用者容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立使用者容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10551	INFO	嘗試建立使用者容器中的使用者容器	使用者容器 DN使用者容器名稱	按一下使用者容器建立頁中的 [新建] 按鈕。	
10552	INFO	於使用者容器中建立使用者容器成功。	使用者容器 DN使用者容器名稱	按一下使用者容器建立頁中的 [新建] 按鈕。	
10553	SEVERE	於使用者容器中建立使用者容器失敗。	使用者容器 DN 使用者容器名稱錯誤訊息	無法建立使用者容器。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10554	SEVERE	於使用者容器中建立使用者容器失敗。	使用者容器 DN 使用者容器名稱錯誤訊息	由於存取管理 SDK 異常，無法建立使用者容器。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10601	INFO	嘗試對組織取得已指定的服務	組織 DN	檢視組織服務設定檔頁。	
10602	INFO	對組織取得已指定的服務成功。	組織 DN	檢視組織服務設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10603	SEVERE	對組織取得已指定的服務失敗。	組織 DN 錯誤訊息	無法取得已指定的服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10604	SEVERE	對組織取得已指定的服務失敗。	組織 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得已指定的服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10611	INFO	嘗試由組織移除服務	組織 DN 服務名稱	按一下組織服務設定檔頁中的 [取消指定] 按鈕。	
10612	INFO	由組織移除服務成功。	組織 DN 服務名稱	按一下組織服務設定檔頁中的 [取消指定] 按鈕。	
10613	SEVERE	由組織移除服務失敗。	組織 DN 服務名稱錯誤訊息	無法移除服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10614	SEVERE	由組織移除服務失敗。	組織 DN 服務名稱錯誤訊息	由於存取管理 SDK 異常，無法移除服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10621	INFO	嘗試搜尋組織中的組織	組織 DN 搜尋式樣	檢視組織的子組織頁。	
10622	INFO	搜尋組織中的組織成功。	組織 DN 搜尋式樣	檢視組織的子組織頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10623	SEVERE	搜尋組織中的組織失敗。	組織 DN搜尋式樣錯誤訊息	無法搜尋組織。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10624	SEVERE	搜尋組織中的組織失敗。	組織 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋組織。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10631	INFO	嘗試修改組織。	組織 DN	按一下組織設定檔頁中的 [儲存] 按鈕。	
10632	INFO	組織修改成功。	組織 DN	按一下組織設定檔頁中的 [儲存] 按鈕。	
10633	SEVERE	組織修改失敗。	組織 DN 錯誤訊息	無法修改組織。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10634	SEVERE	組織修改失敗。	組織 DN 錯誤訊息	由於存取管理 SDK 異常，無法修改組織。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10641	INFO	嘗試建立組織中的組織	組織 DN新的組織名稱	按一下組織建立頁中的 [新建] 按鈕。	
10642	INFO	建立組織中的組織成功。	組織 DN新的組織名稱	按一下組織建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10643	SEVERE	建立組織中的組織失敗。	組織 DN新的組織名稱錯誤訊息	無法建立組織。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10644	SEVERE	建立組織中的組織失敗。	組織 DN新的組織名稱錯誤訊息	由於存取管理 SDK 異常，無法建立組織。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10651	INFO	嘗試取得組織的特性值	組織 DN	檢視組織設定檔頁。	
10652	INFO	組織的特性值取得成功。	組織 DN	檢視組織設定檔頁。	
10653	SEVERE	組織的特性值取得失敗。	組織 DN 錯誤訊息	無法取得組織的特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10654	SEVERE	組織的特性值取得失敗。	組織 DN 錯誤訊息	由於存取管理 SDK 異常，因此無法取得組織的特性值。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10661	INFO	嘗試對組織新增服務	組織 DN 服務名稱	按一下組織服務頁中的 [指定] 按鈕。	
10662	INFO	對組織新增服務成功。	組織 DN 服務名稱	按一下組織服務頁中的 [指定] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10663	SEVERE	對組織新增服務失敗。	組織 DN 服務名稱錯誤訊息	無法對組織新增服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10664	SEVERE	對組織新增服務失敗。	組織 DN 服務名稱錯誤訊息	由於存取管理 SDK 異常，無法對組織新增服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10701	INFO	嘗試由角色移除使用者	角色 DN 使用者名稱	按一下角色使用者頁中的 [移除] 按鈕。	
10702	INFO	由角色移除使用者成功。	角色 DN 使用者名稱	按一下角色使用者頁中的 [移除] 按鈕。	
10703	SEVERE	由角色移除使用者失敗。	角色 DN使用者名稱錯誤訊息	無法移除使用者。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10704	SEVERE	由角色移除使用者失敗。	角色 DN使用者名稱錯誤訊息	由於存取管理 SDK 異常，無法移除使用者。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10711	INFO	嘗試取得角色的特性值	角色 DN	檢視角色設定檔頁。	
10712	INFO	取得角色的特性值成功。	角色 DN	檢視角色設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10713	SEVERE	取得角色的特性值失敗。	角色 DN 錯誤訊息	無法取得特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10714	SEVERE	取得角色的特性值失敗。	角色 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得特性值。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10721	INFO	嘗試修改角色	角色 DN	按一下角色設定檔頁中的 [儲存] 按鈕。	
10722	INFO	角色修改成功。	角色 DN	按一下角色設定檔頁中的 [儲存] 按鈕。	
10723	SEVERE	角色修改失敗。	角色 DN 錯誤訊息	無法修改角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10724	SEVERE	角色修改失敗。	角色 DN 錯誤訊息	由於存取管理 SDK 異常，無法修改角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10731	INFO	嘗試取得角色中的成員	角色 DN 搜尋式樣	檢視角色成員頁。	
10732	INFO	取得角色中的成員成功。	角色 DN 搜尋式樣	檢視角色成員頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10733	SEVERE	取得角色中的成員失敗。	角色 DN搜尋式樣錯誤訊息	無法取得成員。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10734	SEVERE	取得角色中的成員失敗。	角色 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法取得成員。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10741	INFO	嘗試取得組織中的角色	角色 DN 搜尋式樣	檢視組織的角色頁。	
10742	INFO	取得組織中的角色成功。	角色 DN搜尋式樣檢視角色成員頁。	檢視組織的角色頁。	
10743	SEVERE	取得組織中的角色失敗。	角色 DN搜尋式樣錯誤訊息	無法取得角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10744	SEVERE	取得組織中的角色失敗。	角色 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法取得角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10751	INFO	嘗試取得容器中的角色	角色 DN 搜尋式樣	檢視容器角色頁。	
10752	INFO	取得容器中的角色成功。	角色 DN搜尋式樣檢視角色成員頁。	檢視容器角色頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10753	SEVERE	取得容器中的角色失敗。	角色 DN搜尋式樣錯誤訊息	無法取得角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10754	SEVERE	取得容器中的角色失敗。	角色 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法取得角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10761	INFO	嘗試建立容器中的角色	容器 DN 角色名稱	按一下角色建立頁中的 [新建] 按鈕。	
10762	INFO	於容器中建立群組成功。	容器 DN 角色名稱	按一下角色建立頁中的 [新建] 按鈕。	
10763	SEVERE	於容器中建立群組失敗。	容器 DN 角色名稱	無法建立角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10764	SEVERE	於容器中建立角色失敗。	容器 DN角色名稱錯誤訊息	由於存取管理 SDK 異常，無法建立角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10771	INFO	嘗試建立組織中的角色	組織 DN 角色名稱	按一下角色建立頁中的 [新建] 按鈕。	
10772	INFO	於組織中建立角色成功。	組織 DN 角色名稱	按一下角色建立頁中的 [新建] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10773	SEVERE	於組織中建立角色失敗。	組織 DN 角色名稱	無法建立角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10774	SEVERE	於組織中建立角色失敗。	組織 DN角色名稱錯誤訊息	由於存取管理 SDK 異常，無法建立角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10781	INFO	嘗試取得角色中已指定的服務	角色 DN	檢視角色服務頁。	
10782	INFO	取得角色中已指定的服務成功。	角色 DN	檢視角色服務頁。	
10783	SEVERE	取得角色中已指定的服務失敗。	角色 DN 錯誤訊息	無法取得角色中的服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10784	SEVERE	取得角色中已指定的服務失敗。	角色 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得角色中的服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10791	INFO	嘗試由角色移除服務	角色 DN 服務名稱	按一下角色服務頁中的 [取消指定] 按鈕。	
10792	INFO	由角色移除服務成功。	角色 DN 服務名稱	按一下角色服務頁中的 [取消指定] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10793	SEVERE	由角色移除服務失敗。	角色 DN服務名稱錯誤訊息	無法由角色移除服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10794	SEVERE	由角色移除服務失敗。	角色 DN服務名稱錯誤訊息	由於存取管理 SDK 異常，無法由角色移除服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10801	INFO	嘗試對角色新增服務	角色 DN 服務名稱	按一下角色服務頁中的 [指定] 按鈕。	
10802	INFO	對角色新增服務成功。	角色 DN 服務名稱	按一下角色服務頁中的 [指定] 按鈕。	
10803	SEVERE	對角色新增服務失敗。	角色 DN服務名稱錯誤訊息	無法對角色新增服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10804	SEVERE	對角色新增服務失敗。	角色 DN服務名稱錯誤訊息	由於存取管理 SDK 異常，無法對角色新增服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10901	INFO	嘗試取得使用者已指定的角色	使用者 DN	檢視使用者角色頁。	
10902	INFO	取得使用者已指定的角色成功。	使用者 DN	檢視使用者角色頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10903	SEVERE	取得使用者已指定的角色失敗。	使用者 DN 錯誤訊息	無法取得已指定的角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10904	SEVERE	取得使用者已指定的角色失敗。	使用者 DN服務名稱錯誤訊息	由於存取管理 SDK 異常，無法取得已指定的角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10911	INFO	嘗試由使用者移除角色	使用者 DN 角色 *DN*	按一下使用者角色頁中的 [刪除] 按鈕。	
10912	INFO	由使用者移除角色成功。	使用者 DN 角色 *DN*	按一下使用者角色頁中的 [刪除] 按鈕。	
10913	SEVERE	由使用者移除角色失敗。	使用者 DN 角色 *DN* 錯誤訊息	無法移除角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10914	SEVERE	由使用者移除角色失敗。	使用者 DN角色 *DN*服務名稱錯誤訊息	由於存取管理 SDK 異常，無法移除角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10921	INFO	嘗試對使用者新增角色	使用者 DN 角色 *DN*	按一下使用者角色頁中的 [新增] 按鈕。	
10922	INFO	對使用者新增角色成功。	使用者 DN 角色 *DN*	按一下使用者角色頁中的 [新增] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10923	SEVERE	對使用者新增角色失敗。	使用者 DN 角色 *DN* 錯誤訊息	無法新增角色。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10924	SEVERE	對使用者新增角色失敗。	使用者 DN角色 *DN*服務名稱錯誤訊息	由於存取管理 SDK 異常，無法新增角色。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10931	INFO	嘗試取得已指定的使用者服務	使用者 DN	檢視使用者服務頁。	
10932	INFO	取得已指定的使用者服務成功。	使用者 DN	檢視使用者服務頁。	
10933	SEVERE	取得已指定的使用者服務失敗。	使用者 DN 錯誤訊息	無法取得服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10934	SEVERE	取得已指定的使用者服務失敗。	使用者 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10941	INFO	嘗試由使用者移除服務	使用者 DN 服務名稱	按一下使用者服務頁中的 [移除] 按鈕。	
10942	INFO	由使用者移除服務成功。	使用者 DN 服務名稱	按一下使用者服務頁中的 [移除] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10943	SEVERE	由使用者移除服務失敗。	使用者 DN服務名稱錯誤訊息	無法移除服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10944	SEVERE	由使用者移除服務失敗。	使用者 DN服務名稱錯誤訊息	由於存取管理 SDK 異常，無法移除服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10951	INFO	嘗試搜尋組織中的使用者	組織 DN 搜尋式樣	檢視組織的使用者頁。	
10952	INFO	於組織中搜尋使用者成功。	組織 DN 搜尋式樣	檢視組織的使用者頁。	
10953	SEVERE	於組織中搜尋使用者失敗。	組織 DN搜尋式樣錯誤訊息	無法搜尋使用者。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10954	SEVERE	於組織中搜尋使用者失敗。	組織 DN搜尋式樣錯誤訊息	由於存取管理 SDK 異常，無法搜尋使用者。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10961	INFO	嘗試修改使用者	使用者 DN	按一下使用者設定檔頁中的 [儲存] 按鈕。	
10962	INFO	使用者設定檔修改成功。	使用者 DN	按一下使用者設定檔頁中的 [儲存] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10963	SEVERE	使用者設定檔修改失敗。	使用者 DN 錯誤訊息	無法修改使用者。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10964	SEVERE	使用者設定檔修改失敗。	使用者 DN 錯誤訊息	由於存取管理 SDK 異常，無法修改使用者。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10971	INFO	嘗試建立使用者	使用者容器 DN 使用者名稱	按一下使用者建立頁中的 [新增] 按鈕。	
10972	INFO	使用者建立成功。	使用者容器 DN 使用者名稱	按一下使用者建立頁中的 [新增] 按鈕。	
10973	SEVERE	使用者建立失敗。	使用者容器 DN使用者名稱錯誤訊息	無法建立使用者。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10974	SEVERE	使用者建立失敗。	使用者容器 DN使用者名稱錯誤訊息	由於存取管理 SDK 異常，無法建立使用者。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10981	INFO	嘗試取得使用者的特性值	使用者 DN	檢視使用者設定檔頁。	
10982	INFO	取得使用者的特性值成功。	使用者 DN	檢視使用者設定檔頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
10983	SEVERE	取得使用者的特性值失敗。	使用者 DN 錯誤訊息	無法取得特性值。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10984	SEVERE	取得使用者的特性值失敗。	使用者 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得特性值。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10991	INFO	嘗試對使用者新增服務	使用者 DN 服務名稱	按一下使用者服務頁中的 [新增] 按鈕。	
10992	INFO	對使用者新增服務成功。	使用者 DN 服務名稱	按一下使用者服務頁中的 [新增] 按鈕。	
10993	SEVERE	對使用者新增服務失敗。	使用者 DN服務名稱錯誤訊息	無法新增服務。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
10994	SEVERE	對使用者新增服務失敗。	使用者 DN服務名稱錯誤訊息	由於存取管理 SDK 異常，無法新增服務。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
11001	INFO	嘗試取得已指定的使用者群組	使用者 DN	檢視使用者群組頁。	
11002	INFO	取得已指定的使用者群組成功。	使用者 DN	檢視使用者群組頁。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
11003	SEVERE	取得已指定的使用者群組失敗。	使用者 DN 錯誤訊息	無法取得已指定的群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
11004	SEVERE	取得已指定的使用者群組失敗。	使用者 DN 錯誤訊息	由於存取管理 SDK 異常，無法取得已指定的群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
11011	INFO	嘗試由使用者移除群組	使用者 DN 群組 *DN*	按一下使用者群組頁中的 [移除] 按鈕。	
11012	INFO	由使用者移除群組成功。	使用者 DN 群組 *DN*	按一下使用者群組頁中的 [移除] 按鈕。	
11013	SEVERE	由使用者移除群組失敗。	使用者 DN 群組 *DN* 錯誤訊息	無法移除群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
11014	SEVERE	由使用者移除群組失敗。	使用者 DN 群組 *DN* 錯誤訊息	由於存取管理 SDK 異常，無法移除群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
11021	INFO	嘗試對使用者新增群組	使用者 DN 群組 *DN*	按一下使用者群組頁中的 [新增] 按鈕。	
11022	INFO	對使用者新增群組成功。	使用者 DN 群組 *DN*	按一下使用者群組頁中的 [新增] 按鈕。	

表 C–3 Access Manager 主控台的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
11023	SEVERE	對使用者新增群組失敗。	使用者 DN 群組 *DN* 錯誤訊息	無法新增群組。其可爲使用者已過期之單次登入記號；或使用者並不具有執行此作業的權限。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。
11024	SEVERE	對使用者新增群組失敗。	使用者 DN 群組 *DN* 錯誤訊息	由於存取管理 SDK 異常，無法新增群組。	如需更多資訊，請於存取管理 SDK 記錄下進行查詢。

表 C–4 聯合的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	認證網域建立	認證網域名稱	已建立的認證網域	
2	INFO	認證網域刪除	認證網域名稱	已刪除的認證網域	
3	INFO	修改認證網域	認證網域名稱	已修改的認證網域	
4	INFO	遠端提供者建立	提供者 ID	已建立的遠端提供者	
5	INFO	寄存提供者建立	提供者 ID	已建立的寄存提供者	
6	INFO	已刪除的附屬提供者	附屬提供者 ID	已刪除的附屬提供者	
7	INFO	刪除實體	實體 ID	已刪除的實體	
8	INFO	已刪除的提供者	提供者 ID	已刪除的提供者	
9	INFO	修改實體	實體 ID	已修改的實體	
10	INFO	修改附屬提供者	附屬提供者 ID	已修改的附屬提供者	
11	INFO	修改提供者	提供者 ID	已修改的提供者	

表 C–4 聯合的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
12	INFO	建立實體	實體 ID	已建立實體	
13	INFO	建立附屬提供者	附屬提供者 ID	已建立的附屬提供者	
14	INFO	寫入帳號聯合資訊	使用者 DN聯合資訊金鑰聯合資訊值	將含有金鑰的帳號聯合資訊新增至使用者	
15	INFO	遠端帳號聯合資訊	使用者 DN提供者 *ID* 現存的聯合資訊金鑰	含有金鑰的帳號聯合資訊和提供者 ID 已由使用者中移除	
16	FINER	建立指定	指定 ID 或字串	指定已建立	
17	INFO	未啓用 Liberty。	訊息	未啓用 Liberty。無法處理請求。	登入 [管理主控台] 以啓用 [管理主控台服務] 中的 [聯合管理]。
18	INFO	登出請求處理失敗。	訊息	登出請求處理失敗	
19	INFO	終止請求處理失敗	訊息	終止請求處理失敗	
20	INFO	建立 SOAP URL 端點失敗。	soap 端點 url	建立 SOAP URL 端點失敗	
21	INFO	不相符的 AuthType 與協定 (根據 SOAPUrl)。	協定認證類型	AuthType 和協定 (基於 SOAPUrl) 不相符。	
22	INFO	認證類型錯誤。	認證類型	認證類型錯誤。	
23	FINER	SAML SOAP 接收器 URL	soap url	SAML SOAP 接收器 URL	
24	INFO	SOAP 回應無效	訊息	SOAP 回應無效。	
25	INFO	指定無效	訊息	這個指定無效	
26	INFO	單次登入失敗	訊息	單次登入失敗	

表 C–4 聯合的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
27	INFO	授予存取權後重新導向 URL。	重新導向 url	授予存取權後重新導向 URL。	
28	INFO	缺少認證回應	訊息	找不到認證回應	
29	INFO	帳號聯合失敗	訊息	帳號聯合失敗	
30	INFO	SSOToken 產生失敗	訊息	無法產生 SSOToken	
31	INFO	認證回應無效	無效的認證回應	認證回應無效	
32	INFO	認證請求處理失敗	訊息	認證請求處理失敗。	
33	INFO	簽名驗證失敗。	訊息	簽名驗證失敗。	
34	FINER	已建立的 SAML 回應	saml 回應	已建立的 SAML 回應	
35	FINER	重新導向 URL	重新導向 url	重新導向：	
36	INFO	找不到共用網域服務資訊	訊息	找不到共用網域服務資訊。	
37	INFO	提供者不可信任	提供者 ID	提供者不可信任。	
38	INFO	認證請求無效	訊息	認證請求無效	
39	INFO	找不到使用者的帳號聯合資訊	使用者名稱	找不到使用者的帳號聯合資訊：	
40	INFO	找不到使用者。	使用者名稱	找不到使用者。	
41	INFO	不支援登出設定檔。	登出設定檔	不支援登出設定檔。	驗證中介資料是正確的。
42	INFO	登出成功。	使用者名稱	登出成功。	
43	INFO	因爲錯誤 URL，導致登出無法重新導向。	訊息	因爲錯誤 URL，導致登出無法重新導向。	

表 C–4 聯合的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
44	INFO	並未正常地組成登出請求。	使用者名稱	並未正常地組成登出請求。	
45	INFO	無法取得預先/登出處理程式。	登出 url	無法取得預先/登出處理程式。	
46	INFO	單次登出失敗。	使用者名稱	單次登出失敗。	
47	INFO	無法建立 SPProvidedNameIdentifier。	訊息	無法建立 SPProvidedNameIdentifier。	
48	INFO	無效的簽名。	訊息	無效的簽名。	
49	INFO	聯合終止失敗。	使用者名稱	聯合終止失敗。無法更新帳號。	
50	FINER	聯合終止成功。	userDN	聯合終止成功。使用者帳號更新。	
51	INFO	回應無效	saml 回應	SAML 回應無效。	
52	INFO	提供者註冊無效。	提供者 ID	無效的提供者。	

表 C–5 Liberty 的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	無法處理 SASL 請求	訊息 ID認證機制認證 *ID*諮詢認證 *ID*	無法處理 SASL 請求。	
2	INFO	SASL 回應正常	訊息 ID認證機制認證 *ID*諮詢認證 *ID*	SASL 回應正常。	
3	INFO	傳回 SASL 認證回應	訊息 ID認證機制認證 *ID*諮詢認證 *ID*	已傳回 SASL 回應，繼續認證。	
4	INFO	資料存放區中找不到使用者	使用者名稱	資料存放區中找不到使用者	

表 C–5 Liberty 的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
5	INFO	於資料存放區中找到了使用者	使用者名稱	於資料存放區中找到了使用者	
6	INFO	無法由 resourceID 找到使用者	resourceID	無法由 resourceID 找到使用者	
7	INFO	成功更新使用者設定檔	使用者名稱	成功更新使用者設定檔	
8	INFO	未授權。無法查詢個人設定檔服務	資源 ID	無法查詢個人設定檔服務	
9	INFO	互動失敗	資源 ID	與個人設定檔服務互動失敗	
10	INFO	已順利地查詢 PP 服務	資源 ID	個人設定檔服務查詢成功	
11	INFO	修改失敗	資源 ID	無法修改個人設定檔服務	
12	INFO	修改成功	資源 ID	已順利地修改個人設定檔服務。	
13	INFO	互動順利	成功互動訊息	與個人設定檔服務順利互動	
14	INFO	傳送訊息	請求訊息 ID	將 SOAP 請求訊息傳送至 WSP。	
15	INFO	傳回回應訊息	回應訊息 ID 請求訊息 *ID*	傳回 SOAP 請求的回應訊息。	
16	INFO	重新傳送訊息	訊息 ID	將 SOAP 請求訊息重新傳送至 WSP。	
17	INFO	將使用者代理程式重新導向至互動服務的互動管理員	請求訊息 ID	將使用者代理程式重新導向至互動服務的互動管理員	

表 C–5 Liberty的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
18	INFO	互動管理員傳回回應元素	訊息 ID 參照訊息 *ID* 快取項目狀態	互動管理員傳回回應元素	
19	INFO	對使用者代理程式提出互動查詢	訊息 ID	對使用者代理程式提出互動查詢	
20	INFO	對互動查詢回應使用者代理程式	訊息 ID	對互動查詢回應使用者代理程式	
21	INFO	將使用者代理程式重新導向回 SP	訊息 ID	將使用者代理程式重新導向回 SP	
22	INFO	Web 服務成功	訊息 ID 控制器鍵	Web 服務成功。	
23	INFO	Web 服務失敗	錯誤訊息	Web 服務失敗。	

表 C–6 策略的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	評估策略成功	策略名稱範圍名稱服務類型名稱資源名稱動作名稱策略決定	評估策略。	
2	INFO	取得受保護的策略資源成功	主體名稱資源名稱保護策略	取得受保護的策略資源。	
3	INFO	於範圍中建立策略成功	策略名稱範圍名稱	於範圍中建立策略。	
4	INFO	於範圍中修改策略成功	策略名稱範圍名稱	於範圍中修改策略。	
5	INFO	由範圍移除策略成功	策略名稱範圍名稱	由範圍移除策略。	
6	INFO	策略已存在於範圍中	策略名稱範圍名稱	於範圍中建立策略。	

表 C–6 策略的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
7	INFO	於範圍中的建立策略失敗	策略名稱範圍名稱	於範圍中建立策略。	請檢查使用者是否具有於範圍中建立策略的權限。
8	INFO	於範圍中置換策略失敗	策略名稱範圍名稱	於範圍中置換策略。	請檢查使用者是否具有於範圍中置換策略的權限。
81	INFO	請勿置換策略 - 具有新名稱的不同策略已經存在於範圍中	新的策略名稱範圍名稱	於範圍中置換策略	
9	INFO	由範圍移除策略失敗	策略名稱範圍名稱	由範圍移除策略。	請檢查使用者是否具有由範圍中移除策略的權限。
10	INFO	由管理員計算策略決策成功	管理名稱主體名稱資源名稱策略決策	由管理員計算策略決策成功。	
11	INFO	由管理員忽略主旨來計算策略決策成功	管理名稱資源名稱策略決策	由管理員忽略主旨來計算策略決策成功	

表 C–7 SAML的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	已建立新的指定	訊息 ID 指定 *ID* 或若記錄層級爲 *LL_FINER*，則爲指定	瀏覽器工件設定檔瀏覽器 *POST* 設定檔建立指定工件認證查詢特性查詢認證決策查詢	
2	INFO	已建立新的指定工件	訊息 ID 指定工件對應至工件的指定 *ID*	瀏覽器工件設定檔建立指定工件	
3	FINE	由對應表移除指定工件	訊息 ID 指定工件	SAML 工件查詢指定工件到期	

表 C–7 SAML的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
4	FINE	由對應表移除指定	訊息 ID 指定 *ID*	SAML 工件查詢指定到期	
5	INFO	已驗證指定工件的存取權	訊息 ID 指定工件	SAML 工件查詢	
6	INFO	配置的認證類型與實際的 SOAP 協定不相符。	訊息 ID	SAML SOAP 查詢	登入 [主控台]，前往 [聯合]，然後至 SAML，編輯 [可信任的合作夥伴配置]，檢查已選取的 [認證類型] 欄位，請確定其與指定於 SOAP URL 欄位中的協定相符合。
7	INFO	無效的認證類型	訊息 ID	SAML SOAP 查詢	登入 [主控台]，前往 [聯合]，然後至 SAML，編輯 [可信任的合作夥伴配置]，選取 [認證類型] 欄位的任一值，然後儲存。
8	FINE	遠端 SOAP 接收器 URL	訊息 ID *SOAP 接收器 URL*	SAML SOAP 查詢	
9	INFO	沒有任何指定出現於 saml 回應中	訊息 ID *SAML* 回應	SAML 工件查詢	若有任何問題，請連絡遠端合作夥伴
10	INFO	SAML 回應中的指定數與 SAML 請求中的工件數不相等。	訊息 ID *SAML* 回應	SAML 工件查詢	若有任何問題，請連絡遠端合作夥伴
11	INFO	將傳送至遠端合作夥伴的工件	訊息 ID *SAML* 工件	SAML 工件查詢	

表 C–7 SAML的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
12	INFO	可信任的合作夥伴配置中錯誤的 SOAP URL	訊息 ID	SAML 工件查詢	登入 [主控台]，前往 [聯合]，然後至 SAML，編輯 [可信任的合作夥伴配置]，對 SOAP URL 欄位輸入值，然後儲存。
13	FINE	SAML 工件查詢 SOAP 請求	訊息 ID *SAML* 工件查詢訊息	SAML 工件查詢	
14	INFO	並無來自遠端 SAML SOAP 接收器的回應	訊息 ID	SAML 工件查詢	若有任何問題，請與遠端合作夥伴進行確認
15	FINE	SAML 工件查詢回應	訊息 ID *SAML* 工件查詢回應訊息	SAML 工件查詢	
16	INFO	於 SOAP 回應內並無 SAML 回應	訊息 ID	SAML 工件查詢	若有任何問題，請與遠端合作夥伴進行確認
17	INFO	SAML 回應的 XML 簽名無效	訊息 ID	SAML 工件查詢	若對 XML 數位簽名有任何問題，請與遠端合作夥伴進行確認
18	INFO	取得 SAML 回應狀態碼時發生錯誤	訊息 ID	SAML 工件查詢	若對回應狀態碼有任何問題，請與遠端合作夥伴進行確認
19	INFO	請求中缺少 TARGET 參數	訊息 ID	SAML 工件設定檔 *SAML POST* 設定檔	於請求中，新增 TARGET=target_url 爲查詢參數

表 C–7 SAML的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
20	INFO	SAML 工件來源網站的重新導向 URL	訊息 ID 目標重新導向 *URL*若爲 *POST* 設定檔及記錄層級爲 *LL_FINER*，則爲 *SAML* 回應訊息	SAML 工件設定檔來源*SAML POST* 設定檔來源	
21	INFO	指定的目標網站被禁止使用	訊息 ID 目標 *URL*	SAML 工件設定檔來源*SAML POST* 設定檔來源	指定於請求中的 TARGET URL 不爲其他任何可信任的合作夥伴所控制，請核對您的 TARGET url，並請確定其與配置於可信任的合作夥伴網站中的其中一個 Target URL 相符合
22	INFO	無法建立單次登入記號	訊息 ID	SAML 工件設定檔目標*SAML POST* 設定檔目標	認證元件無法建立 SSO 記號，請核對認證記錄與除錯以取得詳細資料
23	INFO	單次登入成功，授予目標存取權	訊息 ID 若爲 *POST* 設定檔及記錄層級爲 *LL_FINER* 或較高，則爲回應訊息	SAML 工件設定檔目標*SAML POST* 設定檔目標	
24	INFO	空 servlet 請求或回應	訊息 ID	SAML 工件設定檔*SAML POST* 設定檔	核對 Web 容器錯誤記錄以取得詳細資料
25	INFO	POST 主體中缺少 SAML 回應	訊息 ID	SAML POST 設定檔目標	與遠端 SAML 合作夥伴進行確認以找出 SAML 回應物件由 HTTP POST 主體缺少的原因

表 C–7 SAML的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
26	INFO	回應訊息中的錯誤	訊息 ID	SAML POST 設定檔目標	無法將編碼的 POST 主體屬性轉換爲 SAML 回應物件，請與遠端 SAML 合作夥伴核對以找出 SAML 回應中建立的任何錯誤，如編碼錯誤、無效的回應子元素等。
27	INFO	回應無效	訊息 ID	SAML POST 設定檔目標	SAML 回應中的收件者特性與此網站的 POST 設定檔 URL 不相符回應狀態碼不成功
28	INFO	無法取得訊息工廠的實例	訊息 ID	SAML SOAP 接收器初始	檢查您的 SOAP 工廠特性 (javax.xml.soap.MessageFactory) 以確保其使用有效的 SOAP 工廠實作
29	INFO	從不信任的網站接收請求	訊息 ID 遠端網站主機名稱或 *IP* 位址	SAML SOAP 查詢	登入 [主控台]，前往 [聯合]，然後至 SAML 服務，編輯 [可信任的合作夥伴配置]，檢查 [主機清單] 欄位，請確定遠端主機/IP 爲其中一個值。於含用戶端認證的 SSL 案例中，請確定 [主機清單] 包含遠端網站的用戶端憑證。

表 C–7 SAML的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
30	INFO	遠端合作夥伴網站請求無效	訊息 ID 與請求主機名稱/IP 位址傳回回應	SAML SOAP 查詢	請與遠端合作夥伴網站的管理員進行確認
31	FINE	合作夥伴網站的請求訊息	訊息 ID 與請求主機名稱/IP 位址請求 *XML*	SAML SOAP 查詢	
32	INFO	由於內部伺服器錯誤，無法建立回應	訊息 ID	SAML SOAP 查詢	核對除錯訊息以找出其失敗的原因，例如，無法建立回應狀態、主要/次要的版本錯誤等
33	INFO	將 SAML 回應傳送至合作夥伴網站	訊息 ID *SAML* 回應或回應 *ID*	SAML SOAP 查詢	
32	INFO	無法建立 SOAP 錯誤回應主體	訊息 ID	SAML SOAP 查詢	核對除錯訊息以找出失敗的原因，例如，無法建立 SOAP 錯誤等

表 C–8 階段作業的記錄檔參照

ID	記錄層級	說明	日期	觸發器	動作
1	INFO	已建立階段作業	使用者 ID	以認證使用者。	
2	INFO	階段作業閒置逾時	使用者 ID	使用者階段作業閒置了很長時間。	
3	INFO	階段作業已逾期	使用者 ID	使用者階段作業已達到其最大限制時間。	
4	INFO	使用者已登出	使用者 ID	使用者已登出系統。	
5	INFO	重新啓動階段作業	使用者 ID	使用者階段作業爲作用中。	

表 C–8 階段作業的記錄檔參照 *(續)*

ID	記錄層級	說明	日期	觸發器	動作
6	INFO	已銷毀階段作業	使用者 ID	使用者階段作業已銷毀且無法進行參照。	
7	INFO	階段作業特性已變更。	使用者 ID	使用者變更階段作業之未受保護的特性。	
8	INFO	階段作業收到未知的事件	使用者 ID	未知的階段作業事件	
9	INFO	嘗試設定受保護的特性	使用者 ID	嘗試設定受保護的特性	
10	INFO	使用者階段作業的配額已用盡。	使用者 ID	階段作業配額已用盡	
11	INFO	用於階段作業容錯移轉與階段作業限制的階段作業資料庫無法使用。	使用者 ID	無法取得階段作業資料庫。	
12	INFO	階段作業資料庫回到線上。	使用者 ID	階段作業資料庫回到線上。	
13	INFO	寄存於 AM 伺服器上的有效階段作業總數已達到最大限度。	使用者 ID	已達到階段作業最大限度。	

◆ ◆ ◆ 附錄 D

錯誤碼

本附錄提供 Access Manager 產生的錯誤訊息清單。雖然此清單並不詳盡，但對於一般問題，本章所提供的資訊可以做爲一個良好起點。本附錄中列出的表格提供了錯誤碼以及錯誤描述和/或可能原因，還描述了修正遇到的問題時可以採取的動作。

本附錄列出了以下功能區域的錯誤碼：

如果您需要有關診斷錯誤的進一步援助，請連絡技術支援：

http://www.sun.com/service/sunone/software/index.html

Access Manager 主控台錯誤

下表描述了 Access Manager 主控台產生和顯示的錯誤碼。

表 D–1 Access Manager 主控台錯誤

錯誤訊息	說明/可能的原因	動作
刪除以下內容時發生錯誤：	物件在被目前使用者移除之前可能已被其他使用者移除。	重新顯示您要刪除的物件，並再次嘗試刪除物件。
您輸入的 URL 無效。	不正確地輸入 Access Manager 主控台視窗的 URL 時會出現此訊息。	
沒有符合搜尋條件的項目。	在搜尋視窗或 [篩選] 欄位中輸入的參數與目錄中的任何物件均不相符。	使用一組不同的參數再次執行搜尋。

表 D–1 Access Manager 主控台錯誤 (續)

錯誤訊息	說明/可能的原因	動作
沒有要顯示的屬性。	所選物件不包含任何在其模式中定義的可編輯屬性。	
沒有關於此服務的資訊顯示。	從服務配置模組所檢視的服務不包含全域屬性或基於組織的屬性。	
超過搜尋大小限制。請精簡搜尋。	搜尋中指定的參數傳回的項目多於允許傳回的項目。	將管理服務中的 [從搜尋傳回的最多結果] 屬性修改爲較大的值。您還可以修改搜尋參數，使其限制更加嚴格。
已超過搜尋時間限制。請精簡搜尋。	指定參數的搜尋佔用的時間已超過允許的搜尋時間。	在管理服務中將 [搜尋逾時] 屬性修改爲較大的值。您還可以修改搜尋參數，使其限制放寬，以便傳回更多值。
無效的使用者起始位置。請連絡您的管理員。	使用者項目中的起始位置 DN 不再有效。	在 [使用者設定檔] 頁面中，將起始 DN 的值變更爲有效的 DN。
無法建立識別物件。使用者沒有足夠的存取權限。	作業由不具有足夠許可權的使用者執行。使用者定義的許可權將決定他們可以執行哪些作業。	

認證錯誤碼

下表描述認證服務所產生的錯誤碼。這些錯誤在認證模組中顯示給使用者/管理員。

表 D–2 認證錯誤碼

錯誤訊息	說明/可能的原因	動作
authentication.already.login.	使用者已登入並擁有有效的階段作業，但是沒有已定義的成功 URL 重新導向。	或者登出，或者透過 Access Manager 主控台設定一些登入成功重新導向 URL。將「goto」查詢參數與諸如管理主控台 URL 的值配合使用。
logout.failure.	使用者無法登出 Access Manager。	重新啓動伺服器。
uncaught_exception	由於處理程式不正確，系統拋出認證異常。	檢查登入 URL，以確定其是否包含任何無效字元或特殊字元。
redirect.error	Access Manager 無法重新導向至成功重新導向 URL 或失敗重新導向 URL。	檢查 Web 容器的錯誤記錄檔以確定是否存在任何錯誤。
gotoLoginAfterFail	大部分錯誤出現後均會產生此連結。此連結會讓使用者返回至原始 [登入 URL] 頁面。	

表 D–2 認證錯誤碼 *(續)*

錯誤訊息	說明/可能的原因	動作
invalid.password	輸入的密碼無效。	密碼必須包含至少 8 個字元。檢查密碼是否包含適當的字元數，並確保其未過期。
auth.failed	驗證失敗。這是顯示在預設登入失敗範本中的一般錯誤訊息。最常見的原因爲憑證無效/不正確。	輸入有效與正確的使用者名稱/密碼 (被呼叫的認證模組所需之憑證。)
nouser.profile	在給定組織中未找到與輸入的使用者名稱相符的使用者設定檔。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	再次輸入您的登入資訊。如果這是您第一次嘗試登入，請在登入畫面上選取 [新建使用者]。
notenough.characters	輸入的密碼字元數不夠。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	依預設，登入密碼必須包含至少個字元此數字可在成員身份認證模組中配置。
useralready.exists	給定組織中已存在具有此名稱的使用者。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	使用者 ID 在組織中必須唯一。
uidpasswd.same	[使用者名稱] 和 [密碼] 欄位不能爲相同的值。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	確保使用者名稱與密碼不同。
nouser.name	尚未輸入使用者名稱。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	確保輸入使用者名稱。
no.password	尚未輸入密碼。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	確保輸入密碼。
missing.confirm.passwd	遺漏確認密碼欄位。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	確保在 [確認密碼] 欄位中輸入密碼。
password.mismatch	密碼與確認密碼不相符。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	確保密碼與確認密碼相符。
儲存使用者設定檔時發生錯誤。	儲存使用者設定檔時發生錯誤。登入至成員身份/自我註冊認證模組時，系統會顯示此錯誤。	確保 `Membership.xml` 檔案中 [自我註冊] 的屬性和元素有效且正確。
orginactive	該組織不在作用中。	藉由將組織狀態從**非作用中**變更爲**作用中**，透過 Access Manger 主控台啓用組織。

表 D–2 認證錯誤碼 *(續)*

錯誤訊息	說明/可能的原因	動作
internal.auth.error	內部認證錯誤。這是一般認證錯誤，可能由不同環境和多重環境問題和/或配置問題引起。	
usernot.active	使用者不再處於作用中狀態。	藉由將使用者狀態從**非作用中**變更爲**作用中**，透過管理主控台啓用使用者。 如果使用者被「記憶體鎖定」鎖定，請重新啓動伺服器。
user.not.inrole	使用者不屬於指定的角色。在基於角色的認證過程中，系統會顯示此錯誤。	確保登入使用者屬於爲基於角色的認證所指定的角色。
session.timeout	使用者階段作業已逾時。	再次登入。
authmodule.denied	指定的認證模組被拒絕。	確保已在所需的組織下註冊所需的認證模組，已爲該模組建立並儲存範本，並且已在核心認證模組的 [組織認證模組] 清單中選取該模組。
noconfig.found	找不到配置。	檢查認證配置服務，以確定其是否包含所需認證方法。
cookie.notpersistent	永久性 Cookie 網域中不存在永久性 Cookie 使用者。	
nosuch.domain	未找到組織。	確保請求的組織有效且正確。
userhasnoprofile.org	使用者在指定的組織中沒有設定檔。	確保使用者在本機 Directory Server 的指定組織中存在且有效。
reqfield.missing	一個必填欄位未填充。請確保所有必填欄位均已填入。	確保所有必填欄位均已填入。
session.max.limit	已達到最大的階段作業限制。	登出並再次登入。

策略錯誤碼

下表描述由策略框架產生並在 Access Manager 主控台中顯示的錯誤碼。

表 D–3 策略錯誤碼

錯誤訊息	說明/可能的原因	動作
illegal_character_/_in_name	策略名稱中存在非法字元「/」。	確保策略名稱不包含「/」字元。
policy_already_exists_in_org	具有相同名稱的規則已存在。	使用不同的名稱建立策略。

表 D–3 策略錯誤碼 *(續)*

錯誤訊息	說明/可能的原因	動作
rule_name_already_present	已經存在另一個帶有給定名稱的規則	使用不同的規則名稱建立策略。
rule_already_present	具有相同規則值的規則已存在。	使用不同的規則值。
no_referral_can_not_create_policy	組織的參考不存在。	爲了於子組織之下建立策略，您必須在其父系組織中建立參考策略，以指示該子組織可以參考哪些資源。
ldap_search_exceed_size_limit	已超過 LDAP 搜尋大小限制。由於搜尋找到的結果超過最大結果數而出現錯誤。	變更搜尋式樣或組織的策略配置，以用於搜尋控制參數。[搜尋大小限制] 位於 [策略配置] 服務中。
ldap_search_exceed_time_limit	已超過 LDAP 搜尋時間限制。由於搜尋找到的結果超過最大結果數而出現錯誤。	變更搜尋式樣或組織的策略配置，以用於搜尋控制參數。[搜尋時間限制] 位於 [策略配置] 服務中。
ldap_invalid_password	無效的 LDAP 連結密碼。	策略配置中定義的 LDAP 連結使用者的密碼不正確。這會導致無法取得認證的 LDAP 連線以執行策略作業。
app_sso_token_invalid	應用程式 SSO 記號無效。	伺服器無法驗證應用程式 SSO 記號。SSO 記號很可能已過期。
user_sso_token_invalid	使用者 SSO 記號無效。	伺服器無法驗證使用者 SSO 記號。SSO 記號很可能已過期。
property_is_not_an_Integer	特性值不是整數。	外掛程式的屬性值應爲整數。
property_value_not_defined	特性值應該被定義。	爲給定特性提供值。
start_ip_can_not_be_greater_than_end_ip	起始 IP 大於結束 IP。	嘗試在 IP 位址條件中將結束 IP 位址設定得大於起始 IP 位址。起始 IP 不能大於結束 IP。
start_date_can_not_be_larger_than_end_date	起始日期晚於結束日期。	嘗試在策略的時間條件中將結束日期設定得晚於起始日期。起始日期不能晚於結束日期。
policy_not_found_in_organization	在組織中未找到策略。嘗試在組織中找到非現有策略時出錯。	確保策略存在於指定的組織中。
insufficient_access_rights	使用者沒有足夠的存取權限。使用者沒有執行策略作業所需的足夠權限。	使用具有適當存取權限的使用者身份執行策略作業。
invalid_ldap_server_host	無效的 LDAP 伺服器主機。	變更在策略配置服務中輸入的無效 LDAP 伺服器主機。

amadmin 錯誤碼

下表描述 amadmin 指令行工具產生之錯誤碼，其會列示於 Access Manager 的除錯檔案中。

表 D–4 amadmin 錯誤碼

錯誤訊息	程式碼	說明/可能的原因	動作
nocomptype	1	引數太少。	確保在指令行中提供強制性引數 (--runasdn、--password、--passwordfile、--schema、--data 及 --addAttributes) 和它們的值。
file	2	未找到輸入 XML 檔案。	檢查語法並確保輸入 XML 有效。
nodnforadmin	3	遺漏 --runasdn 值的使用者 DN。	提供使用者 DN，做爲 --runasdn 的值。
noservicename	4	遺漏 --deletservice 值的服務名稱。	提供服務名稱做爲 --deleteservice 的值。
nopwdforadmin	5	遺漏 --password 值的密碼。	提供密碼，做爲 --password 的值。
nolocalename	6	未提供語言環境名稱。語言環境將預設爲 en_US。	請參閱語言環境清單的「線上說明」。
nofile	7	遺漏 XML 輸入檔案。	提供至少一個要處理的輸入 XML 檔案名稱。
invopt	8	一個或多個引數不正確。	檢查並確保所有引數均有效。若要取得有效引數集，請鍵入 amadmin --help。
oprfailed	9	作業失敗。	amadmin 失敗時，它會產生更精確的錯誤碼來指示特定錯誤。請參考那些更精確的錯誤碼以評估問題。
execfailed	10	無法處理請求。	amadmin 失敗時，它會產生更精確的錯誤碼來指示特定錯誤。請參考那些更精確的錯誤碼以評估問題。
policycreatexception	12	無法建立策略。	amadmin 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
policydelexception	13	無法刪除策略。	amadmin 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
smsdelexception	14	無法刪除服務。	amadmin 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。

表 D–4 amadmin 錯誤碼 *(續)*

錯誤訊息	程式碼	說明/可能的原因	動作
ldapauthfail	15	無法認證使用者。	確保使用者 DN 和密碼均正確。
parserror	16	無法剖析輸入 XML 檔案。	確保該 XML 已正確格式化並遵守 `amAdmin.dtd`。
parseiniterror	17	由於應用程式錯誤或剖析器初始化錯誤而導致無法剖析。	確保該 XML 已正確格式化並遵守 `amAdmin.dtd`。
parsebuilterror	18	由於無法建立具有指定選項的剖析器而導致無法剖析。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
ioexception	19	無法讀取輸入 XML 檔案。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
fatalvalidationerror	20	由於 XML 檔案爲無效檔案而導致無法剖析。	檢查語法並確保輸入 XML 有效。
nonfatalvalidationerror	21	由於 XML 檔案爲無效檔案而導致無法剖析。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
validwarn	22	檔案的 XML 檔案驗證警告。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
failedToProcessXML	23	無法處理 XML 檔案。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
nodataschemawarning	24	指令中沒有 `--data` 選項或 `--schema` 選項。	檢查並確保所有引數均有效。若要取得有效引數集，請鍵入 `amadmin --help`。
doctyperror	25	XML 檔案未依循正確的 DTD。	檢查 XML 檔案的 `DOCTYPE` 元素。
statusmsg9	26	由於無效的 DN、密碼、主機名稱或連接埠號而導致 LDAP 認證失敗。	確保使用者 DN 和密碼均正確。
statusmsg13	28	服務管理程式異常 (SSO 異常)。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
statusmsg14	29	服務管理程式異常。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
statusmsg15	30	模式檔案輸入串流異常。	`amadmin` 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。

表 D–4 amadmin 錯誤碼 *(續)*

錯誤訊息	程式碼	說明/可能的原因	動作
statusmsg30	31	策略管理程式異常 (SSO 異常)。	amadmin 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
statusmsg31	32	策略管理程式異常。	amadmin 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
dbugerror	33	指定了多個除錯選項。	應該僅指定一個除錯選項。
loginFalied	34	登入失敗。	amadmin 會產生異常訊息以指示特定錯誤。請參考那些異常訊息以評估問題。
levelerr	36	屬性值無效。	檢查 LDAP 搜尋的層級設定。它應該是 SCOPE_SUB 或是 SCOPE_ONE。
failToGetObjType	37	取得物件類型時出錯。	確保 XML 檔案中的 DN 有效並包含正確的物件類型。
invalidOrgDN	38	無效的組織 DN。	確保 XML 檔案中的 DN 有效且爲組織物件。
invalidRoleDN	39	無效的角色 DN。	確保 XML 檔案中的 DN 有效且爲角色物件。
invalidStaticGroupDN	40	無效的靜態群組 DN。	確保 XML 檔案中的 DN 有效且爲靜態群組物件。
invalidPeopleContainerDN	41	無效的使用者容器 DN。	確保 XML 檔案中的 DN 有效且爲使用者容器物件。
invalidOrgUnitDN	42	無效的組織單元 DN。	確保 XML 檔案中的 DN 有效且爲容器物件。
invalidServiceHostName	43	服務主機名稱無效。	確保用於擷取有效階段作業的主機名稱正確。
subschemaexception	44	子模式錯誤。	僅全域屬性和組織屬性支援子模式。
serviceschemaexception	45	無法找到服務的服務模式。	確保 XML 檔案中的子模式有效。
roletemplateexception	46	僅當模式類型爲動態時，角色範本才可爲 true。	確保 XML 檔案中的角色範本有效。
cannotAddusersToFileredRole	47	無法將使用者加入已篩選的角色。	確保 XML 檔案中的角色 DN 不是已篩選的角色。
templateDoesNotExist	48	範本不存在。	確保 XML 檔案中的服務範本有效。

表 D–4 amadmin 錯誤碼 (續)

錯誤訊息	程式碼	說明/可能的原因	動作
cannotAdduUersToDynamicGroup	49	無法將使用者加入動態群組。	確保 XML 檔案中的群組 DN 不是動態群組。
cannotCreatePolicyUnder-Container	50	無法在容器的子組織中建立策略。	確保要在其中建立策略的組織不是容器的子組織。
defaultGroupContainer-NotFound	51	未找到群組容器。	爲父系組織或容器建立群組容器。
cannotRemoveUserFrom-FilteredRole	52	無法從已篩選的角色中移除使用者。	確保 XML 檔案中的角色 DN 不是已篩選的角色。
cannotRemoveUsersFrom-DynamicGroup	53	無法從動態群組中移除使用者。	確保 XML 檔案中的群組 DN 不是動態群組。
subSchemStringDoesNotExist	54	子模式字串不存在。	確保子模式字串存在於 XML 檔案中。
defaultPeopleContainer-NotFound	59	您正試圖新增使用者到組織或容器。預設使用者容器不在組織或容器中。	確保預設使用者容器存在。
nodefaulturlprefix	60	--defaultURLPrefix 引數中找不到預設 URL 前綴	提供預設 URL 前綴。
nometaalias	61	--metaalias 引數中找不到預設中介別名	提供中介別名。
missingEntityName	62	未指定實體名稱。	提供實體名稱。
missingLibertyMetaInputFile	63	遺漏匯入中介資料的檔案名稱。	提供包含中介資料的檔案名稱。
missingLibertyMetaOutputFile	64	遺漏儲存匯出中介資料的檔案名稱。	提供儲存中介資料的檔案名稱。
cannotObtainMetaHandler	65	無法取得中介屬性的處理程式。指定的使用者名稱和密碼可能不正確。	確保使用者名稱和密碼均正確。
missingResourceBundleName	66	新增、檢視或刪除儲存在目錄伺服器中的資源套件時遺失資源套件名稱。	遺漏資源套件名稱
missingResourceFileName	67	遺失檔案名稱，該檔案包含新增資源套件到目錄伺服器企時的資源字串。	請提供有效的檔案名稱。
failLoadLibertyMeta	68	無法將 liberty 中介載入 Directory Server。	請再次檢查中介資料後再次載入。

索引