管理指南

Sun™ ONE Identity Server

版本 6.1

817-4410-10
2003 年 12 月

目錄

關於本指南

「*Sun*™ ONE *Identity Server* **管理指南**」提供有關如何自訂 Sun ONE Identity Server 及將其功能整合至組織的目前技術基礎架構的資訊。它還包含有關此產品及其 API 之程式方面的資訊。本前言包含以下小節：

本指南的讀者

本**管理指南**爲使用 Sun ONE 伺服器與軟體實施整合身份管理及網路存取平台的 IT 管理員和軟體開發人員設計。建議管理員瞭解以下技術：

- 輕型目錄存取協定 (LDAP)
- Java™
- JavaServer Pages™ (JSP)
- 超文字傳輸協定 (HTTP)
- 超文字標記語言 (HTML)
- 可延伸標記語言 (XML)

由於 Sun ONE Directory Server 在 Identity Server 部署中用作資料儲存區，因此管理員還應熟悉該產品隨附的說明文件。最新的 Directory Server 說明文件可於線上存取。

Identity Server 6.1 說明文件集

Identity Server 說明文件集分爲兩組核心手冊：Sun ONE Identity Server 6.1 核心應用程式手冊和 Sun ONE Identity Server 策略代理程式書籍。

Identity Server 核心說明文件

Identity Server 說明文件集包含以下標題：

- *Product Brief* 提供 Identity Server 應用程式及其特性與功能的概觀。
- **移轉指南**提供有關如何將現有資料和 Sun ONE 產品部署遷移至最新版 Identity Server 的詳細資訊。如需有關安裝 Identity Server 的說明，請參閱「*Sun Java Enterprise System 2003Q4* **安裝指南**」。
- **管理指南**描述如何使用 Identity Server 主控台，以及如何透過指令行管理使用者與服務資料。
- *Customization and API Guide* 介紹如何自訂 Identity Server 安裝。它還包含有關如何使用公用 API 在應用程式中增加新服務的說明。
- *Deployment Guide* 提供有關在現有資訊技術基礎架構中規劃 Identity Server 部署的資訊。
- **版次注意事項**可在產品發行之後於線上取得。它們匯集了各類最新資訊，包括對目前版次中新功能的描述、已知問題和限制、安裝注意事項，以及如何報告軟體或說明文件的問題。

於 Sun ONE 說明文件網站的 Identity Server 頁面之上，可找到**版次注意事項**更新及核心說明文件修改的連結。已更新的文件標示有修訂日期。

Identity Server 策略代理程式說明文件集

Identity Server 的策略代理程式可於不同的排程 (而不是伺服器產品本身) 上取得。因此，策略代理的說明文件集不在 Identity Server 說明文件核心集之中。本集包括以下標題：

- **網路策略代理程式指南**介紹如何在各種網路伺服器和代理伺服器上安裝和配置 Identity Server 策略代理程式。它還包含疑難排解以及每個代理程式的特定資訊。
- *J2EE* **策略代理程式指南**介紹如何安裝與配置可以保護各種託管 J2EE 應用程式的 Identity Server 策略代理程式。它還包含疑難排解以及每個代理程式的特定資訊。
- **版次注意事項**可在代理程式集發行之後於線上取得。每版代理程式類型一般都有一個**版次注意事項**檔案。**版次注意事項**匯集了各類最新資訊，包括對目前版次中新功能的描述、已知問題和限制、安裝注意事項，以及如何報告軟體或說明文件的問題。

於 Sun ONE 說明文件網站的策略代理程式頁面之上，可找到**版次注意事項**更新和策略代理程式說明文件的修改。已更新的說明文件標示有修訂日期。

您對說明文件的回饋

Sun Microsystems 和 Identity Server 的技術作者有志於改善其說明文件，並且歡迎任何意見和建議。請將意見用電子郵件發送至 `docfeedback@sun.com`。

本指南中使用的說明文件慣例

在 Identity Server 說明文件中，使用了某些印刷排版慣例和術語。以下幾節描述了這些慣例。

印刷排版慣例

本書使用以下印刷排版慣例：

- **斜體文字**用來表示書籍標題內容、新術語內容、強調內容以及依原義使用的文字。
- 固定間距字型用於範例程式碼和程式碼清單、API 和 語言元素 (如函數名稱和類別名稱)、檔案名稱、路徑名稱、目錄名稱、HTML 標記以及必須在螢幕上鍵入的任何文字。
- **斜體** *serif* **字型**用於程式碼和程式碼段，表示變數定位字元。例如，以下指令使用 *filename* 作爲 `gunzip` 指令引數的變數定位字元：

  `gunzip -d` *filename*`.tar.gz`

術語

下面是 Identity Server 說明文件集中使用的一般術語清單：

- *Identity Server* 指 Identity Server 和 Identity Server 軟體的任何安裝實例。
- **策略服務與管理服務**指安裝並執行於專屬部署容器 (如網路伺服器) 上的 Identity Server 元件和軟體的集體。
- *Directory Server* 指 Sun ONE Directory Server 的安裝實例。
- *Application Server* 指 Sun ONE Application Server 的安裝實例。
- *Web Server* 指 Sun ONE Web Server 的安裝實例。
- *IdentityServer_base* 是您安裝 Identity Server 的主目錄之變數定位字元。
- *DirectoryServer_base* 是您安裝 Sun ONE Directory Server 的主目錄之變數定位字元。
- *ApplicationServer_base* 是您安裝 Sun ONE Application Server 的主目錄之變數定位字元。
- *WebServer_base* 是安裝 Sun ONE Web Server 的主目錄之變數定位字元。
- **執行** *Identity Server* **的** *Web* **容器**指安裝策略服務與管理服務的專屬 J2EE 容器 (如 Web Server 或 Application Server)。

相關資訊

除了 Identity Server 隨附的說明文件，還有其他數個有用的說明文件集。表 0-1 列出了這些說明文件集及其他資訊來源。

表 0-1 相關 Sun ONE 資源的所在位置

資訊或資源	網際網路位置
Directory Server 說明文件	http://docs.sun.com/coll/S1_DirectoryServer_52
Web Server 說明文件	http://docs.sun.com/coll/S1_websvr61_en
Web Proxy Server 說明文件	http://docs.sun.com/prod/s1.webproxys#hic
Sun ONE 下載中心	http://wwws.sun.com/software/download/
Sun ONE 技術支援	http://www.sun.com/service/sunone/software/index.html
Sun ONE 專業服務資訊	http://www.sun.com/service/sunps/sunone/index.html
Sun 企業服務、Solaris 修補程式和支援	http://sunsolve.sun.com/
開發人員資訊	http://developers.sun.com/prodtech/index.html

Sun 不負責本文件所述協力廠商網站的可用性。Sun 對在 (或透過) 此類網站或資源取得的任何內容、廣告、產品或其他材料不做保證且不負有法律責任。Sun 對使用在 (或透過) 此類網站或資源取得的任何內容、商品或服務而導致的實際的或可能的損害或損失，或與此使用有關的任何實際的或可能的損害或損失不負有法律責任。

第 1 部分

Identity Server 主控台指南

這是「*Sun™ ONE Identity Server* **管理指南**」的第一部分。本部分論述 Identity Server 圖形使用者介面及如何在其中導覽。本部分包含以下章節：

第 1 章

產品概觀

本章提供 Sun™ ONE Identity Server 功能概觀。包含以下小節：

Sun ONE Identity Server

Sun ONE Identity Server 技術是用於網路身份的 Sun Open Net Environment (Sun ONE) 平台的一部分。Identity Server 是一組工具，用於充分利用 Sun ONE Directory Server (基於輕型目錄存取協定 [LDAP] 的資料儲存區) 的管理和安全潛能。Identity Server 將 Directory Server 與使用者認證以及單一登入功能整合，籍此增加資料安全性。它還允許管理員根據**角色** (一種項目群組機制，在使用者項目中作爲屬性出現) 來開始進行使用者項目管理。最後，開發者可以定義和管理眾多預設服務和定製服務的配置參數。可透過可自訂圖形使用者介面 (基於瀏覽器的 Identity Server 主控台) 存取所有這三項功能。

Identity Server 的功能

Identity Server 建立於 Directory Server 安裝之上。其設計概念是爲目錄管理員提供一個更一致更直觀的工作介面，並提供擴展 Directory Server 能力的功能。

服務配置

可以使用 Identity Server 服務管理元件指定預設商業服務以及自訂商業服務的配置參數。使用 XML 和 Identity Server 框架中定義的 DTD，服務開發人員可定義公司服務 (如郵件服務、記帳服務或記錄服務) 的參數，並管理服務的參數或 [**屬性**]。此外，Identity Server 還允許服務管理員定義這些屬性的值。

策略管理

Identity Server 還提供定義、修改或移除控制存取商業資源的規則的方法。這些規則統稱爲**策略**。

SAML

Identity Server 使用安全宣示標記語言 (SAML) 交換安全資訊。SAML 定義可延伸標記語言 (XML) 框架，以在提供此類資訊的不同供應商平台間實現相互可操作性。「*Sun ONE Identity Server Customization and API Guide*」中描述了 SAML 框架。

聯合管理

Identity Server 整合了聯合管理模組，以便利用自由聯盟專案開發的聯合網路身份開放式標準。

認證

Identity Server 爲使用者認證提供了外掛程式解決方案。認證特定使用者所需的條件是根據爲 Identity Server 企業中的每個組織配置的認證服務而定。使用者必須成功通過認證，才能存取 Identity Server 階段作業。

單一登入

一旦使用者通過認證，Identity Server 中用於單一登入 (SSO) 的 API 便會接管作業。每當認證的使用者嘗試存取受保護頁面時，SSO API 會依據使用者的認證憑證來確定該使用者是否擁有所需的權限。如果使用者有效，無需附加認證即可獲得對頁面的存取權。如果無效，系統將提示使用者再次認證。

策略代理程式

策略代理程式安裝在 Web 容器 (Sun ONE Web Server 或 Sun ONE Application Server) 中。它是 Identity Server 策略元件的特定實例。當使用者發出對受保護的網路伺服器上的網路資源的請求時，該代理程式會用作附加認證步驟。除了執行任何使用者認證檢查之外，資源還必須執行該認證。此代理程式保護網路伺服器，認證外掛程式則保護資源。

身份管理

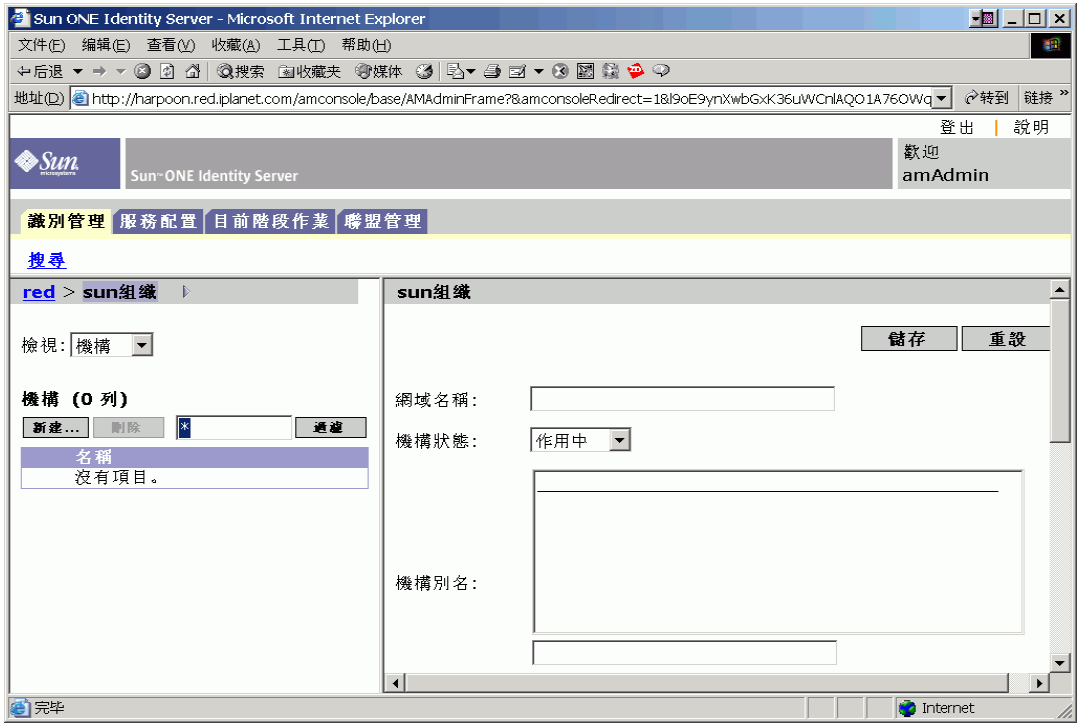
身份管理元件允許建立和管理與身份有關的物件。使用 Identity Server 主控台或指令行介面可定義、修改或刪除使用者物件、角色物件、群組物件、策略物件、組織物件、子組織物件和容器物件。主控台具有預設管理員，他們擁有不同等級的權限，可用來建立和管理組織、群組、容器、使用者、服務和策略。(可基於角色建立其他管理員。) 管理員是在 Directory Server 與 Identity Server 一同安裝時，在 Directory Server 內部定義的。這些管理員是：

- 頂層管理員，具有對 Identity Server 企業中所有項目的讀取存取權和寫入存取權。
- 頂層說明桌面管理員，具有對 Identity Server 企業內部所有項目的讀取存取權和對使用者密碼屬性的寫入存取權。
- 組織管理員，具有對其組織內所有項目的讀取存取權和寫入存取權。
- 組織說明桌面管理員，具有對其組織內所有項目的讀取存取權。
- 容器管理員，具有對所有群組管理員 (具有對其群組所有成員的讀取存取權和寫入存取權) 的讀取存取權和寫入存取權。

Identity Server 主控台

Identity Server 主控台分爲三部分：位置框架、導覽框架和資料框架。使用這三個框架，管理員可以導覽目錄、執行使用者配置和服務配置以及建立策略。

圖 1-1 Identity Server 主控台



標頭框架

標頭框架位於主控台頂端。標頭框架中的標籤可讓管理員在不同的管理模組檢視之間切換：

- 身份管理模組 - 可讓管理員建立和管理與身份有關的物件。
- 服務配置模組 - 可讓管理員配置 Identity Server 的預設服務。
- 目前階段作業模組 - 可讓管理員檢視目前階段作業資訊以及終止任一階段作業。
- 聯合管理模組 - 可使用自由聯盟專案開發的聯合網路身份開放式標準。

[**位置**] 欄位提供管理員在目錄樹中位置的路徑。該路徑作爲導覽之用。

[**歡迎**] 欄位顯示正執行主控台之使用者的名稱，並具有至該使用者設定檔的連結。

[**搜尋**] 連結顯示一個可讓使用者搜尋特定 Identity Server 物件類別之項目的介面。請使用下拉式功能表選取物件類型並輸入搜尋字串。搜尋表格中會傳回結果。允許使用萬用字元。

[**說明**] 連結會開啓一個瀏覽器視窗，其中包含有關身份管理、目前階段作業、聯合管理和本說明文件的第 3 部分 (「屬性參考指南」) 資訊。

[**登出**] 連結可讓使用者登出 Identity Server。

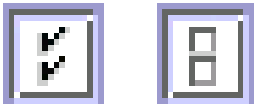
導覽框架

導覽框架位於 Identity Server 主控台的左側部分。**目錄物件**部分 (在灰色方塊內) 顯示目前開啓的目錄物件之名稱及其 [**屬性**] 連結。(導覽框架中顯示的大多數物件均有相應的 [**屬性**] 連結。選取此連結將會在右側的資料框架中描繪項目的屬性。) [檢視] 功能表列出所選目錄物件下的目錄。根據子目錄數，系統會提供分頁機制。

資料框架

資料框架位於主控台的右側部分。此處可顯示並配置所有物件屬性及其值，並可爲它們各自的群組、角色或組織選取項目。

提示 您可以按一下 [全部選取] 或 [全部取消選取] 圖示來選取所有項目或取消選取所有項目。



第 2 章

身份管理

本章描述 Sun™ ONE Identity Server 之身份管理功能。身份管理模組介面用於檢視、管理和配置所有 Identity Server 物件和身份。本章包含以下小節：

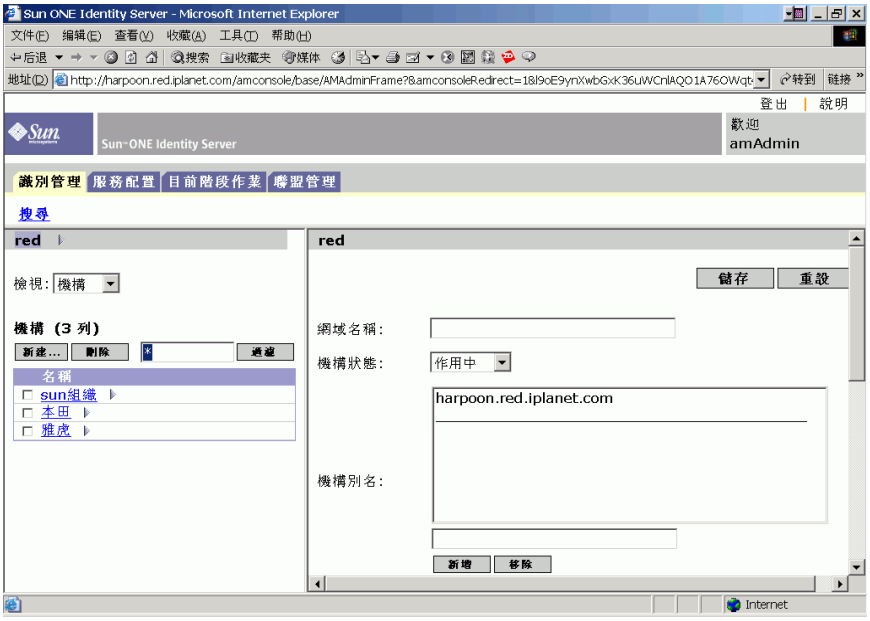
[身份管理] 介面

Identity Server 圖形使用者介面有兩個基本檢視。根據使用者登入的角色，可以存取 [身份管理] 檢視或 [使用者設定檔] 檢視。

[身份管理] 檢視

當具有管理角色的使用者被 Identity Server 認證時，預設檢視爲 [身份管理] 檢視。在該檢視中管理員可以執行管理工作。根據管理員的角色，管理工作可包括建立、刪除和管理物件 (使用者、組織、策略等)，以及配置服務。

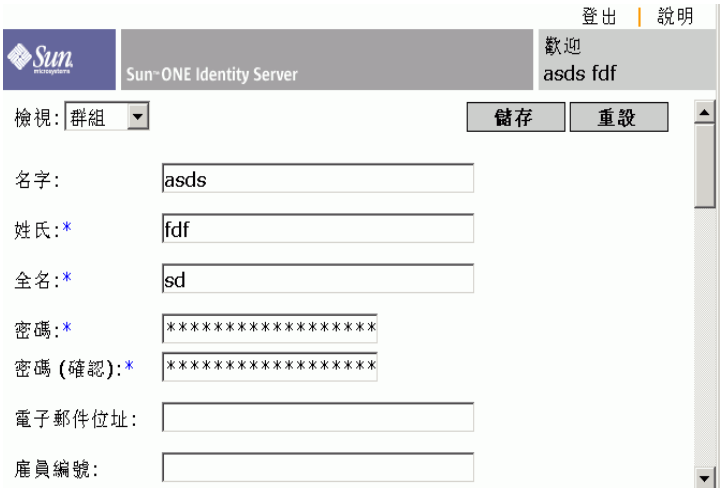
圖 2-1 顯示有組織屬性之 [身份管理] 檢視



[使用者設定檔] 檢視

當未被指定管理角色的使用者被 Identity Server 認證時，預設檢視爲該使用者自己的 [使用者設定檔] 檢視。在此檢視中，使用者可以修改其個人設定檔特定的屬性值。這包括 (但不僅限於) 名稱、住家地址和密碼。[使用者設定檔] 檢視中顯示的屬性可以延伸。如需有關加入物件與身份之自訂屬性的更多資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」。

圖 2-2 [使用者設定檔] 檢視



管理 Identity Server 物件

[使用者管理] 介面包含檢視和管理 Identity Server 物件 (組織、群組、使用者、服務、角色和策略) 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。

屬性功能

若要檢視或修改項目的屬性，請按一下物件名稱旁邊的 [屬性] 箭頭。它的屬性和相應的值會顯示在資料框架中。不同物件顯示不同屬性。

請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得有關如何延伸項目的屬性的資訊。

組織

該物件表示企業用來管理其部門與資源的階層式結構的頂層。在安裝過程中，Identity Server 會動態建立頂層組織 (安裝期間定義) 以管理 Identity Server 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. 從身份管理模組中的 [檢視] 功能表選擇 [組織]。
2. 在導覽框架中按一下 [新建]。

   [新建組織] 範本會顯示在資料框架中。
3. 在 [新建組織] 範本中輸入組織名稱的值。
4. 選擇 [作用中] 或 [非作用中] 狀態。

   預設爲 [作用中]。在組織存在期間，可以透過選取 [屬性] 圖示隨時變更該狀態。如果選擇 [非作用中]，則在登入組織時會停用使用者存取。
5. 如果需要，請輸入選擇性欄位的值。選擇性欄位包括：

   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，並且將 `123` 和 `abc` 定義爲別名，則您可使用以下任一 URL 登入該組織：

   ```
   http://machine.example.com/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example.com/UI/Login?org=abc
   ```

   ```
   http://machine.example.com/UI/Login?org=123
   ```

   網域名稱。輸入組織的完整網域名稱系統 (DNS) 名稱 (如果有)。

   DNS 別名。允許加入組織 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)。例如，如果您有一個名爲 `example.com` 的 DNS，並且將 `example1.com` 和 `example2.com` 定義成名爲 `exampleorg` 之組織的別名，則您可使用以下任一 URL 登入該組織：

   ```
   http://machine.example.com/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example1.com/UI/Login?=org=exampleorg
   ```

   ```
   http://machine.example2.com/UI/Login?org=exampleorg
   ```

唯一屬性清單。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，如果欄位包含以下屬性名稱清單：

```
PreferredDomain, AssociatedDomain
```

而且爲特定使用者將 `PreferredDomain` 定義爲 `http://www.example.com`，則對該 URL 此以逗號分隔的整個清單被定義爲唯一的。

系統強制所有子組織的唯一性。

6. 按一下 [建立]。

   新建的組織會顯示在導覽框架中。

刪除組織

1. 從身份管理的 [檢視] 功能表選擇 [組織]。

   會顯示所有建立的組織。若要顯示特定組織，請輸入搜尋字串，然後按一下 [過濾]。

2. 選取要刪除的組織名稱旁邊的核取方塊。

3. 按一下 [刪除]。

注意 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

透過策略的主題定義可將 Identity Server 物件加入到策略。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 [主題] 頁面中的主題。一旦定義了主題，策略即會套用於物件。如需更多資訊，請參閱第 81 頁的「修改策略」。

群組

群組表示具有共同功能、特性或興趣的使用者集合。通常，這種群組沒有關聯的權限。群組可以存在於兩個層級：組織中和其他受管理群組中 (作爲子群組)。可以將使用者靜態或動態地 (通過過濾) 加入受管理群組。

依訂閱確定成員身份

依訂閱指定群組成員身份時，會基於指定的 [受管理群組類型] 建立靜態群組。如果 [受管理群組類型] 的值爲［靜態］，群組成員會使用 groupOfNames 或 groupOfUniqueNames 物件類別加入群組項目中。如果 [受管理群組類型] 的值爲［動態］，特定 LDAP 過濾器會用於僅搜尋並傳回包含 memberof 屬性的使用者項目。如需更多資訊，請參閱第 157 頁的「受管理群組類型」。

依過濾確定成員身份

過濾的群組是使用 LDAP 過濾器建立的動態群組。所有項目都會透過過濾器過濾並動態指定給群組。過濾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，可以使用過濾器傳回包含建立編號屬性的所有使用者的清單。

注意 **依預設，受管理群組類型為動態。您可在管理服務配置中變更該預設。**

建立受管理群組

1. 導覽至將要建立群組的組織 (或群組)。
2. 從 [檢視] 功能表選擇 [群組]。
3. 按一下 [新建]。
4. 從資料框架中選取群組類型。

   如果要建立靜態訂閱群組，請選取 [依訂閱確定成員身份]。

   a. 在 [名稱] 欄位中輸入群組的名稱。按一下 [下一步]。
   b. 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。
   c. 透過選取 [從成員清單加入]，將使用者加入群組。
   d. 輸入搜尋條件，然後按一下 [過濾]。當傳回使用者清單時，選取希望加入的使用者並按一下 [提交]。將使用者加入群組是選擇性的。可以在群組建立以後再加入使用者。
   e. 按一下 [建立]。

如果要建立動態 (已被 LDAP 過濾) 群組，請選取 [依過濾確定成員身份]。

a. 在 [名稱] 欄位中輸入群組的名稱。按一下 [下一步]。

b. 建構 LDAP 搜尋過濾器。

c. 用於建構過濾器的欄位使用 OR 或 AND 運算子。UI 中列出的所有欄位都會用到。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。

d. 按一下 [建立]。

刪除受管理群組

1. 導覽至群組所屬的組織。
2. 從 [檢視] 功能表選擇 [群組]。
3. 選取要刪除的群組名稱旁邊的核取方塊。
4. 按一下 [刪除]。

注意 應該將 Identity Server 與 Directory Server 一起配置，以使用參考完整性外掛程式。啟用參考完整性外掛程式時，它會在刪除作業或重新命名作業之後，立即對指定的屬性執行完整性更新。如此便可以保持整個資料庫中相關項目之間的關係。資料庫索引可以提昇搜尋 Directory Server 的效能。如需有關啟用此外掛程式的更多資訊，請參閱「*Sun One Identity Server Migration Guide*」。

將群組加入到策略

透過策略的主題定義可將 Identity Server 物件加入到策略。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 [主題] 頁面中的主題。一旦定義了主題，策略即會套用於物件。如需更多資訊，請參閱第 81 頁的「修改策略」。

使用者

使用者表示個人的身份。透過 Identity Server 身份管理模組，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；還可以將服務指定給使用者。

建立使用者

1. 導覽至要在其中建立使用者的組織、容器或個人容器 (或者您可以從使用者建立頁面中選取個人容器)。
2. 從 [檢視] 功能表選擇 [使用者]。
3. 按一下 [新建]。

   這會使 [新建使用者] 頁面顯示在資料框架中。
4. 輸入必備屬性與任何選擇性欄位的值。

   如需有關使用者設定檔屬性的資訊，請參閱第 277 頁的「使用者屬性」。
5. 按一下 [建立]。

將使用者加入到角色和群組

1. 導覽至要修改的使用者所屬的組織。
2. 從 [檢視] 功能表選擇 [使用者]。
3. 在導覽框架中，選取您希望修改的使用者，然後按一下 [屬性] 箭頭。
4. 從資料框架的 [檢視] 功能表，選取 [角色] 或 [群組]。

   [使用者] 檢視允許您修改任何定義了使用者服務的屬性。
5. 選取您希望在其中加入使用者的角色或群組，然後按一下 [儲存]。已過濾的角色和群組無法顯示。

將服務加入使用者

1. 導覽至要修改的使用者所屬的組織。
2. 從 [檢視] 功能表選擇 [使用者]。
3. 在導覽框架中，選取您希望修改的使用者，然後按一下 [屬性] 箭頭。
4. 從資料框架的 [檢視] 功能表，選取 [服務]。
5. 按一下 [加入] 以選取要指定給使用者的服務。
6. 按一下 [儲存]。

刪除使用者

1. 導覽至使用者所屬的組織。
2. 從 [檢視] 功能表選擇 [使用者]。
3. 選取要刪除的使用者名稱旁邊的核取方塊。
4. 按一下 [刪除]。

將使用者加入到策略

透過策略的主題定義可將 Identity Server 物件加入到策略。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 [主題] 頁面中的主題。一旦定義了主題，策略即會套用於物件。如需更多資訊，請參閱第 81 頁的「修改策略」。

服務

啓動組織或容器 (容器與組織的運作方式相同) 服務的程序包含兩個步驟。首先，需要將服務註冊到組織。註冊服務以後，必須建立一個專門爲該組織配置的範本。如需其他資訊，請參閱第 3 章「服務配置」。

注意 新服務必須首先透過指令行的 `amadmin` 匯入 Identity Server。如需有關匯入服務的 XML 綱目之資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」。

註冊服務

1. 導覽至要加入服務的組織。

   從身份管理模組的 [檢視] 功能表選擇 [組織]，然後從導覽框架選取該組織。位置路徑會顯示預設頂層組織與選擇的組織。

2. 從 [檢視] 功能表選擇 [服務]。

3. 按一下 [註冊]。

   資料框架中會顯示可以註冊到該組織的服務清單。

4. 選取將要加入的服務旁邊的核取方塊。

5. 按一下 [註冊]。已註冊的服務會顯示在導覽框架中。

注意 僅有為頂層組織註冊的服務才會在角色層級顯示。

建立服務的範本

1. 導覽至註冊的服務所屬的組織或角色。

   從身份管理模組的 [檢視] 功能表選擇 [組織]，然後從導覽框架選取該組織。

2. 從 [檢視] 功能表選擇 [服務]。

3. 按一下要啓動的服務名稱旁邊的屬性圖示。

   資料框架會顯示訊息：**沒有適用於該服務的範本。要建立範本嗎？**

4. 按一下 [建立]。

   即爲父系組織或角色的該服務建立範本。資料框架中會顯示該服務的預設屬性和值。第 153 頁的「屬性參考指南」中描述了預設服務的屬性。

5. 接受或修改預設值，然後按一下 [儲存]。

取消註冊服務

1. 導覽至要移除的服務所屬的組織。

   從身份管理模組的 [檢視] 功能表選擇 [組織]，然後從導覽框架選取該組織。

2. 從 [檢視] 功能表選擇 [服務]。
3. 選取要移除的服務的核取方塊。
4. 按一下 [取消註冊]。

注意 如果服務已在子組織層級註冊，則無法在父系組織層級取消註冊。

角色

角色是一種 Directory Server 項目機制，與**群組**概念類似。群組具有成員；角色也具有成員。角色的成員是擁有角色的 LDAP 項目。角色本身的條件定義爲具有屬性的 LDAP 項目，由該項目的 [識別名稱 (DN)] 屬性識別。Directory Server 具有大量不同類型的角色，但是 Identity Server 僅可管理其中的一種：受管理角色。

注意 其他 Directory Server 角色類型仍可用於目錄部署；只是無法由 Identity Server 主控台來管理。其他 Directory Server 類型則可用於策略的主題定義。如需有關策略主題之更多資訊，請參閱第 78 頁的「策略管理」。

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 URL 策略代理程式服務屬性的承包人角色。新承包人啓動時，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。如果承包人後來成爲全職雇員，管理員只需爲該使用者重新指定不同的角色。

Identity Server 使用角色來實施存取控制指令。初次安裝時，Identity Server 會配置定義管理員權限的存取控制指令 (ACI)。然後會在角色 (例如組織管理角色與組織說明桌面管理角色) 中指定這些 ACI，這些角色在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 [顯示使用者角色] 屬性，使用者才可檢視指定給他們的角色。如需更多資訊，請參閱第 165 頁的「顯示使用者的角色」。

與群組相似，角色可以透過過濾建立，或者以靜態方式建立。

過濾的角色。過濾的角色是使用 LDAP 過濾器建立的動態角色。在角色建立時，所有使用者都會透過過濾器過濾並指定給角色。過濾器會尋找項目中的任何屬性值對 (例如 `ca=user*`)，並自動將包含屬性的使用者指定給角色。

靜態角色。與過濾的角色不同，靜態角色可以在建立角色時不加入使用者的情況下建立。這樣，在將特定使用者加入給定角色時，您可以進行更多控制。

建立過濾的角色

1. 在導覽框架中，移至要在其中建立角色的組織。
2. 從 [檢視] 功能表選擇 [角色]。

   配置組織時，預設角色集會被建立並顯示在導覽框架中。

   如需這些角色的描述，請參閱 「屬性參考」一節的第 160 頁的 「動態管理員角色 ACI」。
3. 在導覽框架中按一下 [新建]。[新建角色] 範本會顯示在資料框架中。
4. 選取 [過濾的角色]，然後輸入名稱。按一下 [下一步]。
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確定在 DIT 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。第 158 頁的 「預設角色權限 (ACI)」小節中論述了這些權限。(顯示的預設權限未依特定順序排列。)

   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. 輸入搜尋條件資訊。這些欄位包括：

   邏輯運算子。允許您指定您希望過濾的任何欄位中應包含的運算子。AND 傳回符合所有指定欄位的使用者。OR 傳回符合任何指定欄位之一的使用者。

   使用者 ID。依據使用者 ID 搜尋使用者。

   名字。依據其名字搜尋使用者。

   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。依據其狀態 (作用中或非作用中) 搜尋使用者。

   或者，您可以選取 [進階] 按鈕以自行定義過濾器屬性。例如：

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   如果過濾器保留爲空白，依預設會建立以下角色：

   ```
   (objectclass = inetorgperson)
   ```

   按一下 [重設] 以清除過濾器屬性，或者按一下 [取消] 以取消角色建立程序。

9. 按一下 [建立] 以基於過濾條件開始搜尋。過濾條件所定義的使用者會自動指定給角色。

建立靜態角色

1. 在導覽框架中，移至要在其中建立角色的組織。
2. 從 [檢視] 功能表選擇 [角色]。

   配置組織時，預設角色集會被建立並顯示在導覽框架中。

   如需這些角色的描述，請參閱「屬性參考」一節的第 160 頁的「動態管理員角色 ACI」。
3. 在導覽框架中按一下 [新建]。[新建角色] 範本會顯示在資料框架中。
4. 選取 [靜態角色]，然後輸入名稱。按一下 [下一步]。
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確定在 DIT 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。第 158 頁的「預設角色權限 (ACI)」小節中論述了這些權限。(顯示的預設權限未依特定順序排列。)

   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. 按一下 [建立]。

   建立的角色會顯示於導覽框架中，而角色的狀態資訊顯示在資料框架中。

   角色可用的服務是從該角色的父系組織繼承的。如果尚不存在角色的服務範本，可以透過按一下 [編輯] 連結建立範本。如果服務範本已經存在，會顯示服務屬性，並且可以配置這些屬性。如需更多資訊，請參閱第 48 頁的「自訂角色的服務」。

將使用者加入到靜態角色

1. 選取要修改的角色，然後按一下 [屬性] 箭頭。
2. 從資料框架中的 [檢視] 功能表選擇 [使用者]。
3. 按一下 [加入]。
4. 輸入搜尋條件資訊。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：

   邏輯運算子。允許您指定您希望過濾的任何欄位中應包含的運算子。AND 傳回符合所有指定欄位的使用者。OR 傳回符合任何指定欄位之一的使用者。

   使用者 ID。依據使用者 ID 搜尋使用者。

   名字。依據其名字搜尋使用者。

   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。依據其狀態 (作用中或非作用中) 搜尋使用者。

   依據值傳回使用者。允許您指定搜尋傳回的值。

5. 按一下 [過濾] 以開始搜尋。
6. 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。
7. 按一下 [儲存]。

   使用者即會指定給角色。

注意 可以透過 [角色] 設定檔頁面和/或 [使用者] 設定檔頁面將使用者加入角色。

從角色移除使用者

1. 導覽至包含要修改之角色的組織。

   從身份管理模組的 [檢視] 功能表選擇 [組織]，然後從導覽框架選取該組織。
2. 從 [檢視] 功能表選擇 [角色]。
3. 選取要修改的角色。
4. 從 [檢視] 功能表選擇 [使用者]。
5. 選取要移除的使用者核取方塊。
6. 按一下 [移除]。

   使用者即會從角色中移除。

注意 應該將 Identity Server 與 Directory Server 一起配置，以使用參考完整性外掛程式。啟用參考完整性外掛程式時，它會在刪除作業或重新命名作業之後，立即對指定的屬性執行完整性更新。如此便可以保持整個資料庫中相關項目之間的關係。資料庫索引可以提昇搜尋 Directory Server 的效能。如需有關啟用此外掛程式的更多資訊，請參閱「*Sun One Identity Server Migration Guide*」。

將角色加入到策略

透過策略的主題定義可將 Identity Server 物件加入到策略。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 [主題] 頁面中的主題。一旦定義了主題，策略即會套用於物件。如需更多資訊，請參閱第 81 頁的「修改策略」。

自訂角色的服務

可以基於各個角色自訂角色可用的服務，以及服務屬性的存取層級。使用 [一般] 檢視，管理員可以自訂 [服務] 和 [使用者] 頁面，並建立僅可存取特定服務的服務管理員。例如，管理員可以拒絕對給定角色使用者服務中一個或多個屬性的寫入存取，擁有該角色的使用者亦無法修改這些屬性。透過授權存取所有策略服務而拒絕存取其他服務，可以建立策略管理員角色。擁有策略管理員角色的管理員隨後將能夠建立和指定策略，但是無法執行使用者管理工作。

爲了顯示服務，您必須在組織層級註冊服務。加入到角色的使用者將繼承角色的服務屬性。

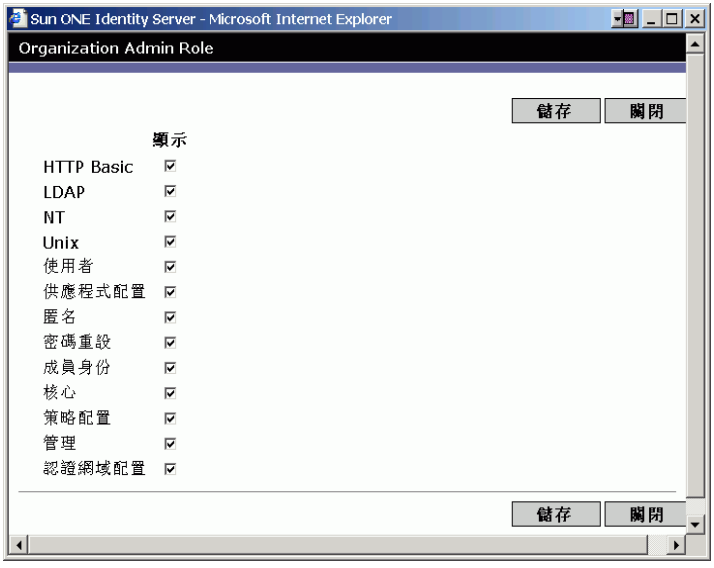
自訂服務存取

1. 針對要修改的角色按一下 [屬性] 箭頭。
2. 從 [檢視] 功能表選取 [一般]。
3. 在 [角色屬性] 頁面中，按一下 [服務] 清單中的 [編輯]。

   系統會顯示 [服務存取] 頁面，如圖 2-3 中所示。
4. 透過按一下 [顯示] 欄中的服務名稱，選擇要授與角色的服務。依預設，一個角色可以存取所有服務。
5. 按一下 [儲存]。

注意 當對某項服務的存取遭到拒絕時 (未核取)，系統將不會在 Identity Server 主控台中為擁有該角色的使用者顯示該服務。另外，不能註冊或取消註冊使用者，不能指定使用者的服務，也不能建立、刪除、檢視或修改 [服務] 範本。

圖 2-3 [服務存取] 頁面



自訂屬性存取

1. 在 [角色屬性] 頁面中，按一下 [服務屬性] 清單中的 [編輯]。系統會顯示 [屬性存取] 頁面，如圖 2-4 中所示。
2. 使用 [跳至] 功能表顯示特定服務的屬性。
3. 透過選取 [讀取 / 寫入] 或 [唯讀] 核取方塊指定屬性的存取層級。
4. 按一下 [儲存]。

注意 如果對於某種給定的屬性，[讀取/寫入] 和 [唯讀] 選項均未選取，則會拒絕對該屬性的讀取或寫入存取。

圖 2-4 [屬性存取] 頁面

如需有關特定服務屬性的更多資訊，請參閱本指南的第 3 部分 「**屬性參考指南**」。

刪除角色

1. 導覽至包含要刪除角色的組織。

   從身份管理的 [檢視] 功能表選擇 [組織]，然後從導覽框架選取該組織。位置路徑會顯示預設頂層組織與選擇的組織。

2. 從 [檢視] 功能表選擇 [角色]。
3. 選取角色名稱旁邊的核取方塊。
4. 按一下 [刪除]。

策略

策略會定義規則，以幫助保護組織的網路資源。雖然可以透過身份管理模組來建立、修改和刪除策略，第 78 頁的「策略管理」中仍描述了其程序。

容器

當由於物件類別與屬性的差異而無法使用組織項目時，將使用容器項目。請切記，Identity Server 容器項目與 Identity Server 組織項目不必等同於 LDAP 物件類別 `organizationalUnit` 與 `organization`。它們是抽象的 Identity 項目。理想情況下，將使用組織項目而不是容器項目。

注意 容器的顯示是選擇性的。若要檢視容器，必須在 Identity Server 管理服務中選取 [在功能表中顯示容器]。如需更多資訊，請參閱第 157 頁的「在功能表中顯示容器」。

建立容器

1. 導覽至要在其中建立新容器的組織或容器。

   從 [檢視] 功能表選取 [容器]。

2. 按一下 [新建]。

   [容器] 範本會顯示在資料框架中。

3. 輸入要建立的容器之名稱。

4. 按一下 [建立]。

刪除容器

1. 導覽至包含要刪除容器的組織或容器。

2. 從 [檢視] 功能表選擇 [容器]。

3. 選取要刪除的容器名稱旁邊的核取方塊。

4. 按一下 [刪除]。

注意 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。

個人容器

個人容器是預設的 LDAP 組織單元。在組織內建立使用者時，所有使用者均會指定給該容器。可以在組織層級和個人容器層級找到個人容器 (作爲子個人容器)。它們僅可包含其他個人容器與使用者。如果需要，可以將附加個人容器加入組織。

注意 個人容器的顯示是選擇性的。若要檢視個人容器，必須在 Identity Server 管理服務中選取 [顯示個人容器]。如需更多資訊，請參閱第 156 頁的 「顯示個人容器」。

建立個人容器

1. 導覽至要在其中建立新個人容器的組織或個人容器。

   從 [檢視] 功能表選取 [個人容器]。

2. 按一下 [新建]。

   [個人容器] 範本會顯示在資料框架中。

3. 輸入要建立的個人容器名稱。

4. 按一下 [建立]。

刪除個人容器

1. 導覽至包含要刪除的個人容器之組織或個人容器。

2. 從 [檢視] 功能表選擇 [個人容器]。

3. 選取要刪除的個人容器名稱旁邊的核取方塊。

4. 按一下 [刪除]。

注意 刪除一個個人容器將會同時刪除該個人容器中存在的所有物件。包含所有使用者和子個人容器。

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。

注意 群組容器的顯示是選擇性的。若要檢視群組容器，您必須在 Identity Server 管理服務中選取 [顯示群組容器]。如需更多資訊，請參閱第 157 頁的「顯示群組容器」。

建立群組容器

1. 導覽至包含要建立的群組容器之組織或群組容器。
2. 從 [檢視] 功能表選擇 [群組容器]。

   組織建立期間會建立預設群組容器「群組」。
3. 按一下 [新建]。
4. 在 [名稱] 欄位中輸入值，然後按一下 [建立]。

   新建群組容器會顯示在導覽框架中。

刪除群組容器

1. 導覽至包含要刪除的群組容器之組織。
2. 從 [檢視] 功能表選擇 [群組容器]。

   預設群組容器「群組」及所有建立的群組容器會顯示在導覽框架中。
3. 選取要刪除的群組容器旁邊的核取方塊。
4. 按一下 [刪除所選項目]。

第 3 章

服務配置

本章描述 Sun™ ONE Identity Server 之服務管理功能。[服務配置] 介面除了用於配置 Identity Server 主控台顯示設定以外，還用於檢視、管理和配置所有 Identity Server 服務及其值 (預設和自訂)。本章包含以下小節：

服務的定義

服務是以共用名稱定義的一組屬性。這些屬性定義服務向組織提供的參數。例如，開發薪水帳冊服務時，開發者可能會決定包括定義員工名稱、時薪和免稅的屬性。將該服務註冊到組織後，該組織便可使用這些屬性來配置其項目。

Identity Server 使用可延伸標記語言 (XML) 定義服務。服務管理服務文件類型定義 (`sms.dtd`) 定義服務 XML 檔案的結構。該檔案位於以下目錄：

IdentityServer_base`/SUNWam/dtd/`

如需有關定義 Identity Server 服務的更多資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」。

Identity Server 服務

與 Identity Server 一同提供的預設服務由位於以下目錄的 XML 檔案定義：

IdentityServer_base/SUNWamconfig/xml

或

/etc/opt/SUNWam/config/xml

透過 [服務配置] 介面配置時，有些服務會定義 Identity Server 應用程式的值。其他服務會註冊到在 Identity Server 內配置的特定組織，並用來定義該組織的預設值。

管理服務

管理服務允許在應用程式層級 (類似於 Identity Server 應用程式的 [**偏好設定**] 或 [**選項**] 功能表) 和已配置組織層級 (已配置組織特定的 [**偏好設定**] 或 [**選項**]) 上對主控台進行配置。

認證服務

存在十個認證模組，其中包括一個基準模組。這可讓管理員有機會選擇每個已定義組織可以用於驗證使用者授權的方法。

匿名

該模組允許在不指定使用者名稱和密碼的情況下登入。匿名連線可有限存取伺服器，並由管理員自訂。

基於證書

該模組允許透過個人數位證書 (PDC) 登入。

注意 6.1 版的 Application Server 部署不支援證書認證服務。

核心

該模組是 Identity Server 認證服務的一般配置基準。必須對它進行註冊和配置，以使用任何特定服務。它可讓管理員定義預設值，這些預設值將會被用於那些未在匿名、基於證書、HTTPBasic、LDAP、成員身份、NT、RADIUS、SafeWord、SecurID 和 Unix 服務中專門設定的值。

HTTP Basic

該模組使用基本認證，即 HTTP 協定的內建認證支援。

LDAP

該模組允許使用 LDAP 連結進行認證，LDAP 連結是將密碼與特定 LDAP 項目相關聯的作業。

成員身份 (自行註冊)

該模組可讓新使用者自行註冊，以透過登入和密碼進行認證。

NT

該模組允許使用 Windows NT™/2000™ 伺服器對使用者進行認證。爲了實現 NT 認證模組，必須下載並安裝 Samba Client (smbclient) 2.2.2。

RADIUS

該模組允許使用外部遠端認證撥入使用者服務 (RADIUS) 伺服器認證使用者。

爲使 RADUIS 認證服務與 Sun ONE Application Server 正確配合使用，您必須配置 Application Server 的 `service.policy` 檔案。如需此作業的說明，請參閱第 89 頁的「認證選項」。

SafeWord

該模組允許使用 Secure Computing 的 SafeWord™ 或 SafeWord PremierAccess™ 認證伺服器對使用者進行認證。

爲使 SafeWord 認證服務與 Sun ONE Application Server 正確配合使用，您必須配置 Application Server 的 `service.policy` 檔案。如需此作業的說明，請參閱第 89 頁的「認證選項」。

SecurID

該模組允許使用 RSA ACE/Server® 認證軟體和 SecurID® 認證程式對使用者進行認證。Solaris x86 上不支援此服務。

Unix

該模組允許使用 Unix® 伺服器和使用者的 UNIX 識別和密碼對使用者進行認證。

注意 Windows 2000 平台不支援 Unix 認證服務。

認證配置服務

認證配置服務可讓您配置角色、使用者、服務和組織的認證，以及設定決定認證模組優先順序的規則。

用戶端偵測服務

用戶端偵測服務可讓 Identity Server 偵測正在存取之瀏覽器的用戶端類型，並可讓管理員依照用戶端類型加入和配置裝置。

全域設定服務

全域設定包含配置 Identity Server 以適應不同字元集的屬性。

記錄服務

記錄服務是管理員爲 Identity Server 應用程式記錄功能配置值的地方。範例包括日誌檔大小和日誌檔位置。

命名服務

命名服務用來獲得和設定 URL、外掛程式、配置以及對各種其他 Identity Server 服務 (如階段作業、認證和記錄) 的請求通知。

密碼重設服務

密碼重設服務可讓使用者接收遺忘密碼或重設密碼，以便存取受 Identity Server 保護的給定服務或應用程式。由頂層管理員定義的密碼重設服務屬性控制使用者驗證憑證 (格式爲「保密問題」)、控制新密碼或現有密碼通知的機制以及爲不正確的使用者驗證設定可能的鎖定間隔時間。

平台服務

在平台服務中，附加伺服器可以加入到 Identity Server 配置以及套用於 Identity Server 應用程式頂層的其他選項中。

策略配置服務

策略配置服務定義策略框架在策略管理和策略評估期間要使用的值。

SAML 服務

安全宣示標記語言 (SAML) 服務定義在提供認證和認證服務的安全授權機構之間交換安全宣示的框架，以實現跨不同平台的相互可操作性。

階段作業服務

階段作業服務爲經認證的使用者階段作業 (如最長階段作業時間和最長閒置時間) 定義值。

使用者服務

預設使用者偏好設定透過使用者服務來定義。(它們包括時區、語言環境和啓動檢視的 DN) 。

屬性類型

組成 Identity Server 服務的屬性分爲以下幾種類型：*Dynamic*、*Policy*、*User*、*Organization* 或 *Global*。使用這些類型將每種服務中的屬性再劃分，可更一致地安排服務綱目、更輕鬆地管理服務參數。

動態屬性

動態屬性可指定至 Identity Server 配置的角色或組織。如果將角色指定給使用者或在組織中建立使用者，則動態屬性會成爲該使用者的一個特徵。例如，爲組織的員工建立角色。該角色可能包含該組織的地址和傳真號碼，這兩項內容對所有員工都是靜態的。將此角色指定給每位員工時，這些動態屬性會由每位員工繼承。

使用者屬性

這些屬性會直接指定給每位使用者。它們不是繼承自角色或組織，通常對於每位使用者都有所不同。使用者屬性範例包括 `userid`、`employee number` 和 `password`。透過修改 `amUser.xml` 檔案，可以在使用者服務中加入或移除使用者屬性。如需更多資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」。

組織屬性

組織屬性僅指定給組織。在這一方面，它們的作用類似動態屬性，但不同於動態屬性，因爲它們不是由子樹中的項目所繼承的。此外，沒有與組織屬性相關的物件類別。認證服務中列出的屬性被定義爲組織屬性，因爲認證是在組織層級而不是在子樹或使用者層級完成的。

全域屬性

全域屬性套用於整個 Identity Server 配置。由於全域屬性旨在自訂 Identity Server 應用程式，因此無法套用於使用者、角色或組織。在 Identity Server 配置中只有一個全域屬性的實例。沒有與全域屬性相關的物件類別。全域屬性的範例包括日誌檔大小、日誌檔位置、連接埠號或 Identity Server 可用來存取資料的伺服器 URL。

策略屬性

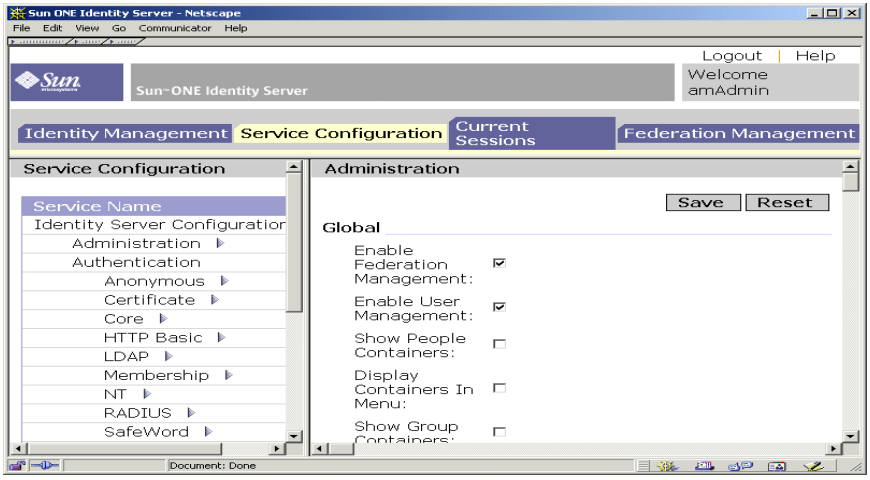
策略屬性指定與服務關聯的存取控制動作 (或權限)。規則被加入至策略時，即成爲規則的一部分了。

[服務配置] 介面

可透過服務配置模組來配置和管理服務。不包括在 Identity Server 預設服務套裝軟體中的組織特定的服務可使用 XML (基於 Identity Server 服務文件類型定義或 DTD) 來寫入並加入到在 [其他配置] 標頭下的介面中。如需有關如何完成此作業的說明，請參閱第 3 部分 「屬性參考指南」，其中描述了預設服務及其相應屬性的定義。

服務配置模組用於顯示全域層級上的服務配置。也就是說，它可用於檢視 Identity Server 中所有可用服務 (無論是否註冊) 的預設配置。服務被組織註冊和啓動後，指定給該服務的初始預設資料會顯示在該服務的 [服務配置] 頁面中。圖 3-1 爲圖形使用者介面的螢幕快照。

圖 3-1 [服務配置] 檢視



可透過選擇服務配置模組來存取 [服務配置] 檢視。導覽框架將會顯示所有已定義的 Identity Server 服務之清單。若要爲某項服務設定全域預設值，請選取該服務名稱旁邊的 [屬性] 箭頭。該服務的屬性將顯示在資料框架中。

第 4 章

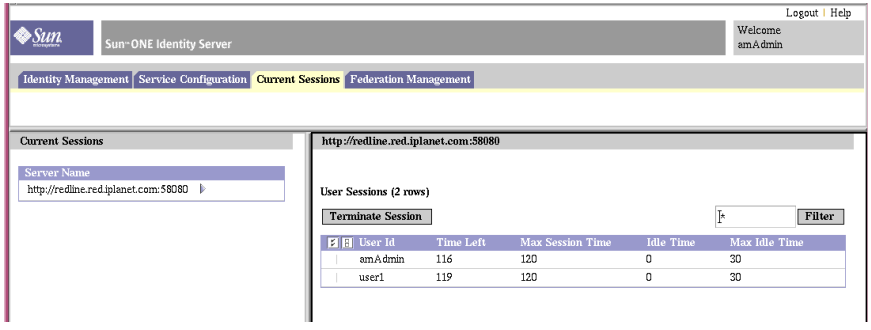
目前階段作業

本章描述 Sun™ ONE Identity Server 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。

[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 Identity Server 的任何使用者之階段作業資訊。

圖 4-1 [目前階段作業] 介面



階段作業管理框架

階段作業管理框架顯示目前受管理的 Identity Server 名稱。

階段作業資訊視窗

階段作業資訊視窗顯示目前登入至 Identity Server 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]。顯示必須重新認證之前，使用者所具有的此階段作業的剩餘時間 (以分鐘計算)。

[最大階段作業時間]。顯示階段作業過期之前使用者可以登入，並且必須重新認證以重新取得存取權限的最大時間 (以分鐘計算)。

[閒置時間]。顯示使用者已閒置的時間 (以分鐘計算)。

[最大閒置時間]。顯示在必須重新認證之前，使用者可以閒置的最大時間 (以分鐘計算)。

時間限制由管理員在階段作業管理服務中定義。請參閱第 275 頁的「階段作業服務屬性」，以取得更多資訊。

在 [使用者 ID] 欄位中輸入字串，然後按一下 [過濾]，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 [重新顯示] 按鈕，將更新使用者階段作業顯示。

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。若要如此，請：

1. 選取您要終止的使用者階段作業。
2. 按一下 [終止]。

第 5 章

聯合管理

本章描述 Sun™ ONE Identity Server 的 [聯合管理] 介面功能。[聯合管理] 介面提供了一種檢視、管理和配置有關認證網域和供應程式之複合資料的方法。

不再支援自由聯盟專案規格 1.0 中概述的功能。由於實際上沒有 1.0 部署，因此這不會造成嚴重影響。

本章包含以下小節：

注意 本章所述屬性欄位之範例資料可在以下預設位置找到：

IdentityServer_base/SUNWam/samples/liberty

認證網域和供應程式概觀

聯合管理模組提供一個介面，用於建立、修改和刪除認證網域、遠端供應程式以及託管供應程式。以下步驟說明基本的聯合管理模型：

1. 建立認證網域。
2. 建立一個或多個屬於已建立的認證網域的託管供應程式。

3. 建立一個或多個屬於已建立的認證網域的遠端供應程式。還必須包括遠端供應程式的複合資料。
4. 建立供應程式之間的信任關係。託管供應程式可選擇信任屬於同一認證網域的託管或遠端供應程式子集。

以下各節說明如何建立和配置認證網域、遠端供應程式以及託管供應程式。

認證網域

本節描述如何建立、修改和刪除認證網域。

建立認證網域

1. 從聯合管理模組的 [檢視] 功能表中，選擇 [認證網域]。
2. 在導覽框架中按一下 [新建]。

   [建立認證網域] 會顯示在資料框架中。
3. 在 [建立認證網域] 視窗中輸入認證網域的名稱。
4. 輸入用於描述認證網域的值。
5. 輸入寫入器服務 URL 的值。

   寫入器服務 URL 指定在共用網域中寫入 Cookie 的寫入器服務位置。例如，如果 example.com 是共用網域，則 URL 可能爲：

   ```
   http://example.com:8080/liberty/WriterServlet
   ```
6. 輸入讀取器服務 URL 的值。

   讀取器服務 URL 指定從共用網域讀取 Cookie 的服務位置。
7. 選擇 [作用中] 或 [非作用中] 狀態。

   預設值爲 [作用中]。在認證網域存在期間，可以透過選取 [屬性] 圖示隨時變更該狀態。選擇 [非作用中] 會停用認證網域中與目前安裝的 Identity Server 有關的「自由」通訊。
8. 按一下 [建立]。

   新建的認證網域會顯示在導覽框架中。

修改認證網域

1. 按一下要修改的認證網域旁邊的 [屬性] 箭頭。

   該認證網域的屬性會顯示在資料框架中。

2. 修改該認證網域的屬性。

3. 按一下 [儲存]。

刪除認證網域

刪除認證網域不會刪除屬於此網域的供應程式。如果供應程式屬於已刪除的認證網域，則它們仍爲此認證網域的一部分，直至明確將它們移除。無法在已刪除的認證網域中加入其他供應程式。

1. 從聯合管理模組的 [檢視] 功能表，選擇 [認證網域]。

   所有建立的認證網域會顯示在導覽框架中。

2. 核取要刪除的認證網域名稱旁邊之方塊。

3. 按一下 [刪除選取的項目]。

注意 執行刪除時不會顯示警告訊息。

供應程式

本節描述如何建立、修改和刪除遠端與託管供應程式。

建立遠端供應程式

遠端供應程式是接收主體 (與系統進行交互作用的組織或個人) 發出之複合資料的實體。若要建立遠端供應程式，請：

1. 從聯合管理模組的 [檢視] 功能表，選擇 [遠端供應程式]。

   依預設，建立的供應程式爲服務供應程式。您可以透過選取步驟 15 中描述的選項，選擇性地決定建立遠端供應程式作爲身份供應程式。

2. 按一下 [新建]。螢幕上會顯示 [建立遠端供應程式] 視窗。

3. 輸入供應程式 ID 的值。

   供應程式 ID 應該指定供應程式的 URL 識別碼。在所有遠端供應程式與託管供應程式中，它必須是唯一的。

4. 輸入對遠端供應程式的描述。

5. 輸入安全鍵。

   安全鍵定義安全證書的別名。證書依據別名儲存在 JKS 鍵值儲存區中。此別名 (安全鍵) 用於擷取所需的證書。

6. 輸入 SOAP 端點 URL。

   此欄位指定 SOAP 請求的接收者位置。用於透過 SOAP 在反向通道上通訊 (非瀏覽器通訊)。

7. 輸入單一登出服務 URL。

   服務供應程式或身份供應程式使用單一登出服務 URL 傳送與接收登出請求。

8. 輸入單一登出傳回 URL。

   此欄位指定登出請求經過處理後重新導向至的 URL。

9. 輸入聯合終止服務 URL。

   此欄位指定將聯合終止請求傳送至的 URL。

10. 輸入聯合終止傳回 URL 的值。

    此欄位指定聯合終止請求經過處理後重新導向至的 URL。

11. 定義單一登入服務 URL。

    此欄位定義在聯合與 SSO 期間，服務供應程式將請求傳送至的身份供應程式 URL。僅在啓用了 [作爲身份供應程式] 選項時才需要定義此欄位。

12. 輸入名稱註冊服務 URL。

    此欄位使用的名稱註冊協定是服務供應程式與身份供應程式進行通訊時註冊其名稱識別碼所使用的協定。註冊僅在聯合階段作業建立後才會進行。此欄位定義服務供應程式用來向身份供應程式註冊名稱識別碼的服務 URL。

13. 輸入名稱註冊傳回 URL。

    此欄位使用的名稱註冊協定是服務供應程式與身份供應程式進行通訊時註冊其名稱識別碼所使用的協定。註冊僅在聯合階段作業建立後才會進行。名稱註冊傳回 URL 是身份供應程式向其傳回註冊狀態的 URL。

14. 輸入假設使用者 URL。

    此欄位定義身份供應程式將向其傳送 SAML 假設的服務供應程式端點。

15. 決定是否將遠端供應程式定義爲身份供應程式。依預設，所有供應程式均爲服務供應程式。如果選取了 [作爲身份供應程式] 選項，它將另外定義遠端供應程式作爲身份供應程式。

16. 按一下 [建立]。

    新建的供應程式會顯示在導覽框架中。

修改遠端供應程式

遠端主機建立後，您可以隨時修改它。若要如此，請：

1. 從導覽框架的 [檢視] 功能表中選取 [遠端供應程式]。

2. 選擇您要修改的供應程式設定檔，然後按一下 [編輯] 箭頭。

   依預設，在導覽框架中顯示 [一般] 檢視。顯示在 [一般] 檢視中的大多數欄位均包含建立遠端供應程式時所輸入的資料。可以修改以下附加欄位：

   供應程式簡明 ID。此欄位唯一地識別身份供應程式的服務供應程式。

   簡明 ID 應該是 SHAI 編碼字串。供應程式 ID 字串應該作爲要編碼的值，因爲這可以確保該字串的唯一性。若要產生 SHAI 編碼，請使用 OpenSSL 指令行工具語法：

   ```
   $ echo providerID | openssl sha1
   ```

   如果修改任一欄位，請按一下 [儲存] 以儲存變更。

   狀態。「作用中」狀態使遠端供應程式能夠參加聯合與 SSO。「非作用中」狀態會使遠端供應程式不可使用，並且不會回應任何請求。

3. 若要修改 [服務供應程式] 欄位，請從 [檢視] 功能表選擇 [服務供應程式]。

   [假設使用者 URL] 欄位包含建立遠端供應程式時所輸入的資料。但是，還有其他欄位可以修改：

   聯合後的名稱註冊。如果啓用了此選項，則服務供應程式可以在聯合後參加名稱註冊。名稱註冊是一種設定檔，服務供應程式透過它指定主體的名稱識別碼，身份供應程式將使用該名稱識別碼與服務供應程式進行通訊。

   是否為帶簽名的認證請求。如果啓用，此選項將指定遠端供應程式傳送帶簽名的認證與聯合請求。身份供應程式將不會處理服務供應程式發出的無簽名請求。

   假設使用者 URL。此欄位定義身份供應程式將向其傳送 SAML 假設的供應程式端點。

   聯合終止設定檔。您可以選擇 SOAP 或 HTTP/重新導向。此欄位指定是使用 SOAP 還是 HTTP/重新導向設定檔來通知聯合終止。在供應程式作用期間可以隨時變更該欄位。

   單一登出設定檔。您可以選擇 SOAP 或 HTTP/重新導向。此欄位指定是使用 SOAP 還是 HTTP/重新導向來通知登出事件。在供應程式作用期間可以隨時變更該欄位。

   名稱註冊設定檔。您可以選擇 SOAP 或 HTTP/重新導向。此欄位指定是將 SOAP 還是將 HTTP/重新導向設定檔用於名稱註冊。在供應程式作用期間可以隨時變更該欄位。

4. 按一下 [儲存]。

5. 如果遠端供應程式在建立時定義爲身份供應程式，則可以透過選取 [檢視] 功能表中的 [身份供應程式] 修改以下欄位：

   [作為身份供應程式]。此欄位指定是否將遠端供應程式定義爲身份供應程式。依預設，所有供應程式均爲服務供應程式。如果選取了 [作爲身份供應程式] 選項，它將另外定義遠端供應程式作爲身份供應程式。

   SSO 期間的名稱註冊。如果啓用了此選項，它可讓身份供應程式在 SSO 期間參加名稱註冊。名稱註冊是一種設定檔，服務供應程式透過它指定主體的名稱識別碼，身份供應程式將使用該名稱識別碼與服務供應程式進行通訊。

   單一登入服務 URL。此欄位定義在聯合與 SSO 期間，服務供應程式將請求傳送至的身份供應程式 URL。僅在啓用了 [作爲身份供應程式] 選項時才需要定義此欄位。

6. 選取 [檢視] 功能表中的 [認證網域]，可以編輯遠端供應程式所屬的認證網域。

   使用方向鍵將選取的認證網域移到 [可用] 清單中。按一下 [儲存]。這樣會將此供應程式指定給認證網域。供應程式可以屬於一個或多個認證網域，但是，沒有指定任何認證網域的供應程式無法參加「自由」通訊。按一下 [儲存]。

建立託管供應程式

託管供應程式是建立、維護和管理主體身份資訊、在認證網域內爲其他服務供應程式提供主體認證的實體。若要建立託管供應程式，請：

1. 從聯合管理模組的 [檢視] 功能表，選擇 [託管供應程式]。

   依預設，建立的供應程式爲服務供應程式。您可以透過選取步驟 6 中描述的選項，選擇性地決定建立遠端供應程式作爲身份供應程式。

2. 按一下 [新建]。螢幕上會顯示 [建立託管供應程式] 視窗。

3. 輸入此供應程式 ID 的值。

   供應程式 ID 指定供應程式的 URL 識別碼。在所有遠端供應程式與託管供應程式中，它必須是唯一的。

4. 輸入對託管供應程式的描述。

5. 輸入供應程式的別名。

   對於每個託管供應程式，此欄位提供的別名會加入至名爲 metaAlias 的字串。然後，此字串將加入至爲託管供應程式自動植入的 URL。這些 URL 稱爲複合資料 URL。在以下範例中，`sunAlias` 是此供應程式的別名：

   聯合終止服務 URL

   ```
   http://www.example.com:58080/amserver/ProcessTermination/metaAlias/sunAlias
   ```

   SOAP 端點 URL

   ```
   http://www.example.com:58080/amserver/SOAPReceiver/metaAlias/sunAlias
   ```

6. 決定是否要將遠端供應程式定義爲身份供應程式。依預設，所有供應程式均爲服務供應程式。如果選取了 [作爲身份供應程式] 選項，它將另外定義遠端供應程式作爲身份供應程式。

7. 輸入安全鍵。

   安全鍵定義安全證書的別名。證書依據別名儲存在 JKS 鍵值儲存區中。此別名 (安全鍵) 用於擷取所需的證書。

8. 輸入供應程式 URL。

   此欄位指定將傳送複合資料的 URL。

9. 決定是否將託管供應程式定義爲身份供應程式。依預設，所有供應程式均爲服務供應程式。如果選取了 [作爲身份供應程式] 選項，則託管供應程式將被另外定義爲身份供應程式。

10. 按一下 [建立]。

    新建的供應程式會顯示在導覽框架中。

修改託管供應程式

1. 選擇您要修改的供應程式設定檔，然後按一下 [編輯] 箭頭。

   依預設，在導覽框架中顯示 [一般] 檢視。顯示在 [一般] 檢視中的大多數欄位均包含建立託管供應程式時輸入的資料。可以修改以下附加欄位：

   SOAP 端點 URL。此欄位指定 SOAP 請求的接收者位置。用於透過 SOAP 在反向通道上通訊 (非瀏覽器通訊)。

   單一登出服務 URL。服務供應程式或身份供應程式使用單一登出服務 URL 傳送與接收登出請求。

   單一登出傳回 URL。此欄位指定登出請求經過處理後重新導向至的 URL。

   聯合終止服務 URL。此欄位指定將聯合終止請求傳送至的 URL。

   聯合終止傳回 URL。此欄位指定聯合終止請求經過處理後重新導向至的 URL。

   名稱註冊服務 URL。此欄位使用的名稱註冊協定是服務供應程式與身份供應程式進行通訊時註冊其名稱識別碼所使用的協定。註冊僅在聯合階段作業建立後才會進行。此欄位定義服務供應程式用來向身份供應程式註冊名稱識別碼的服務 URL。

   名稱註冊傳回 URL。此欄位使用的名稱註冊協定是服務供應程式與身份供應程式進行通訊時註冊其名稱識別碼所使用的協定。註冊僅在聯合階段作業建立後才會進行。名稱註冊傳回 URL 是身份供應程式向其傳回註冊狀態的 URL。

   如果修改任何欄位，請按一下 [儲存]。

2. 若要修改 [服務供應程式] 欄位，請從 [檢視] 功能表選擇 [服務供應程式]。

   [假設使用者 URL] 欄位包含建立遠端供應程式時輸入的資料。您可以修改以下附加欄位：

   聯合後的名稱註冊。如果啓用了此選項，則服務供應程式可以在聯合後參加名稱註冊。名稱註冊是一種設定檔，服務供應程式透過它指定主體的名稱識別碼，身份供應程式與服務供應程式通訊時將使用該名稱識別碼。

   是否為帶簽名的認證請求。如果啓用，此選項會指定託管供應程式傳送帶簽名的認證與聯合請求。身份供應程式將不會處理服務供應程式發出的無簽名請求。

   聯合終止設定檔。您可以選擇 SOAP 或 HTTP/ 重新導向。此欄位指定是使用 SOAP 還是 HTTP/ 重新導向設定檔來通知聯合終止。在供應程式作用期間可以隨時變更該欄位。

   單一登出設定檔。您可以選擇 SOAP 或 HTTP/ 重新導向。此欄位指定是使用 SOAP 還是 HTTP/ 重新導向來通知登出事件。在供應程式作用期間可以隨時變更該欄位。

   名稱註冊設定檔。您可以選擇 SOAP 或 HTTP/ 重新導向。此欄位指定是將 SOAP 還是將 HTTP/ 重新導向設定檔用於名稱註冊。在供應程式作用期間可以隨時變更該欄位。

   認證環境。此欄位允許您指定要使用的認證環境之認證層級。

   如果修改了任何欄位，請按一下 [儲存]。

3. 如果託管供應程式在建立時定義爲身份供應程式，則可以透過選取 [檢視] 功能表中的 [身份供應程式] 修改這些欄位。這些欄位中包含的大多數資料是在託管供應程式建立時輸入的。您可以修改以下欄位：

   作為身份供應程式。此欄位指定是否將遠端供應程式定義爲身份供應程式。依預設，所有供應程式均爲服務供應程式。如果選取了 [作爲身份供應程式] 選項，它將另外定義遠端供應程式作爲身份供應程式。

   SSO 期間的名稱註冊。如果啓用了此選項，它可讓身份供應程式在 SSO 期間參加名稱註冊。名稱註冊是一種設定檔，服務供應程式透過它指定主體的名稱識別碼，身份供應程式與服務供應程式通訊時將使用該名稱識別碼。

   單一登入服務 URL。此欄位定義在聯合與 SSO 期間，服務供應程式將請求傳送至的身份供應程式 URL。僅在啓用了 [作爲身份供應程式] 選項時才需要定義此欄位。

   支援。指定身份供應程式是否支援認證環境。身份供應程式至少應支援一種認證環境。

環境參考。定義認證環境的名稱。在「自由」協定中定義了 10 種環境。

鍵值。傳送至 /UI/Login (Identity Server 認證 servlet) 的查詢字串中將包含一個鍵值 - 值對，用於識別要使用的認證機制。可能的鍵值包括：

- 模組
- 層級
- 角色
- 服務
- 使用者

值。定義認證機制鍵值對的值。

優先級。指出自由定義的認證環境的次序，由身份供應程式決定。如果身份供應程式不支援服務供應程式在認證請求期間請求的認證環境，它可以使用具有相同或更高優先級的任何其他認證環境。

按一下 [儲存] 以儲存變更。

4. 選取 [檢視] 功能表中的 [認證網域]，可以編輯遠端供應程式所屬的認證網域。

   使用方向鍵將選取的認證網域移到 [可用] 清單中。按一下 [儲存]。這樣會將此供應程式指定給認證網域。供應程式可以屬於一個或多個認證網域，但是，沒有指定任何認證網域的供應程式無法參加「自由」通訊。

5. 從 [檢視] 功能表選擇 [可信任的供應程式]。

   遠端供應程式將僅接受自這一組供應程式發出的請求。其他供應程式發出的請求將會忽略。若要建立可信任供應程式的清單，請從 [可用] 欄位選取供應程式，然後使用 [加入] 按鈕將其加入至 [已選取] 欄位。(您可以使用 [移除] 按鈕移除供應程式。) 按一下 [儲存]。

6. 選擇 Identity Server 配置屬性。

   欄位如下所示：

   認證類型。遠端 / 本機 - 指定託管供應程式在收到認證請求時是應該聯絡身份供應程式 (遠端) 還是由託管供應程式本身 (本機) 進行認證。

單一登入/聯合設定檔。指定託管供應程式用來傳送認證請求的設定檔。Identity Server 提供以下協定：

- 瀏覽器 POST - 指定基於 http POST 的正向通道協定。
- 瀏覽器 Artifact - 基於反向通道 (非瀏覽器) SOAP 的協定。

預設認證環境。指定身份供應程式未將此認證環境接收爲服務供應程式請求的一部分時，要使用的認證環境。還指定在未知使用者嘗試存取受保護資源時，服務供應程式使用的認證環境。預設值包括：

- Previous-Session
- Time-Sync-Token
- Smartcard
- MobileUnregistered
- Smartcard-PKI
- MobileContract
- Password
- Password-ProtectedTransport
- MobileDigitalID
- Software-PKI

強制認證身份供應程式。指示在收到授權請求時，身份供應程式是否必須重新認證 (即使在階段作業作用期間)。

請求身份供應程式為被動。如果選取此欄位，將指定身份供應程式不得與主體進行互動，而必須與使用者進行互動。

組織 DN。如果各個託管供應程式選擇在不同組織之間管理使用者 (產生託管模式)，該欄位用於指定組織 DN 的儲存位置。

自由版本 URI。指定自由規格版本。

名稱識別碼實現。允許服務供應程式選擇是否參加名稱註冊。名稱註冊是一種設定檔，服務供應程式透過它指定主體的名稱識別碼，身份供應程式與服務供應程式通訊時將使用該名稱識別碼。

供應程式首頁 URL。指定供應程式的首頁。

單一登入失敗重新導向 URL。爲失敗的 SSO 指定重新導向 URL。

假設間隔時間。指定身份供應程式發送假設的有效間隔時間。身份供應程式將繼續認證主體，直至假設間隔時間到期。

清除間隔時間。指定清除儲存在身份供應程式中的假設之時間間隔。

Artifact 逾時。指定身份供應程式發送假設 Artifact 的逾時時間。

假設限制。指定可以儲存或身份供應程式可以發送的假設數。

7. 按一下 [儲存]。

刪除供應程式

1. 從聯合管理的 [檢視] 功能表，選擇 [供應程式]。

   導覽框架中會顯示已建立的所有供應程式。

2. 核取要刪除的供應程式方塊。

3. 按一下 [刪除選取的項目]。

注意 執行刪除時不會顯示警告訊息。

第 6 章

策略管理

本章描述 Sun™ ONE Identity Server 的策略服務管理功能。策略管理用於檢視、管理和配置所有 Identity Server 策略。

本章包含以下小節：

策略類型

使用 Identity Server 可以配置的策略有兩種：**一般**策略或**參考**策略。一般策略由**規則**、**主題**與**條件**組成。參考策略由組織的**規則**與**參考**組成。

一般策略

在 Identity Server 中，定義存取權限的策略是指**一般**策略。一般策略由**規則**、**主題**與**條件**組成。

規則由**資源**以及一組或多組**動作**與**值**組成。資源定義受保護的物件，動作是可以對資源執行的作業名稱，值定義權限。

注意 在沒有資源的情況下，定義動作是可接受的。

策略未指定給身份。而**主題**指定給了策略。主題是將策略指定與套用至的身份物件。

條件定義策略適用的情形。例如，策略中的時間條件爲上午 7 時至 10 時，表示策略只適用於上午 7 時至 10 時。

注意 術語參考、規則、資源、主題、條件、動作和值分別對應 `policy.dtd` 中的元素 *Referral*、*Rule*、*ResourceName*、*Subject*、*Condition*、*Attribute* 和 *Value*。「*Sun ONE Identity Server Customization and API Guide*」中對這些術語有進一步解釋。

參考策略

通常，管理員可能需要將一個組織的策略定義和決策委託給另一個組織。(或者，可以將資源的策略決策委託給其他策略產品。) **參考**策略控制對建立與評估策略的策略委託。它由一條或多條**規則**與一個或多個**參考**組成。規則定義其策略定義與評估正在被參考的資源。參考定義策略定義與評估正在被參考的組織。

注意 被參考組織可以僅為那些已參考了該組織的資源 (或子資源) 定義或評估策略。但是，此限制不適用於根組織。

Identity Server 隨附兩種類型的參考：同級組織與子組織。它們分別委託給同層級組織與子層級組織。請參閱第 87 頁的 「爲同級組織和子組織建立策略」，以取得更多資訊。

策略管理

您可以透過策略 API、`amadmin` 指令行工具或 Identity Server 主控台建立、刪除和修改策略。

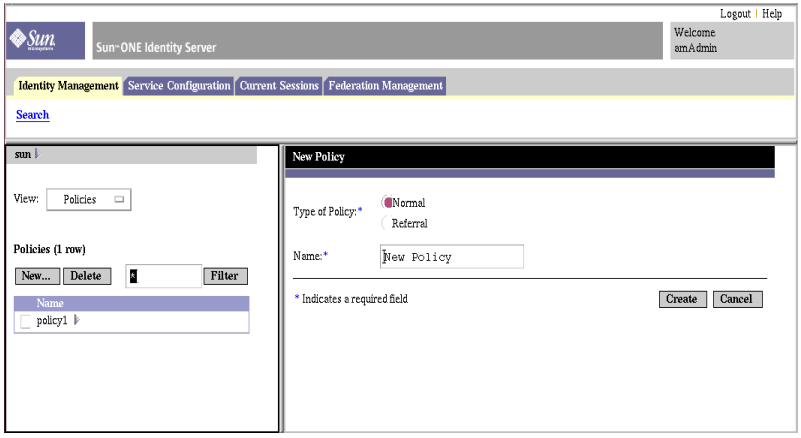
本章重點描述透過主控台建立策略。如需有關 `amadmin` 更多資訊，請參閱第 125 頁的 「amadmin 指令行工具」。如需有關策略 API 的更多資訊，請參閱 「*Sun ONE Identity Server Customization and API Guide*」中的 「Policy Service」一章。

策略是使用 [身份管理] 介面配置。該介面用於：

- 讓頂層管理員檢視、建立、刪除和修改可在所有組織中使用的特定服務的策略。
- 讓組織或子組織管理員檢視、建立、刪除和修改該組織特定用途的策略。

通常，在組織 (或子組織) 層級建立要在整個組織的樹中使用的策略。

圖 6-1 策略檢視



註冊策略配置服務

註冊策略配置服務與註冊任一類型的服務相同，可在 [身份管理] 介面內完成。依預設，策略配置服務會自動註冊到頂層組織。您建立的任一策略服務必須註冊到所有組織。無論您何時註冊策略配置服務，均必須在範本中輸入 LDAP 連結密碼，以便所有策略在組織中生效。

1. 導覽至 [身份管理] 介面。

   主控台開啓時，預設介面是 [身份管理]。

2. 選擇您要建立策略的組織。

   如果以頂層管理員的身份登入，請確定身份管理模組位於可顯示所有已配置組織的頂層組織。預設頂層組織在安裝期間定義。

3. 從 [檢視] 功能表選擇 [服務]。

   如果組織已註冊服務，則這些服務將會顯示在導覽框架中。

4. 在導覽框架中，按一下 [註冊]。

   尚未註冊到該組織之服務的清單會顯示在資料框架中。

5. 從 [註冊服務] 視窗 (在資料框架中開啓) 中選擇 [策略配置] 並按一下 [註冊]。

   策略配置服務即會被加入導覽框架的服務清單中。

6. 按一下 [屬性] 箭頭可配置策略服務。如果尚未配置策略範本，則需要爲新註冊的策略服務建立服務範本。

   若要配置策略服務，請按一下 [建立]。修改策略配置屬性。請參閱第 257 頁的「策略配置服務屬性」，以取得這些屬性的描述。按一下 [儲存]。

   現在，策略配置服務已註冊到所選組織。

注意 子組織必須獨立於其父系組織註冊其策略服務。換言之，子組織 `o=suborg,dc=sun,dc=com` 將不會從其父系組織 `dc=sun,dc=com` 繼承策略配置服務。

建立策略

策略是使用 [身份管理] 介面建立。

1. 導覽至 [身份管理] 介面。
2. 選擇您要爲其建立策略的組織。

   請確定 [策略管理] 視窗位置是您組織的正確位置。

3. 從 [檢視] 功能表選擇 [策略]。

   依預設，在 [檢視] 功能表中可以看見 [組織] 檢視。所有配置的子組織 (如果有的話) 均會顯示在此檢視下面。如果建立子組織策略，請選擇此子組織，然後從 [檢視] 功能表選擇 [策略]。

4. 在導覽框架中按一下 [新建]。將開啓 [新建策略] 視窗。
5. 選取您要建立的策略類型 (一般或參考)。

   如果參考子組織的參考策略不存在，則無法爲該子組織建立任何策略。如需更多資訊，請參閱第 87 頁的「爲同級組織和子組織建立策略」。

   並且此時，無需定義一般策略或參考策略的所有欄位。您可以建立策略，隨後再加入規則、主題、參考等。如需有關配置一般策略和參考策略的資訊，請參閱第 81 頁的「修改策略」。

6. 鍵入此策略名稱，然後按一下 [建立]。

   建立的策略名稱下將會開啓新的策略規則視窗。

7. 依預設，會顯示 [一般] 檢視。

   [一般] 檢視顯示策略的名稱，允許您輸入要建立的策略描述。

8. 按一下 [儲存]，以完成此策略的配置。

修改策略

建立一般策略或參考策略後，您即可修改規則、主題、條件與參考。

1. 從 [身份管理] 介面的 [檢視] 功能表，選取 [策略]。

   將顯示爲該組織建立的策略。

2. 選擇您要修改的策略，然後按一下 [屬性] 箭頭。[編輯策略] 視窗會在資料框架中開啓。

   依預設，會顯示 [一般] 檢視。

修改一般策略

可透過 [身份管理] 介面建立定義存取權限的策略。這種策略即爲一般策略。一般策略可由多個規則、物件和條件組成。本節列出並定義建立一般策略時可指定的預設欄位。

加入規則

規則定義此策略的資源、動作與動作值。

1. 從 [身份管理] 介面的 [檢視]，選取 [策略]。

   將顯示爲該組織建立的策略。

2. 選擇您要修改的策略，然後按一下 [特性] 箭頭。[編輯策略] 視窗會在資料框架中開啓。

   依預設，會顯示 [一般] 檢視。

3. 若要定義此策略的規則，請從 [檢視] 功能表選取 [規則]，然後按一下 [加入]。

   如果存在多種服務，會在資料框架中列出。選擇要爲其建立策略的服務，然後按一下 [下一步]。會顯示 [加入規則] 視窗。

4. 定義 [規則] 欄位中的資源、動作與動作值。

   這些欄位包括：

   [服務]。顯示要建立策略的服務。預設爲 URL 策略代理程式。

   [規則名稱]。輸入此規則的名稱。

   [資源名稱]。輸入資源的名稱。例如：

   ```
   http://www.sunone.com
   ```

   目前，策略代理程式僅支援 `http://` 資源和 `https://` 資源，而不支援用 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
   ```

   對於 URL 策略代理服務，如果未輸入連接埠號，則 `http://` 的預設連接埠號爲 80，`https://` 的預設連接埠號爲 443。

   [選取動作]。對於 URL 策略代理程式服務，您可以選取以下一種預設動作或兩者皆選：

   - `GET`
   - `POST`

   [選取動作值]。對於 URL 策略代理程式服務，您可以選擇以下一種動作值：

   - `Allow` 允許您存取與規則中所定義資源相符的資源。
   - `Deny` 不允許您存取與規則中所定義資源相符的資源。

   策略中的拒絕規則總是要優先於允許規則。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。通常，策略定義程序應該僅使用允許規則，在所有策略均不適於完成此拒絕存取時才使用預設拒絕規則。

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，透過不同主題 (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」(將拒絕策略套用於被認證爲員工角色的使用者，並將允許策略套用於被認證爲管理員角色的使用者) 協助區分這兩種策略。另一種方法爲使用 `authentication level` 條件，在此條件中管理員角色在較高認證層級進行認證。請參閱第 84 頁的「加入條件」，以取得更多資訊。

注意 **如果定義了服務，使動作不需要資源定義，則不會顯示資源欄位。如果此服務包含兩種類型的動作 (某些需要資源，某些不需要資源)，則會顯示一個選項，可以選取包含無需資源的動作規則或需要資源的動作規則。**

5. 按一下 [建立]，以儲存此規則。
6. 重複步驟 1 - 5，以建立其他規則。
7. 爲此策略建立的所有規則均顯示在 [規則] 檢視的表格中。按一下 [儲存]，以將這些規則加入至策略。

   若要從策略中移除某個規則，請選取此規則，然後按一下 [移除]。

   可以透過按一下規則名稱旁邊的 [編輯] 連結，編輯任何規則定義。

加入主題

主題定義此策略將套用至的主題。

1. 若要定義此策略的主題，請從 [檢視] 功能表選取 [主題]，然後按一下 [加入]。
2. 選取其中一個預設主題類型：
   - Identity Server 角色
   - LDAP 群組
   - LDAP 角色
   - LDAP 使用者
   - 組織

   按一下 [下一步] 以繼續。

3. 輸入此主題的名稱。
4. 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此主題成員的身份。如果選取此欄位，則此策略將套用於不屬於此主題成員的身份。

   如果策略中存在多重主題，並且至少一個主題表示策略套用於給定身份，則策略將套用於此身份。無論是否選取 [專用] 欄位，當滿足了策略中定義的所有條件時，策略均套用於此身份。
5. 執行搜尋，以便顯示要加入至此主題的身份。

   預設 (*) 搜尋式樣將顯示所有合格的項目。
6. 選取要爲此主題加入的身份，然後按一下 [加入]，以將其移至 [已選取的] 清單方塊。(或選取 [全部加入]，以加入所有身份)。
7. 按一下 [建立]。
8. 此主題的名稱、類型與專用狀態均會顯示在 [主題] 檢視的表格中。按一下 [儲存]。

   若要從策略中移除某主題，請選取此主題，按一下 [移除]，然後按一下 [儲存]。

   可以透過按一下主題名稱旁邊的 [編輯] 連結，編輯任何主題定義。

加入條件

條件允許您定義對策略的限制。例如，如果您在爲薪津應用程式定義策略，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領域的不同 URL 中配置不同的策略。例如，`http://org.example.com/hr/*jsp` 僅可以在上午 9 時至下午 5 時之間由 `org.example.net` 存取，而 `http://org.example.com/finance/*.jsp` 可以在上午 5 時至晚上 11 時之間由 `org.example2.net` 存取。配合使用 IP 條件與時間條件就可以達到這一目的。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)。

若要將條件加入一般策略：

1. 定義策略的條件。從 [檢視] 功能表選取 [條件]。按一下 [加入] 以加入新的條件，或者按一下 [編輯] 連結以編輯現有條件。
2. 選取以下其中一個預設條件：
   - 認證層級
   - 認證方案
   - IP 位址
   - 階段作業
   - 時間

   按一下 [下一步]。
3. 定義 [規則] 欄位中給定條件的值。這些欄位包括：

   [名稱]。輸入此條件的名稱。

   認證層級

   [認證層級]。指示認證的可信度。可用認證層級顯示在認證層級和認證模組表格中。

   認證方案

   [認證方案]。從下拉式功能表，選擇此條件的認證方案。這些認證方案均取自組織認證模組中的核心服務範本。

   IP **位址**

   [IP 位址自/至]。指定 IP 位址的範圍。

   [DNS 名稱]。指定 DNS 名稱。

   時間

   [日期自/至]。指定日期範圍。

   [時間]。指定一天內的時間範圍。

   [天]。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)。

   階段作業

   [最大階段作業時間]。指定套用策略時使用者階段作業的最大時間。

   [終止階段作業]。如果選取此欄位，則階段作業時間超過 [最大階段作業時間] 欄位定義所允許的最大時間時，此欄位會設定終止使用者階段作業。

4. 定義了此條件後，即按一下 [建立]。
5. 爲此策略建立的所有條件均顯示在 [條件] 檢視的表格中。按一下 [儲存]。

   若要從策略中移除某個條件，請選取此條件，然後按一下 [移除]。

   可以透過按一下條件名稱旁邊的 [編輯] 連結，編輯任何條件定義。

修改參考策略

透過 [身份管理] 介面，您可以將一個組織的策略定義與決策委託給另一個組織。(還可將資源的策略決策委託給其他策略產品。) **參考**策略控制對建立與評估策略的策略委託。它由**規則**和**參考**本身組成。如果策略服務包含不需要資源的動作，則無法爲子組織建立參考策略。

加入規則

規則可定義策略的資源。

1. 若要定義此策略的規則，請從 [檢視] 功能表選取 [規則]。按一下 [加入] 以加入新規則，或按一下 [編輯] 連結以編輯現有規則。
2. 定義 [規則] 欄位中的資源。這些欄位包括：

   [服務]。顯示要建立策略的策略服務。

   [名稱]。輸入此規則的名稱。

   [資源名稱]。輸入資源的名稱。例如：

   `http://www.sunone.com`

   目前，策略代理程式僅支援 `http://` 和 `https://` 資源，而不支援用 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。

   對於 URL 策略代理服務，如果未輸入連接埠號，則 `http://` 的預設連接埠號爲 80，`https://` 的預設連接埠號爲 443。
3. 按一下 [建立]，以儲存此規則。
4. 重複步驟 1 - 3，以建立其他規則。
5. 爲此策略建立的所有規則均顯示在 [規則] 檢視的表格中。按一下 [儲存]。

   若要從策略中移除某個規則，請選取此規則，然後按一下 [移除]。

   可以透過按一下規則名稱旁邊的 [編輯] 連結，編輯任何規則定義。

加入參考

參考定義策略評估正在參考的組織。依預設，有兩種類型的參考：同級組織與子組織。它們分別委託給同層級組織與子層級組織。

1. 若要定義此策略的參考，請從 [檢視] 功能表選取 [參考]。按一下 [加入] 以加入新的參考，或者按一下 [編輯] 連結以編輯現有參考。
2. 定義 [規則] 欄位中的資源。這些欄位包括：

   [參考]。顯示目前的參考。

   [名稱]。輸入此參考的名稱。

   [包含]。指定將要顯示在 [值] 欄位中的組織名稱之過濾器。依預設，該欄位將顯示所有組織名稱。

   [值]。輸入此參考的組織名稱。

3. 按一下 [建立] 和 [儲存]。

   若要從策略中移除某個參考，請選取此參考，然後按一下 [移除]。

   可以透過按一下參考名稱旁邊的 [編輯] 連結，編輯任何參考定義。

為同級組織和子組織建立策略

要爲同級組織或子組織建立策略，必須先在父系組織 (或另一個同級組織) 中建立參考策略。還應該在子組織中註冊策略配置服務並建立範本。參考策略必須在其規則定義中包含正由子組織管理的資源字首。在父系組織 (或另一個同級組織) 中建立參考策略後，便可在子組織 (或同級組織) 中建立一般策略。

如果動作名稱不包含資源名稱，Identity Server 策略框架就不允許建立參考策略。也就是說，如果動作不包含任何資源名稱，就只能在根組織下而不能在子組織下建立策略。

在此範例中，o=isp 爲父系組織，o=sun.com 爲子組織並管理 http://www.example.com 的資源和子資源。若要爲該子組織建立策略，請依循以下步驟：

1. 在 o=isp 建立參考策略。如需有關參考策略的資訊，請參閱程序第 86 頁的「修改參考策略」。

   參考策略必須將 http://www.sun.com 定義爲規則中的資源，且必須包含 SubOrgReferral (sun.com 作爲參考中的值)。

2. 移至 [組織] 檢視，並導覽至子組織 sun.com。

3. 確保策略配置服務已在子組織層級 sun.com 註冊。如需有關資訊，請參閱第 79 頁的「註冊策略配置服務」。

4. 資源既然被 isp 稱爲 sun.com，便可以爲資源 http://www.sun.com 或以 http://www.sun.com 起始的任何資源建立一般策略。

   請參閱程序第 81 頁的「修改一般策略」，以取得有關建立一般策略的資訊。

   若要爲由 sun.com 管理的其他資源定義策略，則必須在 o=isp 建立其他參考策略。

第 7 章

認證選項

Sun™ ONE Identity Server 提供框架以進行認證，認證是驗證在企業內存取應用程式之使用者身份的程序。使用者在存取 Identity Server 主控台或其他受 Identity Server 保護的資源之前，必須通過認證程序。認證可以透過驗證使用者身份的外掛程式來實施。(此外掛程式架構在「*Sun ONE Identity Server Customization and API Guide*」中有更全面的描述。)

Identity Server 主控台用於設定預設值、註冊認證服務、建立認證範本以及啓用服務。本章將概述認證服務，並說明如何註冊認證服務，包含以下小節：

核心認證

依預設，Identity Server 提供十種不同的認證服務，以及核心認證服務。核心認證服務爲認證服務提供總體配置。必須先註冊和啓用核心認證，才可以註冊和啓用匿名、基於證書、HTTP Basic、LDAP、成員身份、NT、RADIUS、SafeWord、SecurID 與 Unix 認證。第 19 章「核心認證屬性」包含核心屬性的詳細清單。

註冊和啟用核心服務

1. 導覽至要爲其註冊核心服務之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [核心認證] 核取方塊並按一下 [加入]。

   核心認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下核心認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
6. 按一下 [建立]。

   核心屬性會顯示在資料框架中。依照需要修改屬性。如需核心屬性的說明，請參閱第 19 章「核心認證屬性」，或按一下主控台右上角的 [說明] 連結。

匿名認證

依預設，啓用此模組時，使用者能以 *anonymous* 使用者的身份登入 Identity Server。透過配置 [有效匿名使用者清單] 屬性 (請參閱第 177 頁)，還可以定義該模組的匿名使用者清單。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。

註冊和啟用匿名認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊匿名認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與匿名認證服務同時註冊。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [匿名認證] 核取方塊並按一下 [加入]。

   匿名認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下匿名認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
6. 按一下 [建立]。

   匿名認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 17 章「匿名認證屬性」，或按一下主控台右上角的 [說明] 連結。
7. 按一下 [儲存]。

   匿名認證服務即已啓用。

使用匿名認證登入

爲了使用匿名認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的 「組織認證模組」) 以定義匿名認證。這會確保使用者登入時，在使用 `http(s)://hostname:port/DEPLOY_URI/Login?module=Anonymous&org=org_name` 中。若要不顯示 [匿名認證] 登入視窗而登入，請使用以下語法：

```
http(s)://hostname:port/DEPLOY_URI/Login?module=Anonymous&org=org_name&IDTolken1=user_id
```

依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

注意 匿名認證服務中的 [預設匿名使用者名稱] 屬性值為 anonymous。這是使用者用來登入的名稱。必須在組織內建立預設匿名使用者。使用者 ID 應該與匿名認證屬性中指定的使用者名稱相同。

基於證書的認證

基於證書的認證需要使用個人數位證書 (PDC) 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，並要根據證書廢止清單進行驗證。

在爲組織註冊基於證書的認證服務之前，需要完成許多工作。首先，需要確保與 Identity Server 一同安裝之 Web 容器的安全，需要對其進行配置，以用於基於證書的認證。啓用基於證書的服務之前，請參閱 「*Sun ONE Web Server 6.1* **管理員指南**」之第 6 章 「使用證書與鍵」，以瞭解這些初始的 Web Server 配置步驟。此文件位於以下位置：

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

或者，請參閱位於以下位置的 「*Sun ONE Application Sever Administrator's Guide to Security*」：

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

注意 將使用基於證書的服務來認證的每位使用者必須為其瀏覽器請求 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。

註冊和啟用基於證書的認證

您必須以組織管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊基於證書的認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與基於證書的認證服務同時註冊。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [基於證書的認證] 核取方塊並按一下 [加入]。

   基於證書的認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下基於證書的認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
6. 按一下 [建立]。

   基於證書的認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 18 章「證書認證屬性」，或按一下主控台右上角的 [說明] 連結。
7. 按一下 [儲存]。

為基於證書的認證加入 [平台伺服器清單]

爲了加入該清單，您必須以組織管理員的身份登入 Identity Server。

1. 選取服務配置模組。
2. 從可用服務清單選擇 [平台] 服務。
3. 將伺服器資訊加入 [伺服器清單] 屬性。如需有關其他伺服器屬性的更多資訊，請參閱第 33 章「平台服務屬性」。

使用基於證書的認證登入

爲了使基於證書的認證成爲預設的認證方法，必須修改 [核心認證] 服務屬性組織認證模組 (請參閱第 188 頁)。這會確保當使用者在使用 `https://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=Cert` 登入時，將會看到 [基於證書的認證] 登入視窗。依據所使用的認證類型 (如角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

HTTP Basic 認證

此模組使用基本認證 (HTTP 協定的內建認證支援)。網路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。Identity Server 會擷取該使用者名稱和密碼，將使用者認證至 LDAP 認證模組。爲使 HTTP Basic 正常工作，必須註冊 LDAP 認證模組 (僅註冊 HTTP Basic 模組將不起作用)。如需更多資訊，請參閱第 95 頁的「註冊和啓用 LDAP 認證」。一旦使用者認證成功，他 / 她即可重新認證，無需提供使用者名稱和密碼。

註冊和啟用 HTTP Basic 認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊 HTTP Basic 認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 HTTP Basic 認證服務同時註冊。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [HTTP Basic 認證] 核取方塊並按一下 [加入]。

   HTTP Basic 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下 HTTP Basic 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**

6. 按一下 [建立]。

   HTTP Basic 認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 20 章「HTTP Basic 認證屬性」，或按一下主控台右上角的 [說明] 連結。

7. 按一下 [儲存]。

   HTPP Basic 認證服務即已啓用。

使用 HTTP Basic 認證登入

爲了使用 LDAP 認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的「組織認證模組」) 以定義 HTTP Basic 認證。這會確保當使用者在使用 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=HTTPBasic` 來登入時，將可看到認證登入視窗。依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。如果認證失敗，則新的實例應該被開啓且使用者應該再次登入。

LDAP 目錄認證

如果使用 LDAP 認證服務，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。這是所有基於組織的認證之預設認證模組。如果使用者提供 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 Identity Server 階段作業，並使用該階段作業進行設定。安裝 Identity Server 後，依預設會啓用 LDAP 認證。服務停用時，系統會提供以下說明。

註冊和啟用 LDAP 認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊 LDAP 認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 LDAP 認證服務同時註冊。

3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。

4. 選取 [LDAP 認證] 核取方塊並按一下 [加入]。

   LDAP 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。

5. 按一下 LDAP 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**

6. 按一下 [建立]。

   LDAP 認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 21 章「LDAP 認證屬性」，或按一下主控台右上角的 [說明] 連結。

7. 在 [超級使用者連結密碼] 屬性中輸入密碼。依預設，在安裝期間輸入的 `amldapuser` 密碼將用作連結使用者。

   若要使用其他連結使用者，請變更 [超級使用者連結 DN] 屬性中的使用者 DN，並在 [超級使用者連結密碼] 屬性中輸入此使用者的密碼。

8. 按一下 [儲存]。

   LDAP 認證服務即已啓用。

使用 LDAP 認證登入

爲了使用 LDAP 認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的「組織認證模組」) 以定義 LDAP 認證。這會確保當使用者在使用 `http://`*`hostname:port/deploy_URI`*`/UI/Login?module=LDAP` 登入時，將會看到 [LDAP 認證] 登入視窗。依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

啟用 LDAP 認證錯誤修復

LDAP 認證屬性包括一個值欄位，用於輸入主 / 次 Directory Server 的值。如果主伺服器不可用，Identity Server 將轉向第二個伺服器進行認證。如需更多資訊，請參閱 LDAP 屬性 (第 200 頁的「主 LDAP 伺服器與連接埠」和第 200 頁的「次 LDAP 伺服器與連接埠」)。

多重 LDAP 配置

作爲一種錯誤修復，或當 Identity Server 主控台僅提供一個值欄位時要配置屬性的多個值，管理員可於一個組織之下定義多重 LDAP 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。如需有關多重 LDAP 配置的資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」中的「*Multi LDAP Configuration*」。

成員身份認證

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`)。啓用此服務時，使用者無需借助管理員，即可建立帳戶並將其作爲個人帳戶。對於這個新帳戶，使用者能以已註冊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。

註冊和啟用成員身份認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊成員身份認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與成員身份認證服務同時註冊。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [成員身份認證] 核取方塊並按一下 [加入]。

   成員身份認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下成員身份認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
6. 按一下 [建立]。

   成員身份認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 22 章「成員身份認證屬性」，或選取主控台右上角的 [說明] 連結。

7. 在 [超級使用者連結密碼] 屬性中輸入密碼。依預設，在安裝期間輸入的 `amldapuser` 密碼將用作連結使用者。

   若要使用其他連結使用者，請變更 [超級使用者連結 DN] 屬性中的使用者 DN，並在 [超級使用者連結密碼] 屬性中輸入此使用者的密碼。

8. 按一下 [儲存]。

   成員身份認證服務即已啓用。

使用成員身份認證登入

爲了使用成員身份認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的 「組織認證模組」) 以定義成員身份認證。這會確保當使用者在使用 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=Membership` 登入時，(注意區分大小寫) 將可看到 [成員身份認證登入 (自行註冊)] 視窗。依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

NT 認證

可以將 Identity Server 配置爲與已安裝的 NT/Windows 2000 伺服器配合工作，Identity Server 提供 NT 認證的用戶端部分。Solaris 平台僅支援 NT 認證服務。

1. 配置 NT 伺服器。

   如需詳細說明，請參閱 NT 伺服器的說明文件。

2. 註冊和啓用 NT 認證服務之前，您必須先獲得並在您的 Solaris 系統上安裝與 Identity Server 通訊的 Samba 用戶端。如需更多資訊，請參閱第 211 頁的 「NT 認證屬性」。

3. 註冊和啓用 NT 認證服務。

註冊和啟用 NT 認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊 NT 認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 NT 認證服務同時註冊。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [NT 認證] 核取方塊並按一下 [加入]。

   NT 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下 NT 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
6. 按一下 [建立]。

   NT 認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 23 章「NT 認證屬性」，或選取主控台右上角的 [說明] 連結。
7. 按一下 [儲存]。

   NT 認證服務即已啓用。

使用 NT 認證登入

爲了使用 NT 認證登入，必須修改 [核心認證] 服務屬性 (第 188 頁的「組織認證模組」) 以定義 NT 認證。這會確保當使用者在使用 `http://`*`hostname:port/deploy_URI`*`/UI/Login?module=NT` 登入時，將會看到 [NT 認證] 登入視窗。依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

RADIUS 伺服器認證

可以將 Identity Server 配置爲與已安裝的 RADIUS 伺服器配合工作。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 認證服務需要兩個步驟。

1. 配置 RADIUS 伺服器。

   如需詳細說明，請參閱 RADIUS 伺服器的說明文件。

2. 註冊和啓用 RADIUS 認證服務。

註冊和啟用 RADIUS 認證

您必須以組織管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊 RADIUS 認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 RADIUS 認證服務同時註冊。

3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。

4. 選取 [RADIUS 認證] 核取方塊並按一下 [加入]。

   RADIUS 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。

5. 按一下 RADIUS 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**

6. 按一下 [建立]。

   RADIUS 認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 24 章「RADIUS 認證屬性」，或選取主控台右上角的 [說明] 連結。

7. 按一下 [儲存]。

   RADIUS 認證服務即已啓用。

使用 RADIUS 認證登入

爲了使用 RADIUS 認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的「組織認證模組」) 以定義 RADIUS 認證。這會確保當使用者在使用 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=RADIUS` 登入時，將會看到 [RADIUS 認證] 登入視窗。依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

使用 Sun ONE Application Server 配置 RADUIS

如果 RADUIS 用戶端形成與其伺服器的套接字連線，則依預設 Application Server 的 `server.policy` 檔案中僅允許 SocketPermissions 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
- 連線
- 偵聽
- 解析

若要爲套接字連線授與權限，您必須將項目加入 Application Server 的 `server.policy` 檔案。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 名稱主機規格中可以使用一次萬用字元「`*`」。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。

`listen` 動作僅在與本端主機配合使用時才有意義。如果存在任何其他動作，則暗含 `resolve` 動作 (解析主機 /IP 名稱服務查找)。

例如，建立 SocketPermissions 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";
```

注意 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 認證

可以配置 Identity Server，使其處理 Secure Computing 的 SafeWord™ 或 SafeWord PremierAccess™ 認證伺服器的 SafeWord 認證請求。Identity Server 提供 SafeWord 認證的用戶端部分。SafeWord 伺服器可以存在於安裝有 Identity Server 的系統或是單獨的系統上。

註冊和啟用 SafeWord 認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊 SafeWord 認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 SafeWord 認證服務同時註冊。

3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。

4. 選取 [SafeWord 認證] 核取方塊並按一下 [加入]。

   SafeWord 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。

5. 按一下 SafeWord 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**

6. 按一下 [建立]。

   SafeWord 認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 24 章「SafeWord 認證屬性」，或按一下主控台右上角的 [說明] 連結。

7. 按一下 [儲存]。

   SafeWord 認證服務即已啓用。

使用 SafeWord 認證登入

爲了使用 SafeWord 認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的「組織認證模組」) 以定義 SafeWord 認證。這會確保當使用者在使用 `http://`*`hostname:port/deploy_URI`*`/UI/Login?module=SAFEWORD` 登入時，將會看到 [SafeWord 認證] 登入視窗。依據所使用的認證類型 (如角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

使用 Sun ONE Application Server 配置 SafeWord

如果 SafeWord 用戶端形成與其伺服器的套接字連線，則依預設 Application Server 的 `server.policy` 檔案中僅允許 SocketPermissions 的 `connect` 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
- 連線
- 偵聽
- 解析

若要爲套接字連線授與權限，您必須將項目加入 Application Server 的 server.policy 檔案。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 名稱主機規格中可以使用一次萬用字元「*」。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。

listen 動作僅在與本端主機配合使用時才有意義。如果存在任何其他動作，則暗含 resolve 動作 (解析主機 /IP 名稱服務查找)。

例如，建立 SocketPermissions 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";
```

注意 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。

SecurID 認證

可以配置 Identity Server，讓其處理 RSA 的 ACE/Server 認證伺服器的 SecureID 認證請求。Identity Server 提供 SecurID 認證的用戶端部分。ACE/Server 可以存在於安裝有 Identity Server 的系統上或是單獨的系統上。若要對在本機管理的使用者 ID 進行認證 (請參閱 `admintool` (1M))，則需要超級使用者存取權限。

SecurID 認證使用認證**輔助程式** `amsecuridd`，它是主 Identity Server 程序以外的單獨程序。此輔助程式會在啓動時偵聽連接埠，以取得配置資訊。如果安裝了 Identity Server 並以 `nobody` 的身份或超級使用者以外的使用者 ID 執行，則必須仍以超級使用者身份執行 *`IdentityServer_base`*`/SUNWam/share/bin/amsecuridd` 程序。如需有關 `amsecuridd` 輔助程式的更多資訊，請參閱第 149 頁的「amsecuridd 輔助程式」。

註冊和啟用 SecurID 認證

您必須以組織管理員或頂層管理員的身份登入 Identity Server。

1. 導覽至要爲其註冊 SecurID 認證之組織的導覽框架。
2. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 SecurID 認證服務同時註冊。
3. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
4. 選取 [SecurID 認證] 核取方塊並按一下 [加入]。

   SecurID 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
5. 按一下 SecurID 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
6. 按一下 [建立]。

   SecurID 認證屬性會顯示在資料框架中。依照需要修改屬性。如需這些屬性的說明，請參閱第 25 章「SecurID 認證屬性」，或按一下主控台右上角的 [說明] 連結。
7. 按一下 [儲存]。

   SecurID 認證服務即已啓用。

使用 SecurID 認證登入

爲了使用 SecurID 認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的 「組織認證模組」) 以定義 SecurID 認證。這會確保當使用者在使用 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=SecurID` 登入時，將會看到 [SecurID 認證] 登入視窗。依據所使用的認證類型 (如角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

Unix 認證

可以將 Identity Server 配置爲根據安裝有 Identity Server 的 Solaris 系統上已知的 Unix 使用者 ID 和密碼處理認證請求。雖然只有一個組織屬性和幾個全域屬性用於 Unix 認證，但有一些針對系統的考量。若要對在本機管理的使用者 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`，它是主 Identity Server 程序以外的單獨程序。此輔助程式會在啓動時偵聽連接埠，以取得配置資訊。每個 Identity Server 只有一個 Unix 輔助程式，可以爲其所有組織提供服務。

如果安裝了 Identity Server 並以 `nobody` 的身份或超級使用者以外的使用者 ID 執行，則必須仍以超級使用者身份執行 *IdentityServer_base*`/SUNWam/share/bin/amunixd` 程序。Unix 認證模組透過開啓 `localhost:58946` 的套接字來呼叫 `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`，請輸入以下指令：

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

IP 位址和連接埠號位於 `AMConfig.properties` 的 `UnixHelper.ipadrs` 屬性 (IPV4 格式) 和 `UnixHelper.port` 屬性中。您可以透過 `amserver` 指令行公用程式 (`amserver` 自動執行程序，並從 `AMConfig.properties` 擷取連接埠號和 IP 位址) 執行 `amunixd`。

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

Unix 認證服務不可用於 Windows 平台。

註冊和啟用 Unix 認證

您必須以頂層管理員的身份登入 Identity Server，以執行以下步驟。

1. 選取服務配置模組。
2. 按一下 [服務名稱] 清單中的 Unix 認證 [屬性] 箭頭。

   螢幕上將顯示數個全域屬性和一個組織屬性。由於一個 Unix 輔助程式爲 Identity Server 伺服器的所有組織提供服務，因此大多數 Unix 屬性是全域屬性。如需這些屬性的說明，請參閱第 26 章「Unix 認證屬性」，或按一下主控台右上角的 [說明] 連結。
3. 按一下 [儲存] 以儲存新的屬性值。

   您能以組織管理員的身份登入 Identity Server，爲組織啓用 Unix 認證。
4. 導覽至要爲其註冊 Unix 認證之組織的導覽框架。
5. 從 [檢視] 功能表選擇 [服務]。

   如果核心服務已註冊，則會顯示在導覽框架中。如果尚未註冊，則可與 Unix 認證服務同時註冊。
6. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。
7. 選取 [Unix 認證] 核取方塊並按一下 [加入]。

   Unix 認證服務將顯示在導覽框架中，從而告知管理員該服務已註冊。
8. 按一下 Unix 認證 [屬性] 箭頭。

   資料框架中會顯示訊息：**目前沒有該服務的範本。您要現在建立一個嗎？**
9. 按一下 [建立]。

   Unix 認證組織屬性會顯示在資料框架中。依照需要修改 [認證層級] 屬性。如需該屬性的說明，請參閱第 26 章「Unix 認證屬性」，或按一下主控台右上角的 [說明] 連結。
10. 按一下 [儲存]。

    Unix 認證服務即已啓用。

使用 Unix 認證登入

爲了使用 Unix 認證來登入，必須修改 [核心認證] 服務屬性 (第 188 頁的「組織認證模組」) 以定義 Unix 認證。這會確保當使用者在使用 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=Unix` 登入時，將會看到 [Unix 認證] 登入視窗。依據所使用的認證類型 (如服務、角色、使用者和組織)，如果將認證模組配置爲預設，則無需在 URL 中指定模組名稱。

認證配置

認證配置服務用於爲以下任一認證類型定義認證模組：

- 組織
- 角色
- 服務
- 使用者

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。

配置認證模組之前，必須先修改 [核心認證] 服務屬性 [組織認證模組]，使之包括特定的認證模組名稱。

認證配置使用者介面

認證配置服務可讓您定義一個或多個認證服務 (或**模組**)，使用者必須先通過這些認證服務，然後才被允許存取主控台或 Identity Server 中任何受保護的資源。組織、角色、服務和基於使用者的認證都使用共用使用者介面來定義認證模組。(有關存取特定物件類型的 [認證配置] 介面的說明，將在後續章節中描述)。

1. 按一下物件的 [認證配置] 屬性旁邊的 [編輯] 連結，以顯示 [模組清單] 視窗。
2. 此視窗列出了已指定給該物件的認證模組。如果不存在任何模組，請按一下 [加入] 顯示 [加入模組] 視窗。

[加入模組] 視窗包含三個欄位要定義：

[模組名稱]。此下拉式清單允許您選取可用於 Identity Server 的認證模組 (包括可以加入的自訂模組)。依預設，這些模組包括：

- LDAP
- 證書
- 匿名
- SafeWord
- SecurID
- HTTPBasic
- 成員身份
- NT
- RADIUS
- Unix

[旗標]。此下拉式功能表允許您指定認證模組要求。可以爲下列選項之一：

- REQUIRED - 要求認證模組必須成功。無論成功或失敗，都將繼續認證清單中的下一個認證模組。
- REQUISITE - 要求認證模組必須成功。如果成功，會繼續認證清單中的下一個認證模組。如果失敗，會將控制權傳回應用程式 (不會繼續認證清單中的下一個認證模組)。
- SUFFICIENT - 不要求認證模組一定成功。如果成功，會將控制權立即傳回應用程式 (不會繼續認證清單中的下一個認證模組)。如果失敗，會繼續認證清單中的下一個認證模組。
- OPTIONAL - 不要求認證模組一定成功。無論成功或失敗，都將繼續認證清單中的下一個認證模組。

這些旗標爲定義了這些旗標的認證模組建立了執行標準。執行的階層結構中，REQUIRED 爲最高層級，OPTION 爲最低層級。

例如，如果管理員使用 REQUIRED 旗標定義 LDAP 模組，則使用者憑證必須通過 LDAP 認證要求，才能存取給定資源。

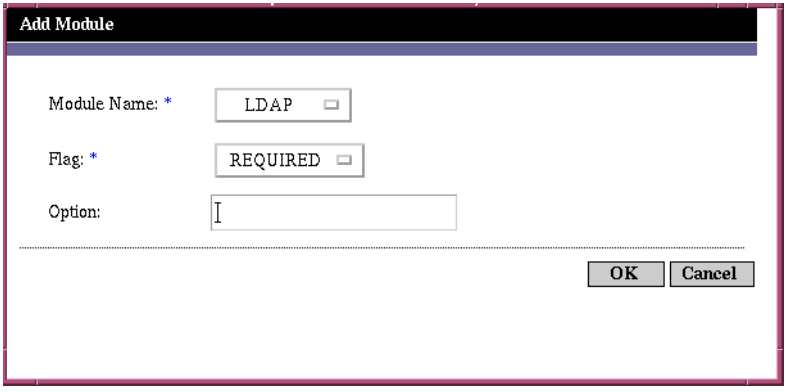
如果您加入多重認證模組，並且每個模組的旗標設定爲 REQUIRED，則使用者必須通過所有認證要求，才能取得存取權限。

如需關於旗標定義的更多資訊，請參考 JAAS (Java 認證與授權服務)，位於：

```
http://java.sun.com/security/jaas/doc/module.html
```

[選項]。允許此模組的其他選項爲鍵值 = 值對。多重選項由空格分隔。

圖 7-1 爲使用者加入 [模組清單] 視窗



3. 選取欄位後，按一下 [確定] 以返回 [模組清單] 視窗。您已定義的認證模組會在此視窗中列出。按一下 [儲存]。

   您可以向此清單中加入任意多個認證模組。加入多個認證模組被稱爲**鏈接**。如果您要鏈接認證模組，請注意模組的列出次序定義執行的階層結構之次序。

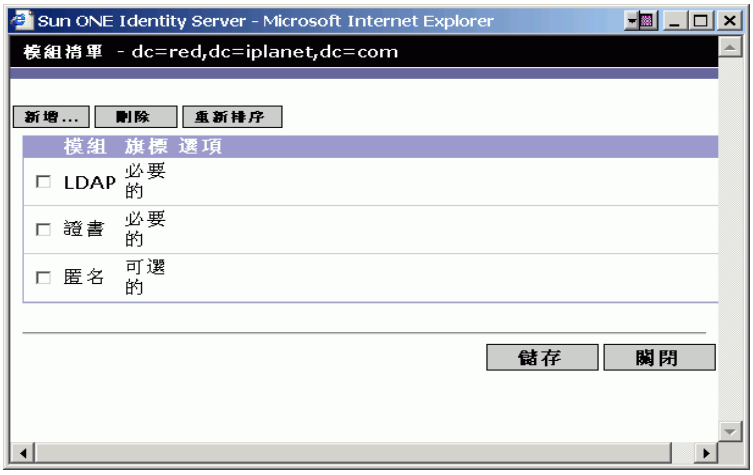
   若要變更認證模組的次序，請：

   a. 按一下 [重新排序] 按鈕。

   b. 選取您要重新排序的模組。

   c. 使用 [向上] 和 [向下] 按鈕將模組放置在所需位置。

圖 7-2 使用者的 [模組清單] 視窗



4. 若要從清單中移除任一認證模組，請選取該認證模組旁邊的核取方塊，然後按一下 [刪除]。

注意 如果您在鏈內的任何模組中輸入 amadmin 憑證，將收到 amadmin 設定檔。在此情況下，認證不會檢查別名對映，也不會檢查鏈內的模組。

組織的認證配置

要爲組織設定認證模組，先爲組織註冊核心認證服務。

若要配置組織的認證屬性：

1. 導覽至要配置認證屬性的組織。
2. 從 [檢視] 功能表選取 [服務]。
3. 按一下服務清單中的核心 [屬性] 箭頭。

   核心認證屬性會顯示在資料框架中。

4. 按一下 [管理員認證者] 屬性旁邊的 [編輯] 連結。此連結可讓您僅爲管理員定義認證服務。管理員是指需要 Identity Server 主控台存取權限的使用者。如果需要管理員的認證模組與一般使用者的認證模組有所不同，則可以使用此屬性。預設認證模組爲 LDAP。

   定義認證服務後，按一下 [儲存] 以儲存變更，然後按一下 [關閉] 以返回至組織的核心認證屬性。

5. 按一下 [組織認證配置] 屬性旁邊的 [編輯] 連結。此連結可讓您爲組織內的所有使用者定義認證模組。預設認證模組爲 LDAP。

6. 定義認證服務後，按一下 [儲存] 以儲存變更，然後按一下 [關閉] 以返回至組織的核心認證屬性。

角色的認證配置

在角色層級註冊認證配置服務後，爲角色設定認證模組。

1. 導覽至要配置認證屬性的組織。
2. 從 [檢視] 功能表選擇 [角色]。
3. 選取要設定認證配置的角色，然後按一下 [屬性] 箭頭。

   角色的屬性會顯示在資料框架中。

4. 從資料框架中的 [檢視] 功能表選取 [服務]。
5. 依照需要修改認證配置屬性。如需這些屬性的說明，請參閱第 27 章「認證配置服務屬性」，或按一下主控台右上角的 [說明] 連結。
6. 按一下 [儲存]。

注意 如果您要建立新的角色，系統不會自動為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。

啟用基於角色的認證後，可以保留 LDAP 認證模組作為預設方式，因為無需配置成員身份。

服務的認證配置

註冊認證配置服務後，爲服務設定認證模組。若要如此，請：

1. 從身份管理模組中的 [檢視] 功能表選擇 [服務]。

   螢幕上將顯示已註冊的服務清單。如果未註冊認證配置服務，請繼續執行以下步驟。如果已註冊該服務，請移至步驟 4。

2. 在導覽框架中按一下 [加入]。

   可用服務清單會顯示在資料框架中。

3. 選取 [認證配置] 核取方塊並按一下 [加入]。

   認證配置服務將顯示導覽框架中，從而告知管理員該服務已註冊。

4. 按一下認證配置 [屬性] 箭頭。

   [服務實例清單] 會顯示在資料框架中。

5. 按一下要配置認證模組的服務實例。

6. 修改認證配置屬性，然後按一下 [儲存]。如需這些屬性的說明，請參閱第 27 章「認證配置服務屬性」，或按一下主控台右上角的 [說明] 連結。

使用者的認證配置

1. 從身份管理模組中的 [檢視] 功能表選擇 [使用者]。

   使用者清單會顯示在導覽框架中。

2. 選取您要修改的使用者，然後按一下 [屬性] 箭頭。

   使用者設定檔會顯示在資料框架中。

注意 如果您要建立新的使用者，系統不會自動為此使用者指定認證配置服務。請確保在建立使用者之前，您已選取 [使用者設定檔] 頁面頂端的 [認證配置服務] 選項。如果未選取此選項，使用者將無法繼承為角色定義的認證配置。

3. 若要確保認證配置服務已指定給該使用者，請從 [檢視] 功能表中選取 [服務]。如果已指定，認證配置服務將作爲已指定的服務列出。

4. 從資料框架中的 [檢視] 功能表選取 [使用者]。
5. 按一下 [使用者認證配置] 屬性旁邊的 [編輯] 連結，爲使用者定義認證模組。
6. 按一下 [儲存]。

根據認證層級的認證

每個認證模組均可與其**認證層級**的整數值相關聯。透過按一下服務配置中認證模組的 [屬性] 箭頭，並變更模組之 [認證層級] 屬性的相應值，則可指定認證層級。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。

當使用者在模組中認證成功後，認證層級將標記在使用者的 SSO 記號上。如果使用者被要求在多個認證模組中認證，並且成功完成認證，則最高的認證層級值將標記在使用者的 SSO 記號上。

如果使用者嘗試存取某項服務，此服務可以透過檢查使用者 SSO 記號中的認證層級來決定是否允許此使用者存取。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
```

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，以供使用者選擇。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。

根據模組認證

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 [組織認證模組]，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 [認證模組被拒絕] 頁面。如需更多資訊，請參閱第 188 頁的「組織認證模組」。

URL 重新導向

在認證配置服務中，您可以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組織，使之可用於爲角色、組織或使用者而配置。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。如需有關爲身份物件註冊認證配置服務的資訊，請參閱第 108 頁的「認證配置」。

第 8 章

密碼重設服務

Sun™ ONE Identity Server 提供密碼重設服務，可讓使用者重設密碼，以便存取受 Identity Server 保護的給定服務或應用程式。由頂層管理員定義的密碼重設服務屬性控制使用者驗證憑證 (格式爲**保密問題**)、控制新的或現有密碼通知的機制以及爲不正確的使用者驗證設定可能的鎖定間隔時間。

本章包含以下小節：

註冊密碼重設服務

使用者所屬組織不需要註冊密碼重設服務。如果密碼重設服務不存在於使用者所屬組織中，它將繼承在服務配置模組中爲此服務定義的值。

若要爲不同組織中的使用者註冊密碼重設服務，請：

1. 在身份管理模組中，選擇 [組織] 並選取要爲其註冊服務的組織。
2. 在導覽框架中，按一下 [註冊]。

   可用服務清單會顯示在資料框架中。
3. 選取 [密碼重設] 核取方塊並按一下 [註冊]。

   密碼重設服務將顯示在導覽框架中，從而告知管理員該服務已註冊。

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。若要配置該服務，請：

1. 選取爲其註冊密碼重設服務的組織。
2. 按一下密碼重設 [屬性] 箭頭。

   資料框架會顯示訊息：「沒有適用於該服務的範本」。按一下 [建立]。
3. 密碼重設屬性會顯示在資料框架中，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 (預設爲啓用)。至少必須定義以下屬性：
   - 使用者驗證
   - 保密問題
   - 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)。

   其餘屬性均爲選擇性的。如需密碼重設屬性的描述，請參閱第 247 頁的 「密碼重設服務屬性」，或按一下主控台右上角的 [說明] 連結。

注意 Identity Server 會自動安裝密碼重設網路應用程式，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:

```
IdentityServer_base/SUNWam/samples/console/PasswordGenerator
```

NotifyPassword:

```
IdentityServer_base/SUNWam/samples/console/NotifyPassword
```

4. 如果使用者要定義其特有的個人問題，則選取 [啓用個人問題] 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保密問題前可以嘗試的次數。鎖定功能透過密碼重設服務屬性來配置。如需這些屬性的描述，請參閱第 247 頁的 「密碼重設服務屬性」。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

該鎖定爲一種暫時鎖定，並且僅當 [密碼重設失敗鎖定持續時間 (分鐘)] 屬性中的值大於零且啓用了 [密碼重設失敗鎖定模式] 屬性時才有效。該鎖定將防止使用者透過密碼重設網路應用程式重設密碼。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。

實體鎖定

該鎖定爲一種比較永久的鎖定。如果 [密碼重設失敗鎖定計數] 屬性中的值設定爲 0，且啓用了 [密碼重設失敗鎖定模式] 屬性，則當使用者對保密問題的回答不正確時，該使用者帳戶狀態會變更爲非作用中。

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 Identity Server 主控台，以便自訂其保密問題。例如：

1. 在使用者名稱和密碼成功通過認證後，使用者登入 Identity Server 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 [可用問題回答] 畫面。

3. 系統會爲使用者顯示管理員爲服務定義的問題，如：
   - 您的寵物叫什麼？
   - 您最喜愛哪個電視節目？
   - 您母親的婚前姓是什麼？
   - 您最喜愛哪家飯店？
4. 使用者可以選取保密問題，最多不超過管理員爲組織定義的最大問題數 (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。這些問題與回答爲重設使用者密碼的依據 (請參閱後面一小節)。如果管理員選取了 [啓用個人問題] 屬性，系統會提供文字欄位，讓使用者輸入特有的保密問題並對其做出回答。

圖 8-1 帶有 [啓用個人問題] 的 [可用問題回答] 畫面

5. 使用者按一下 [儲存]。

重設遺忘密碼

如果使用者遺忘密碼，Identity Server 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：

1. 使用者從管理員爲他們提供的 URL 登入到密碼重設網路應用程式。例如：

   `http://`*`hostname:port`*`/ampassword` (對於預設組織)

   或

   `http://`*`hostname: port`*`/`*`deploy_uri`*`/ui/PWResetUserValidation?org=`*`orgname`*，其中 *orgname* 是組織的名稱。

注意 如果沒有為父系組織啟用密碼重設服務，但為子組織啟用了密碼重設服務，使用者必須使用以下語法存取該服務：

`http://`*`hostname:`*
`port``/`*`deploy_uri`*`/ui/PWResetUserValidation?org=`*`orgname`*

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問題。如果使用者先前未登入 [使用者設定檔] 頁面且未自訂個人問題，則不會產生密碼。

圖 8-2 使用者密碼問題畫面

使用者正確回答問題後，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問題，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 說明文件：

`http://docs.sun.com/source/816-6700-10/aci.html#14773`

`http://docs.sun.com/source/816-6698-10/useracct.html#14386`

第 2 部分

指令行參考指南

此部分爲「指令行參考指南」，它是「Sun™ ONE Identity Server 管理指南」的第二部分。本部分包含以下章節：

- amadmin 指令行工具
- amserver 指令行工具
- ampassword 指令行工具
- am2bak 指令行工具
- bak2am 指令行工具
- VerifyArchive 指令行工具
- amsecuridd 輔助程式

本部分描述的所有指令行工具都位於以下預設位置：

```
IdentityServer_base/SUNWam/bin
```

第 9 章

amadmin 指令行工具

本章提供有關 amadmin 指令行工具的資訊，包含以下小節：

amadmin 指令行工具可執行檔

指令行可執行檔 amadmin 的主要用途是將 XML 服務檔案載入 Directory Server，並對 DIT 執行批次管理工作。amadmin 位於 IdentityServer_base/SUNWam/bin 中，用來執行以下作業：

- 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 Identity Server 中。必須使用 amadmin 載入所有服務；不能透過 Identity Server 主控台匯入這些服務。

注意 XML 服務檔案作為供 Identity Server 參考之 XML 資料的靜態 *blob* 儲存在 Directory Server 中。Directory Server 不使用該資訊，它僅識別 LDAP。

- 對 DIT 執行身份物件的批次更新 - 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。在「*Sun One Identity Server Programmer's Guide*」中的「Service Management」一章中可以找到有關此作業的更多資訊。

注意 amadmin 僅支援 Identity Server 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*] ...

注意 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 亦可透過在網域元件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。

--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 *IdentityServer_base*`/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` 作業日誌，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。如需有關可將何種 XML 檔案傳送至此選項的更多資訊，請參閱「*Sun ONE Identity Server Programmer's Guide*」中的「Servic Management」一章。

--schema (-s)

`--schema` 是將 Identity Server 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。這種 XML 服務檔案基於 `sms.dtd`。可以指定一個或多個 XML 檔案。

注意 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，還是載入服務綱目和配置資料。

--deleteservice (-r)

`--deleteservice` 是用於僅刪除服務及其綱目的選項。

--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。此部分顯示在第 129 頁的程式碼範例 9-1 中。

程式碼範例 9-1 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。

使用 amadmin 建立策略

可以透過 amadmin 管理策略，但是不能使用 amadmin 直接修改策略。若要修改策略，必須先刪除策略，然後使用 amadmin 加入修改後的策略。

若要使用 amadmin 加入策略，必須先根據 policy.dtd. 產生策略 XML 檔案。(「*Sun ONE Identity Server Customization and API Guide*」中描述了 policy.dtd。) 開發了策略的 XML 檔案後，您可以使用以下指令載入此檔案：

IdentityServer_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，請確保建立認證網目條件時將認證模組註冊到組織；建立組織、LDAP 群組的主題、LDAP 角色的主題以及 LDAP 使用者的主題時，相應的 LDAP 物件 (組織、群組、角色和使用者) 已存在；建立 IdentityServerRoles 主題時，Identity Server 角色已存在；以及建立子組織參考或同級組織參考時相關的組織已存在。

請注意，SubOrgReferral、PeerOrgReferral、Organization 主題、IdentityServerRoles 主題、LDAPGroups 主題、LDAPRoles 主題和 LDAPUsers 主題中值元素的文字需要是完整的 DN。

第 10 章

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 指令行可執行檔可以在 Solaris 平台上建立、啓動、停止和刪除附加 Identity Server 實例。在 Windows 2000 平台上，amserver 僅允許啓動和停止 Identity Server。

amserver 語法

此工具的一般語法如下：

```
./amserver { create | delete [instance_name] | startall | start | stop |
stopall | version }
```

針對 Solaris 的 amserver 指令

建立

create 是用於建立 Identity Server 之新實例的指令。應該以超級使用者的身份執行 amserver 程序檔。若要建立實例，請執行 amserver 程序檔 ./amserver create。第 133 頁的「將 amserver 用於多伺服器安裝程式管理 (僅適用於 Web Server 實例)」中描述了建立多重伺服器實例的詳細步驟。此指令僅適用於 Web Server 實例。

startall

`startall` 是用於啓動所有 Identity server 實例的指令。若要啓動個別實例，請執行：

```
IdentityServer_base/SUNWam/bin/amserver.instance_name start
```

stopall

`stopall` 是用於停止所有 Identity server 實例的指令。若要停止個別 Identity Server 實例，請執行：

```
/opt/SUNWam/bin/amserver.instance_name stop
```

delete

`delete` 是刪除 `create` 選項建立的實例的指令。

針對 Windows 2000 的 amserver 指令

在 Windows 2000 平台上，amserver 僅支援以下指令：

start

`start` 是啓動 Identity Server 的指令。

stop

`stop` 是停止 Identity Server 的指令。

注意 如果與新的獨立於容器的部署一同使用，`stop` 和 `start` 可能無法正常運作。如果遇到這種情況，請對該容器使用 `stop` 和 `start`。

restart

`restart` 是重新啓動 Identity Server 的指令。

`amserver` 無法停止或啓動 Directory Server。您可能需要手動重新啓動它。它僅可重新啓動 Web Server 實例。對於其他 Web 容器，此指令僅可重新啓動認證輔助程式。

將 amserver 用於多伺服器安裝程式管理 (僅適用於 Web Server 實例)

您可以使用 amserver 指令行公用程式安裝和管理多個 Identity Server 實例。安裝多個 Identity Server 實例之前，您必須以超級使用者的身份登入。以下步驟中描述的程序檔位於 IdentityServer_base/SUNWam/bin 中。

若要安裝多個實例，請：

1. 輸入 ./amserver create 透過 amServer 建立新的伺服器實例。

   例如，如果您要建立名爲 instance1 的實例，該實例將偵聽 port 81，則程序檔輸出的輸出內容可能如下所示：

```
###############################################################
#####

請輸入伺服器實例的名稱：instance1

請輸入連接埠號：81

您要建立多個伺服器實例嗎？ y/[n]

正在安裝 ... 請稍候 ....

###############################################################
##
```

   a. 然後會爲每個網路伺服器實例建立一個目錄。例如：

      IdentityServer_base/SUNWam/servers/https-*instance_name*

   b. Identity Server 應用程式將被部署到以下位置：

      IdentityServer_base/SUNWam/servers/web-apps-*instance_name*

   c. IdentityServer_base/SUNWam/bin 目錄具有實例特定的 amServer 版本。例如：

      amserver.*instance_name*

d. IdentityServer_base/SUNWam/lib/AMConfig-*instance_name*.properties 中建立了 Identity Server 配置檔案的副本。

e. 檔案 /etc/rc3.d 具有實例特定的初始化檔案之版本：

S55amserver.*instance_name*

K55amserver.*instance_name*

注意 建立實例名稱時請勿使用「_」(底線) 或「.」(句點)。

2. 可輸入以下指令來啓動所有 Identity Server 實例 (包括原先的伺服器實例)：

```
./amserver startall
```

也可以使用以下指令來啓動個別伺服器：

IdentityServer_base/SUNWam/bin/amserver.*instance_name* start

現在，您應該可以透過自己的瀏覽器呼叫所有實例的 Identity Server 登入畫面。

3. 可輸入以下指令來停止所有伺服器實例 (包括原先的伺服器實例)：

```
./amserver stopall
```

也可以使用以下指令來停止個別伺服器：

IdentityServer_base/SUNWam/bin/amserver.*instance_name* stop

4. 可輸入以下指令來呼叫 [刪除指令] 選項：

```
./amserver delete
```

這將移除透過 Create 指令建立的所有檔案。如果您使用 Identity Server 解除安裝公用程式，則不會移除由程序檔產生的檔案。

5. 可輸入以下指令來指定除錯檔案的目錄：

Edit IdentityServer_base/SUNWam/lib/AMConfig-*instan ce_name*.properties

請確定將 com.iplanet.services.debug.directory 屬性變更爲指定的目錄。

6. 可使用以下語法呼叫 ammultiserverinstall 公用程式：

   ammultiserverinstall [*server-instance-name*] [*port*]

   對於需要安裝多個 Identity Server 實例，但更喜歡非互動式介面的應用程式，請使用 ammultiserverinstall 公用程式。如果 ammultiserverinstall 失敗，它將結束，且值爲 1。

7. amserver 會將伺服器實例自動加入平台伺服器清單中。

8. 配置 Identity Server 以在 SSL 模式下執行。如需此作業的說明，請參閱本指南的附錄 B「在 SSL 模式中配置 Identity Server」。

9. 輸入以下指令來啓動所有 Identity Server 實例：

   ./amserver startall

   也可以使用以下指令來啓動個別 Identity Server 實例：

   ./amserver-*instance* start

第 11 章

am2bak 指令行工具

本章提供有關 am2bak 指令行工具的資訊，包含以下小節：

am2bak 指令行可執行檔

Identity Server 在 IdentityServer_base/SUNWam/bin 下包含一個 am2bak 公用程式。該公用程式可執行 Identity Server 全部元件或所選元件的備份。進行日誌備份時必須執行 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
```

注意 必須如語法中所示，準確輸入兩個連字符號。

am2bak 選項

--verbose (-v)

--verbose 用來以冗長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。預設位置爲 IdentityServer_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 指定備份僅用於日誌檔。

--cert (-t)

--cert 指定備份僅用於證書資料庫檔案。

--ds (-d)

--ds 指定備份僅用於 Directory Server。

--all (-a)

--all 指定整個 Identity Server 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。

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：
     - *IdentityServer_base*/SUNWam/config/
     - *IdentityServer_base*/SUNWam/locale/
     - *IdentityServer_base*/SUNWam/servers/httpacl
     - *IdentityServer_base*/SUNWam/lib/*.properties (Java 屬性檔案)
     - *IdentityServer_base*/SUNWam/bin/amserver.*instance-name*
     - *IdentityServer_base*/SUNWam/servers/https-*all_instances*
     - *IdentityServer_base*/SUNWam/servers/web-apps-*all_instances*
     - *IdentityServer_base*/SUNWam/web-apps/services/WEB-INF/config
     - *IdentityServer_base*/SUNWam/web-apps/services/config
     - *IdentityServer_base*/SUNWam/web-apps/applications/WEB-INF/classes
     - *IdentityServer_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
     - *DirectoryServer_base*/slapd-*host*/config/dse.ldif
   - 日誌檔和除錯檔案：
     - var/opt/SUNWam/logs (Identity Server 日誌檔)
     - var/opt/SUNWam/install (Identity Server 安裝日誌檔)
     - var/opt/SUNWam/debug (Identity Server 除錯檔案)

- 證書：
  - *IdentityServer_base*/SUNWam/servers/alias
  - *DirectoryServer_base*/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：
  - *IdentityServer_base*/web-apps/services/WEB-INF/config/*
  - *IdentityServer_base*/locale/*
  - *IdentityServer_base*/web-apps/applications/WEB-INF/classes/*.properties (java 屬性檔案)
  - *IdentityServer_base*/servers/https-*host*/config/jvm12.conf
  - *IdentityServer_base*/servers/https-*host*/config/magnus.conf
  - *IdentityServer_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
- 日誌檔和除錯檔案：
  - var/opt/logs (Identity Server 日誌檔)
  - var/opt/debug (Identity Server 除錯檔案)
- 證書：
  - *IdentityServer_base*/servers/alias
  - *IdentityServer_base*/alias

第 12 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

bak2am 指令行可執行檔

Identity Server 在 IdentityServer_base/SUNWam/bin 下包含一個 bak2am 公用程式。該公用程式可復原透過 am2back 公用程式備份的 Identity Server 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
```

注意 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 `IdentityServer_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 `IdentityServer_base/backup`。此選項僅適用於 Solaris。

--verbose

`--verbose` 用來以冗長模式執行備份公用程式。

--directory

`--directory` 指定備份目錄。依預設，路徑爲 `IdentityServer_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。

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. 解壓縮輸入的 tar 檔案。

   這是在執行備份程序檔時產生的。

第 13 章

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

Identity Server 包含 ampassword 公用程式 (位於 $installroot/SUNWam/bin 下)。該公用程式可讓您變更管理員或使用者的 Identity Server 密碼。

ampassword 語法

使用 ampassword 工具的一般語法如下：

```
ampassword -a | --admin [ -o | --old oldPassword -n | --new newPassword
]

ampassword -p | --proxy [ -o | --old oldPassword -n | --new newPassword
]

ampassword -e | --encrypt [ password ]
```

注意 必須如語法中所示，準確輸入兩個連字符號。

ampassword 選項

--admin (-a)

--admin 用於變更管理密碼。

--proxy (-p)

`--proxy` 用於變更代理密碼。它相當於代理使用者 (`serverconfig.xml` 中的使用者類型 `proxy`。)

--encrypt (-e)

`--encrypt` 用於加密密碼。它會被列印到指令行中。

於 SSL 之上執行 ampassword

若要使用以安全套接層 (SSL) 模式執行的 Identity Server 來執行 ampassword，請：

1. 修改位於以下目錄中的 serverconfig.xml 檔案：

   `IdentityServer_base/SUNWam/config/ums`

2. 將伺服器屬性 `port` 變更爲 Identity Server 正在執行的 SSL 連接埠。
3. 將屬性 `type` 變更爲 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` 以及 Identity Server 的所有認證範本中的密碼。

第 14 章

VerifyArchive 指令行工具

本章提供有關 VerifyArchive 指令行工具的資訊，包含以下小節：

VerifyArchive 指令行可執行檔

VerifyArchive 的用途是驗證日誌歸檔檔案。日誌歸檔檔案是一組標記了時間的日誌及其相應的鍵值儲存區 (鍵值儲存區包含用於產生 MAC 和數位簽名 [用於偵測日誌檔竄改] 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。執行後，VerifyArchive 搜尋每個日誌記錄，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。

VerifyArchive 語法

需要所有的參數選項。語法如下所示：

VerifyArchive -l logName -p *path* -u *uname* -w *password*

VerifyArchive 選項

logName

logName 指要驗證的日誌之名稱 (如 amConsole、amAuthentication 等等)。VerifyArchive 驗證給定 logName 的存取權限和錯誤日誌。例如，如果指定 amConsole，檢驗器會驗證 amConsole.access 和 amConsole.error 檔案。或者，可以將 logName 指定爲 amConsole.access 或 amConsole.error，只對那些日誌進行驗證。

path

path 是儲存日誌檔的完整目錄路徑。

uname

uname 是 Identity Server 管理員的使用者 ID。

password

password 是 Identity Server 管理員的密碼。

第 15 章

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

Identity Server SecurID 認證模組透過 Security Dynamic ACE/Client C API 和 amsecruidd 輔助程式來實施，此輔助程式可在 Identity Server 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。

注意 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。

由於 amsecuridd 的介面透過 stdin 爲明文，因此僅允許有本機主機連線。amsecuridd 可使用後端的 SecurID 遠端 API (5.x 版) 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 *IdentityServer_base*/SUNWam/lib/ 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 Identity Sever。

注意 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

冗長 *(-v)*

開啓冗長模式，並記錄到 /var/opt/SUNWam/debug/securidd_client.debug。

配置連接埠號 *(-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 *IdentityServer_base*/SUNWam/share/bin 中。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，但它僅可以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

注意 將 LD_LIBRARY_PATH 設定爲 *IdentityServer_base*/Sunwam/lib/ 以找到 libaceclnt.so。

第 3 部分

屬性參考指南

「屬性參考指南」是「Sun ONE Identity Server 管理指南」的第三部分。本部分論述 Identity Server 的預設服務中的配置屬性。本部分包含以下章節：

- 記錄服務屬性
- 命名服務屬性
- 密碼重設服務
- 平台服務屬性
- 策略配置服務屬性
- SAML 服務屬性
- 階段作業服務屬性
- 使用者屬性

第 16 章

管理服務屬性

管理服務由全域屬性與組織屬性組成。套用於全域屬性的值也套用於整個 Sun ONE Identity Server 配置，並由每個配置的組織繼承。由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。套用於組織屬性的值是每個配置組織的預設值，並且在向組織註冊此服務時可以變更。組織屬性不會由組織項目來繼承。管理屬性分爲：

- 全域屬性
- 組織屬性

全域屬性

管理服務中的全域屬性包括：

- 啓用聯合管理
- 啓用使用者管理
- 顯示個人容器
- 在功能表中顯示容器
- 顯示群組容器
- 受管理群組類型
- 預設角色權限 (ACI)
- 啓用網域元件樹

- 啓用管理員群組
- 啓用相容性使用者刪除
- 動態管理員角色 ACI
- 使用者設定檔服務類別
- DC 節點屬性清單
- 用於已刪除物件的搜尋過濾器

啟用聯合管理

選取此欄位會啓用聯合管理。依預設會選取此欄位。若要停用此功能，請取消選取該欄位，主控台中將不會顯示 [聯合管理服務] 標籤。

啟用使用者管理

選取此欄位 (True) 會啓用使用者管理。依預設會啓用使用者管理。

顯示個人容器

此屬性指定是否在 Identity Server 主控台中顯示 [個人容器]。如果選取此選項，組織、容器與群組容器的 [檢視] 功能表中將顯示 [個人容器] 功能表選項。僅在平面 DIT 的頂層才會顯示 [個人容器]。

個人容器是包含使用者設定檔的組織單元。建議您在 DIT 中使用單一個人容器，並充分利用角色的靈活性來管理帳戶與服務。Identity Server 主控台的預設運作方式是隱藏 [個人容器]。但是，如果在 DIT 中有多重個人容器，請選取 [顯示個人容器]，以將個人容器顯示爲 Identity Server 主控台中的受管理物件。

在功能表中顯示容器

此屬性指定是否在 Identity Server 主控台的 [檢視] 功能表中顯示任何容器。預設值爲 `false`。管理員可以選擇性地選擇以下兩個值之一：

- `false` (未選取核取方塊) — 組織頂層與其他容器頂層的 [檢視] 功能表選項中不列出容器。
- `true` (選取核取方塊) — 組織頂層與其他容器頂層的 [檢視] 功能表選項中列出容器。

顯示群組容器

此屬性指定是否在 Identity Server 主控台中顯示 [群組容器]。如果選取此選項，組織、容器與群組容器的 [檢視] 功能表中將顯示 [群組容器] 功能表選項。群組容器是群組的組織單元。

受管理群組類型

此選項指定透過主控台建立的是靜態訂閱群組還是動態訂閱群組。主控台將建立並顯示靜態訂閱群組或動態訂閱群組，但不能兩者皆選。(無論此屬性給定何值，將始終支援過濾群組。) 預設值爲動態。

- 靜態群組會使用 `groupOfNames` 或 `groupOfUniqueNames` 物件類別明確列出每個群組成員。群組項目包含此群組每個成員的 `uniqueMember` 屬性。可以手動加入靜態群組成員，使用者項目本身保持不變。靜態群組適用於成員較少的群組。
- 動態群組使用每個群組成員項目中的 `memberOf` 屬性。LDAP 過濾可以搜尋並傳回包含 `memberOf` 屬性的所有項目。透過使用該過濾，可以產生動態群組成員。動態群組適用於具有很多成員的群組。
- 已過濾群組使用 LDAP 過濾搜尋並傳回滿足過濾要求的成員。例如，過濾可以產生具有特定 uid (`uid=g*`) 或電子郵件位址 (`mail=*@sun.com`) 的成員。在這些範例中，LDAP 過濾會分別傳回 uid 以 g 開頭或電子郵件位址以 `sun.com` 結尾的所有使用者。在 [使用者管理] 檢視內，只能透過選擇 [依過濾確定成員身份] 來建立過濾群組。

管理員可以選取以下一種選項：

- `Dynamic` — 透過 [依訂閱確定成員身份] 選項建立的將是動態群組。
- `Static` — 透過 [依訂閱確定成員身份] 選項建立的將是靜態群組。

預設角色權限 (ACI)

此屬性定義在建立新角色時，用來授與管理員權限的預設存取控制指令 (ACI) 或**權限**清單。可以依據所需權限層級選取其中一個 ACI。Identity Server 隨附了四種預設角色權限：

無權限

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存取權限。

組織說明桌面管理員

組織說明桌面管理員具有對配置組織中所有項目的讀取存取權限，以及對 `userPassword` 屬性的寫入存取權限。

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存取權限。組織策略管理員無法建立同級組織的參考策略。

注意

使用格式 `aci_name | aci_desc | dn:aci ## dn:aci ## dn:aci` 定義角色，其中：

- *aci_name* 為 ACI 的名稱。
- *aci_desc* 為這些 ACI 所允許之存取權限的描述。為了使描述更簡單易懂，請假定此描述的讀者不瞭解 ACI 或其他目錄概念。

aci_name 與 *aci_desc* 是 `amAdminUserMsgs.properties` 檔案中包含的 i18n 鍵值。顯示在主控台中的值來自 `.properties` 檔案，可以使用鍵值擷取這些值。

- *dn:aci* 表示由 ## 分隔的 DN 與 ACI 對，Identity Server 會在關聯的 DN 項目中設定每個 ACI。此格式還支援可以取代值的標籤 (否則必須在 ACI 中逐字指定這些值)：ROLENAME、ORGANIZATION、GROUPNAME 與 PCNAME。使用這些標籤可讓您非常靈活地定義角色，以將其作為預設角色。基於一種預設角色建立角色時，ACI 中的標籤將解析為從新角色 DN 中提取的值。

啟用網域元件樹

網域元件樹 (DC 樹) 是許多 Sun ONE 元件使用的特定 DIT 結構，用於在 DNS 名稱與組織的項目之間建立對映。

如果在建立組織時輸入了組織的 DNS 名稱，則啓用此選項會建立組織的 DC 樹項目。[建立組織] 頁面中將顯示 [DNS 名稱] 欄位。此選項僅適用於頂層組織，對於子組織將不會顯示此選項。

透過 Identity Server SDK 對組織樹中的 `inetdomainstatus` 屬性所做的任何狀態變更都將更新對應的 DC 樹項目狀態。(不是透過 Identity Server SDK 進行的狀態更新將不會同步進行。) 例如，如果建立一個 DNS 名稱屬性爲 sun.com 的新組織 `sun`，則將在 DC 樹中建立以下項目：

`dc=sun,dc=com,o=internet,`*root suffix*

透過在 `AMConfig.properties` 中設定 `com.iplanet.am.domaincomponent`，可以選擇性地配置 DC 樹的根字尾。依預設，其設定爲 Identity Server root。如果需要其他字尾，則必須使用 LDAP 指令建立此字尾。需要修改建立組織的管理員 ACI，以便它們能夠無限制地存取新的 DC 樹根。

啟用管理員群組

此選項指定是否建立 DomainAdministrators 和 DomainHelpDeskAdministrators 群組。如果選取此選項 (`true`)，會建立這些群組，並分別與組織管理員角色和組織說明桌面管理員角色相關聯。一旦建立了這些群組，在某個關聯角色中加入或移除使用者時，相應的群組中也會加入或移除該使用者。但是，該運作方式不可反向進行。在某個群組中加入或移除使用者時，將不會在使用者關聯角色中加入或移除此使用者。

僅在啓用此選項後所建立的組織中，才會建立 DomainAdministrators 和 DomainHelpDeskAdministrators 群組。

注意 此選項不適用於子組織，`root org` 除外。在 `root org` 中，會建立 ServiceAdministrators 與 ServiceHelpDesk Administrators 群組，並將它們分別與頂層管理員角色與頂層說明桌面管理員角色關聯。同樣的運作方式在此也適用。

啟用相容性使用者刪除

此選項指定是否從目錄中刪除使用者的項目，還是僅將其標記爲已刪除。如果在選取此選項 (`true`) 的情況下刪除使用者項目，使用者的項目仍將存在於此目錄中，但是將會標記爲已刪除。Directory Server 搜尋時不會傳回標記爲已刪除的使用者項目。如果未選取此選項，則將從目錄中刪除使用者的項目。

動態管理員角色 ACI

此屬性定義管理員角色 (使用 Identity Server 配置群組或組織時動態建立的角色) 的存取控制指令。這些角色用於爲所建立的特定項目群組授與管理權限。僅在此屬性清單中才可修改預設 ACI。

警告 **組織層級管理員的存取權限比群組管理員大。但是，依預設，使用者加入至群組管理員角色後，該使用者可以變更此群組中的任何成員密碼。其中包括作為此群組成員的任何組織管理員。**

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中的所有項目均具有讀取存取權限，但是僅對此容器單元中使用者項目的 `userPassword` 屬性具有寫入存取權限。

組織說明桌面管理員

組織說明桌面管理員具有對組織中所有項目的讀取存取權限，以及對 `userPassword` 屬性的寫入存取權限。

注意 **建立子組織時，請記住在子組織中建立管理角色，而不是在父系組織中建立。**

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存取權限。在 Identity Server 中，LDAP 組織單元常指容器。

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存取權限，可以建立、指定、修改和刪除此組織內的所有策略。

個人容器管理員

依預設，新建組織中的任何使用者項目均爲該組織的個人容器的成員。個人容器管理員對組織的個人容器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」具有讀取寫入存取權限，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。

注意 可以透過 Identity Server 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

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。角色必須由群組建立者或任何具有群組管理員角色存取權限的人員指定。

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存取權限。換句話說，此頂層管理員角色具有 Identity Server 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存取權限。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。

使用者設定檔服務類別

此屬性列出將在 [使用者設定檔] 頁面中具有自訂顯示的服務。對於某些服務，主控台產生的預設顯示可能無法滿足需要。此屬性爲任何服務建立自訂顯示，並完全控制顯示服務資訊的內容與方式。語法如下所示：

service name | *relative url*

注意 [建立使用者] 頁面中將不會顯示此屬性中列出的服務。必須在 [使用者設定檔] 頁面中執行自訂服務顯示的所有資料配置。

DC 節點屬性清單

此欄位定義建立物件時將在 DC 樹項目中設定的一組屬性。預設參數包括：

- maildomainwelcomemessage
- preferredmailhost
- mailclientattachmentquota
- mailroutingsmarthost
- mailroutingsmarthost
- mailroutingsmarthost
- mailaccessproxyreplay
- preferredlanguage
- domainuidseparator
- maildomainmsgquota
- maildomainallowedserviceaccess
- preferredmailmessagestore
- maildomaindiskquota
- maildomaindiskquota
- objectclass=maildomain
- mailroutinghosts

用於已刪除物件的搜尋過濾器

此欄位定義啓用使用者相容性刪除模式時用於要刪除物件的搜尋過濾器。

組織屬性

管理服務中的組織屬性包括：

- 群組預設個人容器
- 群組個人容器清單
- 使用者設定檔顯示類別
- 顯示使用者的角色
- 顯示使用者的群組
- 使用者群組自訂閱
- 使用者設定檔顯示選項
- 使用者建立預設角色
- 檢視功能表項目
- 搜尋傳回的最大結果數
- 搜尋逾時 (秒)
- JSP 目錄名稱
- 線上說明文件
- 必需的服務
- 使用者搜尋關鍵字
- 使用者搜尋傳回屬性
- 使用者建立通知清單
- 使用者刪除通知清單
- 使用者修改通知清單

- 每頁的最大項目數
- 顯示選項
- 事件偵聽程式類別
- 處理前和處理後的類別
- 啓用外部屬性擷取

群組預設個人容器

此欄位指定預設的個人容器 (使用者建立後將放置於其中的容器)。此欄位沒有預設值。有效值爲個人容器 DN。請參閱 [群組個人容器清單] 屬性下的注意事項，以瞭解個人容器退回的次序。

群組個人容器清單

此欄位指定個人容器的清單，群組管理員在建立新使用者時可以從中選擇個人容器。如果在目錄樹中有多重個人容器，則可以使用此清單。(如果未在此清單或 [群組預設個人容器] 欄位中指定任何個人容器，則將在預設的 Identity Server 個人容器 `ou=people` 中建立使用者。) 此欄位沒有預設值。此屬性的語法如下所示：

group name|*dn of people container*

注意 建立使用者時，會檢查此屬性中是否有放置此項目的容器。如果此屬性為空，將會檢查 [群組預設個人容器] 屬性是否存在容器。如果後一個屬性為空，則將在 `ou=people` 下建立此項目。

使用者設定檔顯示類別

此屬性指定顯示 [使用者設定檔] 頁面時，Identity Server 主控台所使用的 Java 類別。

顯示使用者的角色

此選項指定是否在使用者的使用者設定檔頁面中顯示指定給使用者的角色清單。如果值爲 `false`（未選取），使用者設定檔頁面將僅對管理員顯示使用者的角色。預設值爲 `false`。

顯示使用者的群組

此選項指定是否在使用者的使用者設定檔頁面中顯示指定給使用者的群組清單。如果值爲 `false`（未選取），使用者設定檔頁面將僅對管理員顯示使用者的群組。預設值爲 `false`。

使用者群組自訂閱

此選項指定使用者是否可以將自己加入至可自由訂閱的群組。如果值爲 false，則使用者設定檔頁面僅允許管理員修改使用者的群組成員身份。預設值爲 `false`。

注意 此選項僅在選取 [顯示使用者的群組] 選項時才適用。

使用者設定檔顯示選項

此功能表指定將顯示在使用者設定檔頁面中的服務屬性。管理員可以選取以下選項：

- `UserOnly` — 顯示指定給使用者的服務之可檢視使用者綱目屬性。

  使用者服務屬性包含關鍵字「Display」時，使用者可以檢視此屬性值。請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得詳細資訊。

- `Combined` — 顯示指定給使用者的服務之可檢視使用者與動態綱目屬性。

使用者建立預設角色

此清單定義將自動指定給新建使用者的角色。此欄位沒有預設值。管理員可以輸入一個或多個角色的 DN。

注意 此欄位僅採用完整的識別名稱位址，不採用角色名稱。

檢視功能表項目

此欄位列出將在主控台頂端的 [檢視] 功能表中顯示的 Java 服務類別。語法爲 `i18N key | java class name`。(i18N key 作爲 [檢視] 功能表中項目的本土化名稱。)

搜尋傳回的最大結果數

此欄位定義搜尋傳回的最大結果數。預設值爲 100。

警告 將此屬性設定為大的值時請小心。如需大小限制的資訊，請參閱以下位置的「*Sun ONE Directory Server Installation and Tuning Guide*」：

`http://docs.sun.com/db/doc/816-6697-10`

搜尋逾時 (秒)

此欄位定義搜尋在逾時之前所執行的時間 (秒數)。可以使用它終止潛在的長時間搜尋。達到最大搜尋時間後，會傳回一個錯誤。預設值爲 5 秒。

JSP 目錄名稱

此欄位指定包含 `.jsp` 檔案的目錄名稱，該檔案用於建構主控台，以使組織具有不同外觀 (自訂)。需要將 `.jsp` 檔案複製到此欄位中指定的目錄。

線上說明文件

此欄位列出將在主 Identity Server 說明頁面上建立的線上說明連結。這樣其他應用程式可以在 Identity Server 頁面中加入其線上說明連結。此屬性的格式如下所示：

linki18nkey | **按一下時要載入的** *html* **頁面** | *i18n* **屬性檔案**

例如：

`IdentityServer Help | /AMAdminHelp.html | amAdminModuleMsgs`

必需的服務

此欄位列出在建立使用者的項目時動態加入其中的服務。管理員可以選擇建立時要加入的服務。

此屬性並非由主控台使用，而是由 Identity Server SDK 使用。動態建立的使用者和由 `amadmin` 指令行公用程式建立的使用者，將被指定給此屬性中列出的服務。

使用者搜尋關鍵字

此屬性定義在 [導覽] 頁面中執行簡單搜尋時要依據的屬性名稱。此屬性的預設值爲 `cn`。例如，如果此屬性使用預設值：

如果在導覽框架的 [名稱] 欄位中輸入 `j*`，則會顯示名稱以「j」或「J」開頭的使用者。

使用者搜尋傳回屬性

此欄位定義顯示簡單搜尋傳回的使用者時所使用的屬性名稱。此屬性的預設值爲 `uid cn`。這將顯示使用者 ID 和使用者的全名。

列在最前面的屬性名稱還會作爲關鍵字來排序將被傳回的一組使用者。若要避免效能降低，請使用在使用者的項目中設定值的屬性。

使用者建立通知清單

此欄位定義建立新使用者時要將通知傳送至的電子郵件位址清單。可以指定多重電子郵件位址，如以下語法中所示：

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

透過使用 |locale 選項，通知清單還可接受不同的語言環境。例如，將通知傳送至在法國的管理員：

someuser@example.com|fr|fr

請參閱第 191 頁的表 19-1 ，以取得語言環境清單。

注意 透過修改 amProfile.properties (依預設位於 IdentityServer_base/Identity-Server/SUNWam/locale) 中的屬性 497，可以變更寄件者電子郵件 ID。

使用者刪除通知清單

此欄位定義刪除使用者時要將通知傳送至的電子郵件位址清單。可以指定多重電子郵件位址，如以下語法中所示：

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

透過使用 |locale 選項，通知清單還可接受不同的語言環境。例如，將通知傳送至在法國的管理員：

someuser@example.com|fr|fr

請參閱第 191 頁的表 19-1 ，以取得語言環境清單。

注意 透過修改 amProfile.properties (依預設位於 IdentityServer_base/Identity-Server/SUNWam/locale) 中的屬性 497，可以變更寄件者電子郵件 ID。預設寄件者 ID 為 DSAME。

使用者修改通知清單

此欄位定義屬性及其關聯的電子郵件位址清單。如果修改了清單中定義的使用者屬性，通知將會傳送至與此屬性關聯的電子郵件位址。每個屬性都可以具有不同的關聯位址集。可以指定多重電子郵件位址，如以下語法中所示：

```
attrName e-mail|locale|charset e-mail|locale|charset .....

attrName e-mail|locale|charset e-mail|locale|charset .....
```

可以使用 `self` 關鍵字來取代其中一個位址。這時將向其設定檔已修改的使用者傳送電子郵件。

例如：

```
manager someuser@sun.com|self|admin@sun.com
```

電子郵件將傳送至 `manager` 屬性中指定的位址：`someuser@sun.com`、`admin@sun` 以及修改了使用者的人員 (`self`)。

通過使用 `|locale` 選項，通知清單還可以接受不同的語言環境。例如，將通知傳送至在法國的管理員：

```
manager someuser@sun.com|self|admin@sun.com|fr
```

請參閱第 191 頁的表 19-1 ，以取得語言環境清單。

注意 此屬性名稱與 Directory Server 綱目中顯示的名稱相同，但與主控台中顯示的名稱不同。

每頁的最大項目數

此屬性允許您定義每頁可顯示的最大列數。預設值爲 25。例如，如果使用者搜尋傳回 100 列，則會顯示 4 頁，每頁顯示 25 列。

顯示選項

此屬性允許您加入值，以在 Identity Server 主控台中配置顯示選項。輸入值並按一下 [加入] 可以配置顯示選項。可能的值如下所示：

表 16-1 顯示選項值

參數	描述和語法
generateUserCN	設定爲 true 時，此參數將在建立使用者時動態產生使用者 CN。預設值爲 false。語法： `generateUserCN=[false|true]`
userAttributeNameForProfileTitle	決定在 [使用者設定檔] 頁面的標題上顯示的使用者屬性值。預設值爲 uid。 語法： `userAttributeNameForProflleTitle=[uid|`*`userAttribute`*`]`
autoSelect	設定爲 true (預設值) 時，此參數可讓 Identity Server 自動選取 [導覽] 檢視中給定身份物件類型的第一個項目。 語法： `autoselect=[true|false]`
disableIntitialSearch	此值將停用 Identity Server 對一個或多個身份物件類型的初始搜尋。停用初始搜尋可縮短顯示 Identity Server 主控台的時間。主控台中與此指令對應的服務屬性是顯示選項，即管理服務中的組織屬性。此主控台選項優先於 `com.iplanet.am.console.display.off` 中定義的任何值。如果在 `AMConfig.properties` 中配置此屬性，請勿使用主控台進行配置 (反之亦然)。 語法 (用逗號分隔多重值)： `disableInitialSearch=[users|organizaitons|peopleContainers|organizationalUnits|roles|groups|policies]`

參數	描述和語法
defaultUserView	此參數設定 [使用者設定檔] 頁面之 [檢視] 功能表中的預設檢視。所有值均依預設設定。 語法： `defaultUserView=[roles|groups|services|IplanetAMUserService|`*`service name]`*
defaultGroupView	此參數設定 [群組設定檔] 頁面之 [檢視] 功能表中的預設檢視。所有值均依預設設定。 語法： `defaultGroupView=[general|users]`
defaultRoleView	此參數設定 [角色設定檔] 頁面之 [檢視] 功能表中的預設檢視。所有值均依預設設定。 語法： `defaultRoleView=[general|users|services]`
defaultPolicyView	此參數設定 [策略設定檔] 頁面之 [檢視] 功能表中的預設檢視。所有值均依預設設定。 語法： `defaultPolicyView=[general|rules|subjects|referrals|conditions]`
defaultFederationHostedProviderView	此參數設定聯合管理模組的 [託管供應商設定檔] 頁面之 [檢視] 功能表中的預設檢視。所有值均依預設設定。語法： `defaultFederationHostedProviderView=[general|serviceProvider|identityProvider|authenticaionDomain|trustedProviders|identityServerConfiguration]`

參數	描述和語法
defaultFederationRemoteProviderView	此參數設定聯合管理模組的 [遠端供應商設定檔] 頁面之 [檢視] 功能表中的預設檢視。所有值均依預設設定。語法： `defaultFederationRemoteProviderView=[general|serviceProvider|identityProvider|authenticaionDomain]`
rootNavMenu	此參數設定根字尾導覽檢視中身份物件的預設檢視。所有值均依預設設定。 語法： `rootNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`
organizationNavMenu	此參數設定組織導覽檢視中身份物件的預設檢視。所有值均依預設設定。 語法： `organizationNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`
groupContainerNavMenu	此參數設定群組容器導覽檢視中身份物件的預設檢視。所有值均依預設設定。 語法： `groupContainerNavMenu=[groupContainers|groups]`
peopleContainerNavMenu	此參數設定個人容器導覽檢視中身份物件的預設檢視。所有值均依預設設定。 語法： `peopleContainerNavMenu=[peopleContainers|users]`

參數	描述和語法
federationNavMenu	此參數設定聯合管理模組導覽檢視中身份物件的預設檢視。所有值均依預設設定。 語法： `federationNavMenu=[authenticationDomains|hostedProviders|remoteProviders]`
userProfileMenu	此參數設定 [使用者設定檔] 頁面中的子檢視功能表項目。所有值均依預設設定。 語法： `userProfileMenu=[roles|groups|services|iPlanetAMUserService|`*`service name`*`]`
groupProfileMenu	此參數設定 [群組設定檔] 頁面中的子檢視功能表項目。所有值均依預設設定。 語法： `groupProfileMenu=[general|users]`
roleProfileMenu	此參數設定 [角色設定檔] 頁面中的子檢視功能表項目。所有值均依預設設定。 語法： `roleProfileMenu=[general|users|services]`
policyProfileMenu	此參數設定 [策略設定檔] 頁面中的子檢視功能表項目。所有值均依預設設定。 語法： `policyProfileMenu=[general|rules|subjects|referrals|conditions]`

參數	描述和語法
federationRemoteProviderProfile Menu	此參數設定 [聯合遠端供應商設定檔] 頁面中的子檢視功能表項目。所有值均依預設設定。 語法： `federationRemoteProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain]`
FederationHostedProviderProfile Menu	此參數設定 [聯合託管供應商設定檔] 頁面中的子檢視功能表項目。所有值均依預設設定。 語法： `federationHostedProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain|trustedProviders|identityServerConfiguration]`

事件偵聽程式類別

此屬性包含接收 Identity Server 主控台中建立、修改和刪除等事件的偵聽程式清單。

處理前和處理後的類別

此欄位經由外掛程式定義實施類別清單，這些外掛程式可延伸 `com.iplanet.am.sdk.AMCallBack` 類別，以在針對使用者、組織、角色和群組的處理前作業和處理後作業期間接收回呼。這些作業包括：

- 建立
- 刪除
- 修改
- 將使用者加入角色/群組
- 從角色/群組中刪除使用者

您必須輸入外掛程式的完整類別名稱，例如：

```
com.iplanet.am.sdk.AMCallbacSample
```

然後，您必須變更 Web 容器的類別路徑 (來自 Identity Server 安裝基準)，使之包括外掛程式類別所在位置的完整路徑。

啟用外部屬性擷取

此選項可讓外掛程式的回呼擷取外部屬性 (任何特定於外部應用程式的屬性)。外部屬性並不在 Identity Server SDK 中進行快取，因此該屬性可讓您按組織層級啓用屬性擷取。依預設，不啓用此選項。

第 17 章

匿名認證屬性

匿名認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲匿名認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊之後組織的管理員可以變更預設值。組織屬性不會由組織子樹中的項目繼承。匿名認證屬性包括：

- 有效匿名使用者清單
- 區分大小寫的使用者名稱
- 預設匿名使用者名稱
- 認證層級

有效匿名使用者清單

此欄位包含無需提供憑證便可登入的使用者 ID 清單。如果使用者的登入名稱與此清單中的使用者 ID 相符，則授與存取權並將階段作業指定給指定的使用者 ID。

如果此清單爲空，則存取以下預設模組登入 URL 將被認證爲預設匿名使用者名稱：

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

如果此清單不爲空，則存取預設模組登入 URL (與上述相同) 將會提示使用者輸入任何有效匿名使用者名稱

如果此清單不爲空，使用者透過存取以下 URL 可以無需看到登入頁面而登入：

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=<valid Anonymous username>
```

區分大小寫的使用者名稱

如果啓用了此選項，則使用者 ID 會區分大小寫。依預設，不啓用此屬性。

預設匿名使用者名稱

如果 [有效匿名使用者清單] 爲空且以下預設模組登入 URL 被存取，此欄位會定義已被指定階段作業的使用者 ID：

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

預設值爲 anonymous。同時，必須在組織中建立匿名使用者。

注意 如果 [有效匿名使用者清單] 不為空，您可透過使用 [預設匿名使用者名稱] 中定義的使用者無需存取登入頁面而登入。透過存取以下 URL 可完成此作業：

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=<DefaultAnonymous User Name>
```

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式會使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 0。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 18 章

證書認證屬性

證書認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲證書認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊之後組織的管理員可以變更預設值。組織屬性不會由組織子樹中的項目繼承。證書認證屬性包括：

- 與 LDAP 中的證書相符
- 主題 DN 中用於搜尋 LDAP 的屬性
- 證書與 CRL 相符
- 發行者 DN 中用於搜尋 CRL 的屬性
- 啓用 OCSP 驗證
- LDAP 伺服器與連接埠
- LDAP 起始搜尋 DN
- LDAP 伺服器主體使用者
- LDAP 伺服器主體密碼
- 設定檔 ID 的 LDAP 屬性
- 使用 SSL 存取 LDAP
- 證書中用於存取使用者設定檔的欄位
- 證書中用於存取使用者設定檔的其他欄位
- 可信任的遠端主機
- SSL 連接埠號
- 認證層級

與 LDAP 中的證書相符

此選項指定是否檢查登入時出示的使用者證書是否儲存在 LDAP 伺服器中。如果找不到相符的證書，則會拒絕使用者存取。如果找到相符的證書，並且不需要其他驗證，則允許使用者存取。依預設，證書認證服務不會檢查使用者證書。

注意 儲存在 Directory Server 中的證書不一定有效，證書廢止清單中也可能存在該證書。請參閱第 180 頁的「證書與 CRL 相符」。但是，Web 容器可能會檢查登入時所出示使用者證書的有效性。

主題 DN 中用於搜尋 LDAP 的屬性

此欄位指定證書 SubjectDN 值的屬性，該值將用於在 LDAP 中搜尋證書。該屬性必須唯一地識別使用者項目。搜尋將使用此實際值。預設值爲 CN。

證書與 CRL 相符

此選項指定是否針對 LDAP 伺服器中的證書廢止清單 (CRL) 比對使用者證書。此 CRL 的位置由發行者的 SubjectDN 中的某個屬性名稱確定。如果 CRL 中存在此證書，則拒絕使用者存取；如果不存在，則允許使用者存取。依預設，此屬性是停用的。

注意 發生以下情況時應該廢止證書：證書擁有者的狀態已經變更，不再具有使用此證書的權限；或者證書擁有者的私密密鑰已經洩漏。

發行者 DN 中用於搜尋 CRL 的屬性

此欄位指定已收到證書的發行者 subjectDN 值的屬性，此值將用於在 LDAP 中搜尋 CRL。僅在 [證書與 CRL 相符] 屬性啓用時，才使用此欄位。搜尋將使用此實際值。預設值爲 CN。

啟用 OCSP 驗證

此參數透過與相應的 OCSP 回應者進行聯絡，來啓用要執行的 OCSP 驗證。在運行時間，OCSP 回應者如下決定：

- 如果 `com.sun.identity.authentication.ocspCheck` 爲 **true**，且在 `com.sun.identity.authentication.ocsp.repsonder.url` 屬性中設定了 OCSP 回應者，則此屬性的值將作爲 OCSP 回應者。
- 如果將 `com.sun.identity.authentication.ocspCheck` 設定爲 **true**，且未在 `AMConfig.properties` 檔案中設定此屬性值，則在您的用戶端證書中顯示的 OCSP 回應者會作爲 OCSP 回應者。

如果將 `com.sun.identity.authentication.ocspCheck` 設定爲 **false**，或將 `com.sum.identity.authentication.ocspCheck` 設定爲 **true**，且無法找到 OCSP 回應者，則不會執行任何 OCSP 驗證。

注意 在啟用 OCSP 驗證之前，請確定 Identity Server 機器與 OCSP 回應者機器上的時間儘可能同步。而且，Identity Server 機器上的時間不能晚於 OCSP 回應者機器上的時間。例如：

OCSP 回應者機器 - 中午 12:00:00

Identity Server 機器 - 下午 12:00:30

LDAP 伺服器與連接埠

此欄位指定儲存證書的 LDAP 伺服器名稱與連接埠號。預設值爲安裝 Identity Server 時指定的主機名稱與連接埠。可以使用任何儲存證書的 LDAP 伺服器之主機名稱與連接埠。格式爲 *hostname:port*。

LDAP 起始搜尋 DN

此欄位指定應該開始搜尋使用者證書的節點 DN。此欄位沒有預設值。此欄位將識別任何有效 DN。多重項目必須以本機伺服器名稱作爲字首。

LDAP 伺服器主體使用者

此欄位會接受儲存證書的 LDAP 伺服器之主體使用者 (通常爲目錄管理員) DN。將辨識任何有效 DN 的此欄位沒有預設值。必須授與主體使用者讀取與搜尋儲存於 Directory Server 中之認證資訊的權限。

LDAP 伺服器主體密碼

此欄位具有與 [LDAP 伺服器主體使用者] 欄位中指定的使用者關聯的 LDAP 密碼。此欄位沒有預設值，它將辨識指定的主體使用者之有效 LDAP 密碼。

注意 此值作爲可讀文字儲存在目錄中。

設定檔 ID 的 LDAP 屬性

此欄位指定與證書 (應該使用其值識別正確的使用者設定檔) 相符的 Directory Server 項目中之屬性。此欄位沒有預設值，它將辨識使用者項目中可以作爲使用者 ID 的任何有效屬性 (`cn`、`sn` 等)。

使用 SSL 存取 LDAP

此選項指定是否使用 SSL 存取 LDAP 伺服器。預設情況下，證書認證服務不使用 SSL 存取 LDAP。

證書中用於存取使用者設定檔的欄位

此功能表指定應該使用證書主題 DN 中的哪個欄位來搜尋相符的使用者設定檔。例如，如果選擇 `email address`，則證書認證服務將搜尋與使用者證書中 `emailAddr` 屬性相符的使用者設定檔。然後使用者會使用此相符設定檔進行登入。預設欄位爲 `subject CN`。此清單包含：

- 電子郵件位址
- 主題 CN
- 主題 DN
- 主題 UID
- 其他

證書中用於存取使用者設定檔的其他欄位

如果將 [證書中用於存取使用者設定檔的欄位] 屬性值設定爲 `other`，則此欄位指定要從接收的證書 `subjectDN` 值中選取的屬性。然後，此認證服務將搜尋與該屬性值相符的使用者設定檔。

可信任的遠端主機

此屬性定義可信任的主機清單，這些主機可被信任以向 Identity Server 傳送證書。Identity Server 必須驗證證書是否來自這些主機中的一個。此配置僅用於 Sun ONE Portal Server。

SSL 連接埠號

此屬性指定安全套接層的連接埠號。目前，此屬性僅由 Gateway servlet 使用。加入或變更 SSL 連接埠號之前，請參閱「Sun ONE Identity Server Customization and API Guide」的第 7 章中「Policy-Based Resource Management」一節。

認證層級

會分別爲每個認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式將使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 0。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 19 章

核心認證屬性

核心認證服務是所有預設認證服務的基本服務，也是使用認證 SPI 建立的任何自訂認證服務的基本服務。必須爲每個希望使用任何形式認證的組織配置核心認證服務。核心認證屬性由全域屬性與組織屬性組成。套用於全域屬性的值也套用於整個 Sun ONE Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。) 在服務配置下套用於組織屬性的值將成爲核心認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊之後組織的管理員可以變更預設值。組織屬性不會由組織中的項目繼承。核心認證屬性分爲：

- 全域屬性
- 組織屬性

全域屬性

核心認證服務中的全域屬性包括：

- 可插接式認證模組類別
- 用戶端支援的認證模組
- LDAP 連線區大小
- LDAP 連線區預設大小

可插接式認證模組類別

此欄位指定 Identity Server 平台內部配置的所有組織均可以使用的認證模組的 Java 類別。依預設，包含 LDAP、SafeWord、SecurID、Application、Anonymous、HTTP Basic、Membership、Unix、Certification、NT 與 RADIUS。Identity Server 還包含一個可用於加入其他認證服務的公用 SPI。若要定義新的服務，此欄位必須採用指定每個新認證服務之完整類別名稱 (包括套裝軟體名稱) 的文字字串。

用戶端支援的認證模組

此屬性指定特定用戶端支援的認證模組清單。格式如下所示：

```
clientType | module1,module2,module3
```

此屬性在啓用了用戶端偵測時有效。

LDAP 連線區大小

此屬性指定在特定伺服器與連接埠上使用的最小與最大連線區。此屬性僅用於 LDAP 與成員身份認證服務。格式如下所示：

```
host:port:min:max
```

注意 此連線區不同於 `serverconfig.xml` 中配置的 SDK 連線區。

LDAP 連線區預設大小

此屬性設定與所有 LDAP 認證模組配置一同使用的連線區預設最小值與最大值。如果 [LDAP 連線區大小] 屬性中存在主機與連接埠的項目，則不會使用 [LDAP 預設連線區大小] 中的最小與最大設定。

組織屬性

核心認證服務中的組織屬性包括：

- 組織認證模組
- 使用者設定檔
- 管理員認證者
- 使用者設定檔動態建立預設角色
- 永久性的 Cookie 模式
- 永久性的 Cookie 最大時間 (秒)
- 所有使用者的個人容器
- 別名搜尋屬性名稱
- 預設認證層級
- 使用者命名屬性
- 預設認證語言環境
- 組織認證配置
- 登入失敗鎖定模式
- 登入失敗鎖定計數
- 登入失敗鎖定間隔時間 (分鐘)
- 接收鎖定通知的電子郵件位址
- N 次失敗後警告使用者
- 登入失敗鎖定持續時間 (分鐘)
- 鎖定屬性名稱
- 鎖定屬性值
- 預設成功登入 URL
- 預設失敗登入 URL
- 認證處理後類別
- 使用者名稱產生器模式
- 可插接式使用者名稱產生器類別

組織認證模組

此清單指定組織可以使用的認證模組。每個管理員可爲每個特定組織選擇認證類型。雖然多重認證模組的使用很靈活，但是使用者必須確定其登入設定適用於選取的認證模組。預設認證模組爲 LDAP。Identity Server 含括的認證服務有：

- LDAP
- Cert
- Anonymous
- HTTP Basic
- Membership
- NT
- SafeWord
- RADIUS
- SecurID
- Unix

注意 若要使已建立的組織正常運作，管理員必須在該組織中建立並通知核心與認證模組範本。

使用者設定檔

此選項允許您爲使用者設定檔指定選項。

- 必需 - 此選項指定，對於成功認證，安裝有 Identity Server 的本機 Directory Server 中需要存在使用者設定檔，認證服務才會發行 SSOToken。
- 動態建立 - 此選項指定對於成功認證，如果尚不存在使用者設定檔，認證服務將建立一個使用者設定檔。然後將發行 SSOToken。使用者設定檔將在安裝有 Identity Server 的本機 Directory Server 中建立。
- 忽略 - 此選項指定對於成功認證，認證服務不需要使用者設定檔便可以發行 SSOToken。

管理員認證者

按一下 [編輯] 連結將允許您僅爲管理員定義認證服務。管理員是需要 Identity Server 主控台存取權限的使用者。如果需要管理員的認證模組與一般使用者的認證模組有所不同，則可以使用此屬性。此屬性中配置的模組將存取 Identity Server 主控台時被挑選。

使用者設定檔動態建立預設角色

如果在第 188 頁的「使用者設定檔」特性中選取了 [動態建立]，則此欄位指定被分配了新使用者的角色，且此新使用者的設定檔已建立。此欄位沒有預設值。管理員必須指定將分配給新使用者的角色之 DN。

注意 指定的角色必須位於正在為其配置認證的組織下。

永久性的 Cookie 模式

此選項確定使用者是否可以重新啓動瀏覽器，並且仍然返回至其經過認證的階段作業。可以透過啓用 [永久性的 Cookie 模式] 來保留使用者階段作業。啓用了 [永久性的 Cookie 模式] 時，使用者階段作業在其永久性的 Cookie 過期或者該使用者明確登出後才會過期。過期時間在 [永久性的 Cookie 最大時間 (秒)] 中指定。預設值是不啓用 [永久性的 Cookie 模式]，並且認證服務僅使用記憶體 Cookie。

注意 用戶端必須使用登入 URL 中的 `iPSPCookie=yes` 參數，明確請求永久性的 Cookie。

永久性的 Cookie 最大時間 (秒)

此欄位指定永久性的 Cookie 多長時間後會過期。(必須透過選取 [永久性的 Cookie 模式] 的核取方塊來啓用它。) 這一間隔時間在成功認證使用者階段作業後開始。預設值爲 `2147483` (時間以秒計算)。此欄位可以是 `0` 與 `2147483` 之間的任何整數值。

所有使用者的個人容器

使用者成功認證後，將擷取其設定檔。此欄位中的值指定搜尋設定檔的位置。通常，此值將爲預設個人容器的 DN。加入至組織的所有使用者項目會自動被加入至組織的預設個人容器。預設值爲 `ou=People`，通常使用組織名稱與根字尾組成此值。此欄位可以接受任何組織單元的有效 DN。

注意 認證透過以下方法搜尋使用者設定檔：

- 在預設個人容器下搜尋，然後
- 在預設組織下搜尋，然後
- 使用 [別名搜尋屬性名稱] 屬性搜尋預設組織中的使用者。

最後一種搜尋適用於 SSO 情形，此時用於認證的使用者名稱可能不是設定檔中的命名屬性。例如，使用者可以使用 `jn10191` 的 Safeword ID 認證，但是設定檔為 `uid=jamie`。

別名搜尋屬性名稱

使用者成功認證後，將擷取其設定檔。如果依據第 190 頁的「使用者命名屬性」中指定的首選 LDAP 屬性執行的搜尋，無法找到相符的使用者設定檔，則此欄位會指定另一個要從中搜尋的 LDAP 屬性。此屬性將主要在從認證模組傳回的使用者識別不同於 [使用者命名屬性] 中指定的識別時使用。例如，RADIUS 伺服器可能會傳回 `abc1234`，但是使用者名稱卻爲 `abc`。此屬性沒有預設值。此欄位將接受任何有效的 LDAP 屬性 (例如，`cn`)。

使用者命名屬性

使用者成功認證後，將擷取其設定檔。此屬性的值指定要用於搜尋的 LDAP 屬性。依預設，Identity Server 將假定使用者項目是由 `uid` 屬性識別的。如果 Directory Server 使用的是其他屬性 (例如 `givenname`)，請在此欄位中指定屬性名稱。

預設認證語言環境

此欄位指定認證服務要使用的預設語言子類型。預設值爲 en_US。在表 19-1 中可找到有效語言子類型的清單。

為了使用其他語言環境，必須首先建立此語言環境的所有認證範本。然後必須為這些範本建立新目錄。請參閱「*Sun ONE Identity Server Customization and API Guide*」中的「Chapter 3: Authentication Service」，以取得更多資訊。

表 19-1 支援的語言環境

語言標籤	語言
af	南非荷蘭文
be	白俄羅斯文
bg	保加利亞文
ca	加泰蘭文
cs	捷克文
da	丹麥文
de	德文
el	希臘文
en	英文
es	西班牙文
eu	巴斯克文
fi	芬蘭文
fo	法洛文
fr	法文
ga	愛爾蘭文
gl	加里西亞文
hr	克羅埃西亞文
hu	匈牙利文
id	印尼文
is	冰島文
it	義大利文
ja	日文

表 19-1 支援的語言環境 (續)

語言標籤	語言
ko	韓國文
nl	荷蘭文
no	挪威文
pl	波蘭文
pt	葡萄牙文
ro	羅馬尼亞文
ru	俄文
sk	斯洛伐克文
sl	斯洛維尼亞文
sq	阿爾巴尼亞文
sr	瑟比雅文
sv	瑞典文
tr	土耳其文
uk	烏克蘭文
zh	中文

組織認證配置

此屬性設定組織的認證模組。預設認證模組爲 LDAP。可以透過按一下 [編輯] 連結，選取一個或多個認證模組。如果選取了多個模組，則使用者必須通過所有選取模組的鏈接。

當使用者使用 `/server_deploy_uri/UL/Login` 格式存取認證模組時，將使用在此屬性中配置的模組進行認證。請參閱「Sun ONE Identity Server Customization and API Guide」，以取得更多資訊。

登入失敗鎖定模式

此功能指定使用者在首次認證嘗試失敗後是否可以再次嘗試。選取此屬性會啓用鎖定，使用者僅有一次認證的機會。依預設，鎖定功能是停用的。此屬性同與鎖定相關的屬性以及通知屬性配合使用。

登入失敗鎖定計數

此屬性定義在 [登入失敗鎖定間隔時間 (分鐘)] 所定義的時間間隔內，使用者在鎖定之前可以嘗試進行認證的次數。

登入失敗鎖定間隔時間 (分鐘)

此屬性定義兩次登入嘗試失敗之間的時間 (以分鍾爲單位)。如果某次登入失敗，並且在鎖定間隔時間內再次登入失敗，則增加鎖定計數。否則重設鎖定計數。

接收鎖定通知的電子郵件位址

此屬性指定將接收使用者鎖定通知的電子郵件位址。若要將電子郵件通知傳送至多重位址，請使用空格分隔每個電子郵件位址。

N 次失敗後警告使用者

此屬性指定在 Identity Server 傳送使用者將被鎖定的警告訊息之前，可以發生的認證失敗次數。

登入失敗鎖定持續時間 (分鐘)

此屬性啓用記憶體鎖定。依預設，鎖定機制將使 [鎖定屬性名稱] 中定義的 [使用者設定檔] 處於非作用中 (登入失敗後)。如果 [登入失敗鎖定持續時間] 的值大於 0，則其記憶體鎖定和使用者帳戶將被鎖定一段指定的時間 (分鐘)。

鎖定屬性名稱

此屬性指定要被設定爲鎖定的所有 LDAP 屬性。還必須變更 [鎖定屬性值] 中的值以啓用此屬性名稱的鎖定。依預設，Identity Server 主控台中的 [鎖定屬性名稱] 爲空。當使用者被鎖定且 [登入失敗鎖定持續時間] 設定爲 0 時，預設實施值爲 `inetuserstatus` (LDAP 屬性) 和 `inactive`。

鎖定屬性值

此屬性指定啓用還是停用 [鎖定屬性名稱] 中定義之屬性的鎖定。依預設，`inetuserstatus` 的值設定爲 0。

預設成功登入 URL

此欄位指定認證成功後使用者將重新導向至的 URL。此欄位可以接受任何有效的 URL。成功登入 URL 在 `remote-auth.dtd` 的 `LoginStatus` 元素中設定。請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得更多資訊。

預設失敗登入 URL

此欄位指定認證失敗後使用者將重新導向至的 URL。此欄位可以接受任何有效的 URL。`remote-auth.dtd` 的 `LoginStatus` 元素中設定了失敗登入 URL。請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得更多資訊。

認證處理後類別

此欄位指定 Java 類別名稱，用於自訂登入成功或失敗的認證後程序。例如：

```
com.abc.authentication.PostProcessClass
```

Java 類別必須實施以下 Java 介面：

`com.sun.identity.authentication.spi.AMPostAuthProcessInterface`

此外，您必須將此類別所在位置的路徑加入到 Web Server 的 [Java 類別路徑] 屬性中。

使用者名稱產生器模式

成員身份認證模組使用此屬性。如果啓用了此屬性欄位，則成員身份模組能夠在自行註冊過程中，產生特定使用者的多個使用者 ID (如果使用者 ID 已經存在)。這些使用者 ID 是從可插接式使用者名稱產生器類別中指定的 Java 類別產生的。

可插接式使用者名稱產生器類別

此欄位指定啓用了 [使用者名稱產生器模式] 時，用來產生使用者 ID 的 Java 類別之名稱。

預設認證層級

認證層級值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，該應用程式可以使用儲存的值以確定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。

應該在組織的特定認證範本內部設定認證層級。僅當在 [認證層級] 欄位中尚未指定特定組織認證範本的任何認證層級時，此處描述的 [預設認證層級] 值才適用。[預設認證層級] 預設值爲 0。(Identity Server 並不使用此屬性中的值，而是由可以選擇使用它的任何外部應用程式使用。)

第 20 章

HTTP Basic 認證屬性

HTTP Basic 認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲 HTTP Basic 認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊後組織的管理員可以變更預設值。組織屬性不會由組織中的項目繼承。

HTTP Basic 認證屬性包括：

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式會使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 0。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 21 章

LDAP 認證屬性

LDAP 認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲 LDAP 認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊之後組織的管理員可以變更預設值。組織屬性不會由組織中的項目繼承。LDAP 認證屬性包括：

- 主 LDAP 伺服器與連接埠
- 次 LDAP 伺服器與連接埠
- 開始使用者搜尋的 DN
- 超級使用者連結 DN
- 超級使用者連結密碼
- 超級使用者連結密碼 (確認)
- 使用者命名屬性
- 使用者項目搜尋屬性
- 使用者搜尋過濾
- 搜尋範圍
- 對 LDAP 伺服器啓用 SSL
- 將使用者 DN 傳回認證
- LDAP 伺服器檢查間隔時間
- 使用者建立屬性清單
- 認證層級

主 LDAP 伺服器與連接埠

此欄位指定在安裝 Identity Server 期間指定的主 LDAP 伺服器之主機名稱與連接埠號。這是 LDAP 認證所聯絡的首選伺服器。格式爲 `hostname:port`。(如果沒有連接埠號，則假定爲 `389`。)

如果您使用多重網域部署 Identity Server，則可按以下格式 (多重項目必須以本機伺服器名稱爲字首) 指定 Identity Server 和 Directory Server 之間特定實例的通訊連結：

```
local_servername|server:port local_servername2|server:port ...
```

例如，若要將兩個 Identity Server 部署在與不同的 Identity Server 實例 (`L1-machine1-DS` 和 `L2-machine2-DS`) 通訊的不同位置 (`L1-machine1-IS` 和 `L2-machine2-IS`) 中，則如下所示：

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

次 LDAP 伺服器與連接埠

此欄位指定 Identity Server 平台上可用的次 LDAP 伺服器之主機名稱與連接埠號。如果主 LDAP 伺服器未對認證請求進行回應，則會聯絡此次伺服器。如果主伺服器開啓，則 Identity Server 將切換回此主伺服器。格式也爲 `hostname:port`。多重項目必須以本機伺服器名稱作爲字首。

警告 認證位於 Identity Server 企業遠端的 Directory Server 使用者時，請務必使主/次 LDAP 伺服器連接埠均有值。兩個欄位可以使用一個 Directory Server 位置的值。

開始使用者搜尋的 DN

此欄位指定使用者搜尋起始處的節點 DN。(出於效能原因，此 DN 應該儘可能明確。) 預設值是目錄樹的根。將識別任何有效 DN。多重項目必須以本機伺服器名稱作爲字首。格式如下：

```
servername|search dn
```

對於多重項目

`servername1|search dn servername2|search dn servername3|search dn...`

如果同一次搜尋找到多個使用者，則認證將失敗。

超級使用者連結 DN

此欄位指定使用者的 DN，該使用者將用來作爲管理員連結至 [主 LDAP 伺服器與連接埠] 欄位中指定的 Directory Server。認證服務需要以此 DN 連結，以便基於使用者登入 ID 搜尋相符的使用者 DN。預設值爲 `amldapuser`。將識別任何有效 DN。

登出前請確保密碼正確，因爲如果密碼不正確，您將被鎖定。如果您被鎖定，可使用 `AMConfig.Properties` 檔案之 `com.iplanet.authentication.super.user` 屬性中的超級使用者 DN 登入。雖然您可以使用完整的 DN，但依預設這才是您通常用來登入的 amAdmin 帳戶。例如：

`uid_amAdmin,ou=People,`*`IdentityServer_base`*

超級使用者連結密碼

此欄位中爲在 [超級使用者連結 DN] 欄位中指定的管理員設定檔的密碼。此欄位沒有預設值。僅會識別管理員的有效 LDAP 密碼。

超級使用者連結密碼 (確認)

對此密碼的確認。

使用者命名屬性

使用者成功認證後，其設定檔會被擷取。此屬性的值用於執行搜尋。此欄位指定要使用的 [LDAP] 屬性。依預設，Identity Server 會假定使用者項目是由 `uid` 屬性識別的。如果 Directory Server 使用的是其他屬性 (例如 `givenname`)，請在此欄位中指定屬性名稱。

注意 使用者搜尋過濾將是 [搜尋過濾] 屬性與 [使用者項目命名] 屬性的組合。

使用者項目搜尋屬性

此欄位列出了用於爲要認證的使用者形成搜尋過濾的屬性，並且允許使用者使用使用者的項目中多個屬性進行認證。例如，如果此欄位設定爲 `uid`、`employeenumber` 和 `mail`，則使用者可以使用其中任一名稱進行認證。

使用者搜尋過濾

此欄位指定一個屬性，用於在 [開始使用者搜尋的 DN] 欄位下尋找使用者。它與 [使用者項目命名] 屬性配合使用。此欄位沒有預設值。將會辨識任何有效的使用者項目屬性。

搜尋範圍

此功能表指示 Directory Server 中將於其中搜尋相符使用者設定檔的層級數。搜尋從第 200 頁的「開始使用者搜尋的 DN」屬性中指定的節點開始。預設值爲 `SUBTREE`。可以從清單中選取以下其中一個選項：

- OBJECT - 僅搜尋指定的節點
- ONELEVEL - 搜尋指定節點的層級以及下一個層級
- SUBTREE - 搜尋指定的節點及以下的所有項目

警告 即使子組織的狀態處於非作用中，子組織的使用者也可登入。為了避免這種情況，請確保將 [搜尋範圍] 和 [基準 DN] 設定為此使用者所屬的特定組織。

對 LDAP 伺服器啟用 SSL

此選項對在 [主/次 LDAP 伺服器與連接埠] 欄位中指定的 Directory Server 啓用 SSL 存取。依預設，不啓用 SSL 存取，且不使用 SSL 協定存取 Directory Server。但是，如果啓用了此屬性，則可以連結至非 SSL 伺服器。

將使用者 DN 傳回認證

Identity Server 目錄與爲 LDAP 配置的目錄相同時，則可能啓用了此選項。如果啓用了此選項，則允許 LDAP 認證模組傳回 DN，而不是 `userId`，並且不必進行任何搜尋。通常，認證模組僅傳回 `userId`，並且認證服務會搜尋本機 Identity Server LDAP 中的使用者。如果使用外部 LDAP 目錄，則通常不啓用此選項。

LDAP 伺服器檢查間隔時間

此屬性用於 LDAP 伺服器故障修復。它定義驗證該 LDAP 主伺服器正在執行前，執行緒將「休息」的秒數。

使用者建立屬性清單

此屬性在 LDAP 伺服器被配置爲外部 LDAP 伺服器時，由 LDAP 認證模組使用。它包含本機 Directory Server 和外部 Directory Server 之間的屬性對映。此屬性具有以下格式：

```
attr1|externalattr1
attr2|externalattr2
```

植入此屬性後，會從外部 Directory Server 讀取外部屬性的值，並將之設定爲內部 Directory Server 屬性。僅當 [使用者設定檔] 屬性 (在核心認證模組中) 設定爲「動態建立」，並且本機 Directory Server 實例中不存在使用者時，才在內部屬性中設定外部屬性的值。新建立的使用者將包含內部屬性的值 (如使用者建立屬性清單中所指定) 及它們對映的外部屬性的值。

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式會使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 `0`。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 22 章

成員身份認證屬性

成員身份認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲成員身份認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊之後組織的管理員可以變更預設值。組織屬性不會由組織子樹中的項目繼承。成員身份認證屬性包括：

- 最小密碼長度
- 預設使用者角色
- 註冊後的使用者狀態
- 主 LDAP 伺服器與連接埠
- 次 LDAP 伺服器與連接埠
- 開始使用者搜尋的 DN
- 超級使用者連結 DN
- 超級使用者連結密碼
- 超級使用者連結密碼 (確認)
- 使用者命名屬性
- 使用者項目搜尋屬性
- 使用者搜尋過濾
- 搜尋範圍
- 對 LDAP 伺服器啓用 SSL
- 將使用者 DN 傳回認證
- 認證層級

最小密碼長度

此欄位指定在自行註冊過程中設定密碼時所需的最小字元數。預設值爲 8。

如果變更此值，則也應該在註冊中以及以下檔案的錯誤文字中進行變更：

IdentitySever_base/locale/amAuthMembership.properties (PasswdMinChars *entry)*

預設使用者角色

此欄位指定分配給新使用者的角色，該使用者的設定檔透過自行註冊建立。此欄位沒有預設值。管理員必須指定將分配給新使用者的角色之 DN。

注意 指定的角色必須位於正在為其配置認證的組織下。自行註冊期間僅加入可以指定給使用者的角色。所有其他 DN 均會被忽略。

註冊後的使用者狀態

此功能表指定服務是否立即可以供已自行註冊的使用者使用。預設值爲 Active，新使用者可以使用服務。透過選取 Inactive，管理員選擇不向新使用者提供服務。

主 LDAP 伺服器與連接埠

此欄位指定在安裝 Identity Server 期間所指定主 LDAP 伺服器之主機名稱與連接埠號。這是 LDAP 認證所聯絡的首選伺服器。格式爲 hostname:port。(如果沒有連接埠號，則假定爲 389。)

如果您使用多重網域部署 Identity Server，則可按以下格式 (多重項目必須以本機伺服器名稱爲字首) 指定 Identity Server 和 Directory Server 之間特定實例的通訊連結：

```
local_servername|server:port local_servername2|server:port ...
```

例如，若要將兩個 Identity Server 部署在與不同的 Identity Server 實例 (L1-machine1-DS 和 L2-machine2-DS) 通訊的不同位置 (L1-machine1-IS 和 L2-machine2-IS) 中，則如下所示：

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

次 LDAP 伺服器與連接埠

此欄位指定 Identity Server 平台上可用的次 LDAP 伺服器之主機名稱與連接埠號。如果主 LDAP 伺服器未回應認證請求，則聯絡該次伺服器。如果主伺服器開啓，則 Identity Server 將切換回此主伺服器。格式也爲 `hostname:port`。多重項目必須以本機伺服器名稱爲字首。

警告 認證位於 Identity Server 企業遠端的 Directory Server 使用者時，請務必使主/次 LDAP 伺服器連接埠均有值。兩個欄位可使用一個 Directory Server 位置的值。

開始使用者搜尋的 DN

此欄位指定使用者搜尋起始處的節點 DN。(出於效能原因，此 DN 應該儘可能明確。) 預設值是目錄樹的根。將識別任何有效 DN。如果使用多重項目，則這些項目必須以本機伺服器名稱爲字首。

注意 如果有多重使用者與同一個搜尋相符，認證將會失敗。

超級使用者連結 DN

此欄位指定使用者的 DN，該使用者將用來作爲管理員連結至 [主 LDAP 伺服器與連接埠] 欄位中指定的 Directory Server。認證服務需要以此 DN 連結，以便基於使用者登入 ID 搜尋相符的使用者 DN。預設值爲 `amldapuser`。將識別任何有效 DN。

超級使用者連結密碼

此欄位中爲在 [超級使用者連結 DN] 欄位中指定的管理員設定檔的密碼。此欄位沒有預設值。僅會識別管理員的有效 LDAP 密碼。

超級使用者連結密碼 (確認)

對此密碼的確認。

使用者命名屬性

此欄位指定用於使用者項目命名慣例的屬性。依預設，Identity Server 會假定使用者項目是由 `uid` 屬性識別的。如果 Directory Server 使用的是其他屬性 (例如 `givenname`)，請在此欄位中指定屬性名稱。

使用者項目搜尋屬性

此欄位列出了用於爲要認證的使用者形成搜尋過濾的屬性，並且允許使用者使用使用者的項目中多個屬性進行認證。例如，如果此欄位設定爲 `uid`、`employeenumber` 和 `mail`，則使用者可以使用其中任一名稱進行認證。

使用者搜尋過濾

此欄位指定一個屬性，用於在 [開始使用者搜尋的 DN] 欄位下尋找使用者。它與 [使用者命名屬性] 配合使用。此欄位沒有預設值。將會辨識任何有效的使用者項目屬性。

搜尋範圍

此功能表指示 Directory Server 中將於其中搜尋相符使用者設定檔的層級數。搜尋從第 207 頁的「開始使用者搜尋的 DN」屬性中指定的節點開始。預設值爲 `SUBTREE`。可以從清單中選取以下其中一個選項：

- OBJECT — 僅搜尋指定的節點
- ONELEVEL — 在指定節點的層級以及下一層級搜尋
- SUBTREE — 搜尋指定的節點及以下的所有項目

對 LDAP 伺服器啟用 SSL

此選項對在 [主/次 LDAP 伺服器與連接埠] 欄位中指定的 Directory Server 啓用 SSL 存取。依預設不會核取此方塊，將不使用 SSL 協定存取 Directory Server。

將使用者 DN 傳回認證

Identity Server 目錄與爲 LDAP 配置的目錄相同時，則可能啓用了此選項。如果啓用了此選項，則允許 LDAP 認證模組傳回 DN，而不是 `userId`，並且不必進行任何搜尋。通常，認證模組僅傳回 `userId`，並且認證服務會搜尋本機 Identity Server LDAP 中的使用者。如果使用外部 LDAP 目錄，則通常不啓用此選項。

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式將使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 `0`。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 23 章

NT 認證屬性

NT 認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲 NT 認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊之後組織的管理員可以變更預設值。組織屬性不會由組織子樹中的項目繼承。

NT 認證僅在 Identity Server 的 Solaris 版本上受支援。爲了實現 NT 認證模組，必須下載並安裝 Samba Client 2.2.2。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。

NT 認證屬性包括：

- NT 認證網域
- NT 認證主機
- 認證層級

NT 認證網域

此屬性定義使用者所屬的網域名稱。

NT 認證主機

此屬性定義 NT 認證主機名稱。主機名稱應爲 netBIOS 名稱，與完整網域名稱 (FQDN) 相對。依預設，FQDN 的第一部分爲 netBIOS 名稱。

如果使用 DHCP (動態主機配置協定)，則會在 Windows 2000 機器上將相符的項目放入 HOSTS 檔案。

將基於 netBIOS 名稱執行名稱解析。如果子網路上沒有任何提供 netBIOS 名稱解析的伺服器，則對映應爲硬碼式的。

例如，主機名稱應爲 `example1`，而不是 `example1.company1.com`。

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式會使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 `0`。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 24 章

RADIUS 認證屬性

RADIUS 認證屬性是組織屬性。在服務配置下套用於這些屬性的值會成爲 RADIUS 認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊後組織的管理員可以變更預設值。組織屬性不會由組織中的項目繼承。RADIUS 認證屬性包括：

- RADIUS 伺服器 1
- RADIUS 伺服器 2
- RADIUS 共用密碼
- RADIUS 共用密碼 (確認)
- RADIUS 伺服器的連接埠
- 逾時 (秒)
- 認證層級

RADIUS 伺服器 1

此欄位顯示主 RADIUS 伺服器的 IP 位址或完整主機名稱。預設 IP 位址爲 `127.0.0.1`。此欄位會辨識任何有效的 IP 位址或主機名稱。多重項目必須以本機伺服器名稱作爲字首，如以下語法中所示：

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS 伺服器 2

此欄位顯示輔助 RADIUS 伺服器的 IP 位址或完整領域名稱 (FQDN)。此伺服器是在無法聯絡主伺服器時，將會聯絡的錯誤修復伺服器。預設 IP 位址爲 `127.0.0.1`。多重項目必須以本機伺服器名稱作爲字首，如以下語法中所示：

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS 共用密碼

此欄位中爲 RADIUS 認證的共用密碼。共用密碼應該與相適的密碼具有相同的權限。此欄位沒有預設值。

RADIUS 共用密碼 (確認)

對 RADIUS 認證的共用密碼進行確認。

RADIUS 伺服器的連接埠

此欄位指定 RADIUS 伺服器正在偵聽的連接埠。預設值爲 `1645`。

注意 如果未指定任何認證層級，則 SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

逾時 (秒)

此欄位指定在逾時之前等待 RADIUS 伺服器回應的時間間隔 (以秒計算)。預設值爲 3 秒。此欄位將辨識指定逾時 (以秒計算) 的任何數字。

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式將使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 0。

注意 如果未指定任何認證層級，則 SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 24 章

SafeWord 認證屬性

SafeWord 認證屬性爲組織屬性。在服務配置下套用於這些屬性的值將成爲 SafeWord 認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊後組織的管理員可以變更預設值。組織屬性不會由組織子樹中的項目繼承。

此服務允許使用 Secure Computing 的 SafeWord 或 SafeWord PremierAccess 認證伺服器對使用者進行認證。SafeWord 認證屬性包括：

- SafeWord 伺服器規格
- SafeWord 系統名稱
- SafeWord 伺服器驗證檔案路徑
- SafeWord 記錄層級
- SafeWord 日誌路徑
- 認證層級

SafeWord 伺服器規格

此欄位指定 SafeWord 或 SafeWord PremiereAccess 伺服器名稱與連接埠。連接埠 7482 設定爲 SafeWord 伺服器的預設值。SafeWord PremierAccess 伺服器的預設連接埠號爲 5030。

SafeWord 系統名稱

此欄位指定在 SafeWord 伺服器中配置的系統名稱。預設系統名稱爲 STANDARD。

SafeWord 伺服器驗證檔案路徑

此欄位指定 SafeWord 用戶端程式庫存放其驗證檔案的目錄。預設路徑如下所示：

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

如果在此欄位中指定了不同目錄，則在嘗試 SafeWord 認證之前必須確保此目錄存在。

SafeWord 記錄層級

不使用此屬性。

SafeWord 日誌路徑

此屬性指定 SafeWord 用戶端記錄的目錄路徑與日誌檔名稱。預設路徑如下所示：

```
/var/opt/SUNWam/auth/safeword/safe.log
```

如果指定了不同路徑或檔案名稱，則在嘗試 SafeWord 認證之前必須確保其存在。

如果爲 SafeWord 認證配置了多個組織，並且使用不同的 SafeWord 伺服器，則必須指定不同的路徑，否則只有進行 SafeWord 認證的第一個組織才能使用。同樣，如果組織變更了 SafeWord 伺服器，則必須刪除指定目錄中的 swec.dat 檔案，新配置的 SafeWord 伺服器認證才能生效。

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式將使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 0。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 25 章

SecurID 認證屬性

SecurID 認證屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲 SecurID 認證範本的預設值。組織註冊服務後，需要建立服務範本。註冊後組織的管理員可以變更預設值。組織屬性不會由組織子樹中的項目繼承。

此服務允許使用 RSA ACE/Server 認證伺服器對使用者進行認證。SecurID 認證屬性包括：

- SecurID ACE/Server 配置路徑
- SecurID 輔助程式配置連接埠
- SecurID 輔助程式認證連接埠
- 認證層級

注意 在 Identity Server 6.1 中，x86 作業系統不支援 SecurID 認證服務。

SecurID ACE/Server 配置路徑

此欄位指定 SecurID ACE/Server `sdconf.rec` 檔案所在的目錄。預設路徑如下所示：

```
/opt/ace/data
```

如果在此欄位中指定了不同目錄，則在嘗試 SecurID 認證之前必須確保此目錄存在。

SecurID 輔助程式配置連接埠

此屬性指定 SecurID 輔助程式啓動時「偵聽」的連接埠，以取得 [SecurID 輔助程式認證連接埠] 屬性中包含的配置資訊。預設值爲 58943。

如果變更了此屬性，則必須同時變更 `AMConfig.properties` 檔案中的 `securidHelper.ports` 項目，然後重新啓動 Identity Server。`AMConfig.properties` 檔案中的項目是 SecurID 輔助程式實例偵聽的連接埠之清單 (以空格分隔)。對於每個與不同 ACE/Server (具有不同的 `sdconf.rec` 檔案) 通訊的組織來說，必須具有單獨的 SecurID 輔助程式。

SecurID 輔助程式認證連接埠

此屬性指定組織 SecurID 認證模組將配置其 SecurID 輔助程式實例進行「偵聽」的連接埠，以取得認證請求。此連接埠號在使用 SecurID 或 Unix 認證的所有組織中均必須是唯一的。預設連接埠爲 57943。

認證層級

會分別爲各種認證方法設定認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式將使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 `0`。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 26 章

Unix 認證屬性

Unix 認證服務由全域屬性與組織屬性組成。套用於全域屬性的值也套用於整個 Sun ONE Identity Server 配置，並由每個配置的組織繼承。由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。套用於組織屬性的值是每個配置組織的預設值，並且在向組織註冊此服務時可以變更。組織屬性不會由組織項目來繼承。Unix 認證屬性分爲：

- 全域屬性
- 組織屬性

注意 Windows 2000 平台不支援 Unix 認證服務。

全域屬性

Unix 認證服務中的全域屬性包括：

- Unix 輔助程式配置連接埠
- Unix 輔助程式認證連接埠
- Unix 輔助程式逾時 (分鐘)
- Unix 輔助程式執行緒

Unix 輔助程式配置連接埠

此屬性指定 Unix 輔助程式啓動時「偵聽」的連接埠，以取得 [Unix 輔助程式認證連接埠]、[Unix 輔助程式逾時 (分鐘)] 和 [Unix 輔助程式執行緒] 屬性中包含的配置資訊。預設值爲 58946。

如果變更了此屬性，則必須同時變更 `AMConfig.properties` 檔案中的 `unixHelper.port` 項目，然後重新啓動 Identity Server。

Unix 輔助程式認證連接埠

此屬性指定 Unix 輔助程式「偵聽」的連接埠，以取得配置後的認證請求。預設連接埠爲 57946。

Unix 輔助程式逾時 (分鐘)

此屬性指定使用者必須完成認證所用的時間 (分鐘)。如果使用者認證超過分配的時間，則認證將自動失敗。預設時間設定爲 3 分鐘。

Unix 輔助程式執行緒

此屬性指定允許同時進行 Unix 認證階段作業的最大數目。如果在給定時間達到最大數目，則只有釋放某個階段作業後才允許進行後續認證嘗試。預設值設定爲 5。

組織屬性

Unix 認證服務的組織屬性爲：

認證層級

會分別爲各種認證方法設定認證層級。會分別爲各種認證方法設定值和認證層級。此值指示信任認證的程度。使用者進行認證後，此值便會儲存在階段作業的 SSO 記號中。SSO 記號呈現給使用者要存取的應用程式時，應用程式將使用此儲存值以決定此層級是否達到了允許使用者存取的層級。如果儲存在 SSO 記號中的認證層級不滿足最小值需求，應用程式可以提示使用者透過具有較高認證層級的服務重新進行認證。預設值爲 0。

注意 如果未指定任何認證層級，SSO 記號會將 [核心認證] 屬性中指定的值儲存為預設認證層級。請參閱第 195 頁的「預設認證層級」，以取得詳細資訊。

第 27 章

認證配置服務屬性

認證配置服務屬性爲動態的組織屬性。可以爲組織、服務或角色定義這些屬性。核心認證模組中定義組織屬性。

如果角色指定給使用者或者使用者指定給組織，依預設，這些屬性將由此使用者繼承。認證配置屬性包括：

- 認證配置
- 登入成功 URL
- 登入失敗 URL
- 認證處理後類別

認證配置

按一下 [編輯] 連結將顯示 [認證配置] 介面。該介面允許您配置基於角色認證或組織認證的認證模組。

下表列出了認證模組配置選項：

模組名稱	允許您從 Identity Server 可以使用的預設認證模組清單中選取。
旗標	此下拉式功能表允許您指定認證模組要求。可以為以下一種選項： • REQUIRED - 要求認證模組必須成功。無論成功或失敗，都將繼續認證清單中的下一個認證模組。 • REQUISITE - 要求認證模組必須成功。如果成功，會繼續認證清單中的下一個認證模組。如果失敗，會將控制權傳回應用程式 (不會繼續認證清單中的下一個認證模組)。 • SUFFICIENT - 不要求認證模組一定成功。如果成功，會將控制權立即傳回應用程式 (不會繼續認證清單中的下一個認證模組)。如果失敗，會繼續認證清單中的下一個認證模組。 • OPTIONAL - 不要求認證模組一定成功。無論成功或失敗，都將繼續認證清單中的下一個認證模組。 這些旗標為定義了這些旗標的認證模組建立了執行標準。執行的階層結構中，REQURIED 為最高層級，OPTION 為最低層級。 例如，如果管理員使用 REQUIRED 旗標定義 LDAP 模組，則使用者的憑證必須通過 LDAP 認證要求，才能存取給定資源。 如果您加入多重認證模組，並且每個模組的旗標設定為 REQUIRED，則使用者必須通過所有認證要求，才能取得存取權限。 如需有關旗標定義的更多資訊，請參考 JAAS (Java 認證與授權服務)，位於： `http://java.sun.com/security/jaas/doc/module.html`
選項	允許此模組的其他選項為鍵值 = 值對。多重選項由空格分隔。

登入成功 URL

此屬性指定使用者認證成功後將重新導向至的 URL。

登入失敗 URL

此屬性指定使用者認證失敗後將重新導向至的 URL。

認證處理後類別

此屬性定義在登入成功或失敗後用來自訂認證後程序的 Java 類別名稱。

衝突解決層級

此屬性僅套用於角色。[衝突解決層級] 爲可能包含相同使用者的角色設定認證配置屬性的優先層級。例如，如果使用者 1 同時指定給角色 1 與角色 2，您可以爲角色 1 定義較高的優先層級，從而當使用者嘗試認證時，無論對於成功或失敗後重新導向還是對於認證後程序，角色 1 都將具有最高的優先層級。

第 28 章

用戶端偵測服務屬性

用戶端偵測服務屬性爲全域屬性。套用於這些屬性的值也套用於整個 Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。) 用戶端偵測屬性包括：

- 用戶端類型
- 預設用戶端類型
- 用戶端偵測類別
- 啓用用戶端偵測

用戶端類型

爲了偵測用戶端類型，Identity Server 需要識別它們的識別特徵。這些特徵可識別用戶端資料格式的所有支援類型的屬性。此屬性可讓您透過 [用戶端管理員] 介面修改用戶端資料。若要存取 [用戶端管理員]，請按一下 [編輯] 連結。

依預設，可用於基於 HTML 的瀏覽器的唯一配置的 Identity Server 用戶端資料被定義爲總綱目 genericHTML 及其父系 HTML 的子配置。

用戶端管理員

[用戶端管理員] 爲列出基本用戶端、樣式和關聯屬性的介面，它可讓您加入和配置裝置。

基本用戶端類型

基本用戶端類型在 [用戶端管理員] 頂部列出。這些用戶端類型包含屬於此用戶端類型的所有裝置可繼承的預設屬性。

樣式設定檔

[用戶端管理員] 在 [樣式] 下拉式功能表中將所有可用用戶端 (包括基本用戶端類型本身) 分組。所選 [樣式] (或父系設定檔) 定義其配置的子裝置共用的屬性。這些裝置動態地繼承父系設定檔的屬性

[目前樣式屬性] 連結啓動唯讀 [用戶端編輯程式] 視窗，以便檢視樣式屬性。

裝置設定檔

選取樣式後，[用戶端管理員] 會顯示爲此樣式配置的裝置設定檔。裝置按使用者代理程式 (裝置名稱) 排序，並可透過在 [過濾] 欄位 (接受萬用字元) 中輸入使用者代理程式字串來過濾。

對於每個裝置，您可以按一下每個裝置名稱旁邊的 [編輯] 連結來修改用戶端屬性。這些屬性則顯示在 [用戶端編輯程式] 視窗中。若要編輯這些屬性，請從下拉式清單中選取以下類別：

硬體平台。包含裝置的硬體屬性，如顯示大小、支援的字元集等。

軟體平台。包含裝置的應用程式環境的屬性、作業系統的屬性以及安裝軟體的屬性。

網路特徵。包含描述網路環境 (包括支援的載送程式) 的屬性。

BrowserUA。包含與在此裝置上執行的瀏覽器使用者代理程式相關的屬性。

WapCharacteristics。包含此裝置支援的無線應用程式協定 (WAP) 環境的屬性。

PushCharacteristicsNames。包含此裝置支援的 WAP 環境的屬性。

其他屬性。可讓您加入裝置的其他屬性。

對於特定的屬性定義，請參閱以下位置的 Open Mobile Alliance Ltd. (OMA) Wireless Application Protocol, Version 20-Oct-2001：

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

修改這些屬性之後，請按一下 [儲存]。裝置將顯示「**」字元來表示已將其自訂。可使用 [預設] 連結移除自定的屬性，並將裝置重設回預設設定。

若要爲某樣式加入新裝置，請按一下 [新增裝置] 按鈕。螢幕上會顯示 [建立新裝置] 視窗，該視窗具有以下欄位：

[樣式]。顯示裝置的基本樣式，例如 HTML。

[裝置使用者代理程式]。接受裝置的名稱。

按一下 [下一步] 顯示以下欄位：

[用戶端類型名稱]。顯示用戶端類型，例如 HTML。用戶端類型名稱在所有裝置中必須是唯一的。

[本裝置的直接父系]。接受裝置的父系 (基本) 用戶端類型。例如 HTML。

[HTTP 使用者代理程式字串]。定義 HTTP 請求標頭中的使用者代理程式。例如 Mozilla/4.0。

按一下 [確定] 並自訂裝置屬性。對於特定的屬性定義，請參閱以下位置的 Open Mobile Alliance Ltd. (OMA) Wireless Application Protocol, Version 20-Oct-2001：

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

若要複製裝置及其屬性，請按一下 [複製] 連結。裝置名稱必須唯一。依預設，Identity Server 會將此裝置重新命名爲 `copy_of_`*devicename*。

若要刪除任何裝置，請按一下與裝置一起列出的 [刪除] 連結。

預設用戶端類型

此屬性定義從 [用戶端類型] 屬性的用戶端類型清單中導出的預設用戶端類型。預設值爲 `genericHTML`。

用戶端偵測類別

此屬性定義路由所有用戶端偵測請求的用戶端偵測類別。此屬性傳回的字串應該與 [用戶端類型] 屬性中列出的某種用戶端類型相符。預設用戶端偵測類別爲 `com.iplanet.services.cdm.ClientDetectionDefaultImpl`。

啟用用戶端偵測

此屬性允許您啓用用戶端偵測。如果啓用 (選取) 了用戶端偵測，則會透過 [用戶端偵測類別] 屬性中指定的類別路由每個請求。

依預設，停用除 genericHTML 以外的所有用戶端類型的用戶端偵測功能。如果未選取此屬性，則 Identity Server 假定用戶端是 genericHTML，並可透過 HTML 瀏覽器存取。

第 29 章

全域設定服務屬性

全域設定服務屬性爲全域屬性。套用於這些屬性的值也套用於整個 Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。) 全域設定屬性包括：

- 受每種語言環境支援的字元集
- 字元集別名
- 自動產生的共用名稱格式

受每種語言環境支援的字元集

此屬性列出每種語言環境支援的字元集，指示語言環境與字元集之間的對映。格式如下所示：

`locale=`*localename*`|charset=charset1;charset2;charset3;...;charsetn`

您可以使用位於此屬性底端的按鈕，加入、編輯、複製和移除字元集。

字元集別名

此屬性列出將用於傳送回應的字碼集名稱 (對映至 IANA 名稱)。這些字碼集名稱不需要與 Java 字碼集名稱相符。目前存在一種雜湊表，可以將 Java 字元集對映至 IANA 字元集，反之亦然。此別名格式如下所示：

`mimeName=`*charset*`|javaName=`*charset*

例如：

```
mimeName=Shift_JIS|javaName=SJIS
```

這指示兩者代表同一字元集。

您可以使用位於此屬性底端的按鈕，加入、編輯、複製和移除字元集別名。

自動產生的共用名稱格式

此顯示選項允許您定義自動產生名稱的方式，以適應不同語言環境和字元集的名稱格式。預設語法如下 (請注意，定義中包含的逗號和 / 或空格將顯示在名稱格式中)：

```
en_us = {givenname} {initials} {sn}
```

例如，如果您希望以新的名稱格式，即以中文字元集顯示帶有 uid (11111) 的使用者 (User One)，請使用以下結構：

```
zh = {sn}{givenname}({uid})
```

顯示結果如下：

```
OneUser 11111
```

第 30 章

記錄服務屬性

記錄服務屬性爲全域屬性。套用於這些屬性的值也套用於整個 Sun ONE Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。) 記錄屬性包括：

- 最大日誌大小
- 歷史檔案數目
- 日誌位置
- 記錄類型
- 資料庫使用者名稱
- 資料庫使用者密碼
- 資料庫使用者密碼 (確認)
- 資料庫驅動程式名稱
- 可配置日誌欄位
- 日誌驗證時間
- 日誌簽名時間
- 安全記錄
- 最大記錄數
- 每個歸檔檔案的檔案數目
- 緩衝區大小
- 緩衝時間
- 啓用緩衝時間

最大日誌大小

此屬性指定 Identity Server 日誌檔最大大小的值 (以位元組爲單位)。預設值爲 1000000。

歷史檔案數目

此屬性的值與用於歷程分析而保留的備份日誌檔數目相等。依本機系統分割區與可用磁碟空間大小，可以輸入任何整數。預設值爲 3。

日誌位置

基於檔案的記錄功能需要可以儲存日誌檔的位置。此欄位接受該位置的完整目錄路徑。預設位置爲：

/var/opt/SUNWam/logs

如果正在使用非預設目錄，則正在執行 Identity Server 的使用者必須對此目錄具有寫入權限。

爲 DB (資料庫) 記錄 (如 Oracle 或 MySQL) 配置日誌位置時，日誌位置的某些部分區分大小寫。

例如，如果您記錄到 Oracle 資料庫，則日誌位置應該是：

jdbc:oracle:thin:@machine.domain:port:DBName

jdbc:oracle:thin 必須爲小寫。

注意 記錄屬性值中的任何變更均需要重新啟動 Identity Server 後才能生效。

記錄類型

此屬性允許您指定平面檔記錄的檔案或資料庫記錄的 DB。

資料庫使用者名稱

在 [記錄類型] 屬性設定爲 DB 時，此屬性接受將連接至資料庫的使用者名稱。

資料庫使用者密碼

[記錄類型] 屬性設定爲 DB 時，此屬性接受資料庫使用者密碼。

資料庫使用者密碼 (確認)

對資料庫密碼的確認。

資料庫驅動程式名稱

此屬性允許使用者指定將用於記錄實施類別的驅動程式。

可配置日誌欄位

此參數表示要記錄的欄位清單。依預設，會記錄以下欄位：

- Domain
- Hostname
- IPAddress
- LoggedBy
- Loglevel
- LoginID
- ModuleName

日誌驗證時間

此屬性設定伺服器爲偵測竄改而應該驗證日誌的頻率 (以秒計算)。預設時間爲 3600 秒。此參數僅適用於安全記錄。

日誌簽名時間

此參數設定要對記錄進行簽名的頻率 (以秒計算)。預設時間爲 900 秒。此參數僅適用於安全記錄。

安全記錄

此屬性指定是否啓用安全記錄。依預設，安全記錄是關閉的。啓用安全記錄後，可以偵測對安全日誌進行的未授權變更或竄改。

最大記錄數

此屬性設定 Java LogReader 介面傳回的最大記錄數，無論有多少記錄與讀取查詢相符。依預設，設定爲 500。記錄 API 的呼叫者可以透過 LogQuery 參數置換此屬性。

每個歸檔檔案的檔案數目

此屬性僅適用於安全記錄。它指定對於後續的安全記錄，何時需要歸檔日誌檔與鍵值儲存區、何時重新產生安全鍵值儲存區。預設爲每個記錄程式有五個檔案。

緩衝區大小

此屬性指定在傳送至記錄服務進行記錄前，日誌記錄要在記憶體中緩衝的最大數目。預設爲一條記錄。

緩衝時間

此屬性定義在傳送至記錄服務進行記錄前，日誌記錄要在記憶體中緩衝的時間。預設值爲 3600 秒。

啟用緩衝時間

選取此屬性，使之處於開啓狀態時，Identity Server 將設定日誌記錄要在記憶體中緩衝的時間限制。該時間會在 [緩衝時間] 屬性中設定。

第 31 章

命名服務屬性

命名服務屬性爲全域屬性。套用於這些屬性的值也套用於整個 Sun ONE Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。)

如果此平台執行多個 Identity Server，則命名服務允許用戶端尋找正確的服務 URL。找到命名 URL 後，命名服務將解碼使用者階段作業，並且動態使用此階段作業的參數取代協定、主機與連接埠。這樣可確保爲此服務傳回的 URL 用於在其上建有使用者階段作業的主機。命名屬性包括：

- 設定檔服務 URL
- 階段作業服務 URL
- 記錄服務 URL
- 策略服務 URL
- 認證服務 URL
- SAML Web 設定檔 /Artifact 服務 URL
- SAML SOAP 服務 URL
- SAML Web 設定檔 /POST 服務 URL
- SAML 假設管理程式服務 URL
- 聯合假設管理程式服務 URL
- 身份 SDK 服務 URL

設定檔服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/profileservice`

此語法允許基於特定的階段作業參數動態取代設定檔 URL。

階段作業服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/sessionservice`

此語法允許基於特定的階段作業參數動態取代階段作業 URL。

記錄服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/loggingservice`

此語法允許基於特定的階段作業參數動態取代記錄 URL。

策略服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/policyservice`

此語法允許基於特定的階段作業參數動態取代策略 URL。

認證服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/authservice`

此語法允許基於特定的階段作業參數動態取代認證 URL。

SAML Web 設定檔 /Artifact 服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*`Server_DEPLOY_URI`*`/SAMLAwareServlet`

此語法允許基於特定的階段作業參數動態取代 SAML Web 設定檔 /Artifact URL。

SAML SOAP 服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*`Server_DEPLOY_URI`*`/SAMLSOAPReceiver`

此語法允許基於特定的階段作業參數動態取代 SAML SOAP URL。

SAML Web 設定檔 /POST 服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*`Server_DEPLOY_URI`*`/SAMLPOSTProfileServlet`

此語法允許基於特定的階段作業參數動態取代 SAML Web 設定檔 /POST URL。

SAML 假設管理程式服務 URL

此欄位採用的值等於

`%protocol://%host:%port/`*`Server_DEPLOY_URI`*`/AssertionManagerServlet/AssertionManagerIF`

此語法允許基於特定的階段作業參數動態取代 SAML 假設管理程式服務 URL。

聯合假設管理程式服務 URL

此欄位採用的值等於

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssertionMana
gerIF
```

此語法允許基於特定的階段作業參數動態取代聯合假設管理程式服務 URL。

身份 SDK 服務 URL

此欄位採用的值等於

```
%protocol://%host:%port/amserver/UserManagementServlet/
```

此語法允許基於特定的階段作業參數動態取代身份 SDK 服務 URL。

第 32 章

密碼重設服務屬性

密碼重設服務屬性爲組織屬性。在服務配置下套用於這些屬性的值會成爲給定組織中密碼重設服務的預設值。組織屬性不會由組織子樹中的項目繼承。

密碼重設屬性包括：

- 使用者驗證
- 保密問題
- 搜尋過濾
- 基準 DN
- 連結 DN
- 連結密碼
- 密碼重設選項
- 密碼變更通知選項
- 啓用密碼重設
- 啓用個人問題
- 問題數目
- 密碼重設失敗鎖定計數
- 密碼重設失敗鎖定間隔時間 (分鐘)
- 接受鎖定通知的電子郵件位址
- N 次失敗後警告使用者

- 密碼重設失敗鎖定持續時間 (分鐘)
- 密碼重設失敗鎖定模式
- 密碼重設鎖定屬性名稱
- 密碼重設鎖定屬性值

使用者驗證

此屬性指定用於搜尋要重設密碼的使用者之值。

保密問題

此欄位允許您加入使用者可以用來重設其密碼的問題清單。若要加入問題，請在 [保密問題] 欄位中鍵入問題，然後按一下 [加入]。選取的問題將顯示在使用者的 [使用者設定檔] 頁面中。然後，使用者可以選取一個要重設密碼的問題。

如果選取了 [啓用個人問題] 屬性，使用者可以建立自己的問題。

搜尋過濾

此屬性指定用於尋找使用者項目的搜尋過濾。

基準 DN

此屬性指定使用者搜尋的起點 DN。如果未指定 DN，則會從組織 DN 開始搜尋。由於代理認證衝突，您不應該將 `cn=directorymanager` 用作基準 DN。

連結 DN

將此屬性值與連結密碼結合使用，以重設使用者密碼。

連結密碼

將此屬性值與連結 DN 結合使用，以重設使用者密碼。

密碼重設選項

此屬性決定重設密碼的類別名稱。預設類別名稱爲：

```
com.sun.identity.password.RandomPasswordGenerator
```

可以透過外掛程式自訂密碼重設類別，此類別需要由 `PasswordGenerator` 介面實施。請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得更多資訊。

密碼變更通知選項

此屬性決定密碼重設的使用者通知方法。預設類別名稱爲：

```
com.sun.identity.password.EmailPassword
```

可以透過外掛程式自訂密碼通知類別。類別需要由 `NotifyPassword` 介面實施。請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得更多資訊。

啟用密碼重設

選取此屬性會啓用密碼重設功能。

啟用個人問題

選取此屬性將允許使用者爲密碼重設建立特有的問題。

問題數目

此值指定要在密碼重設頁面中詢問的最大問題數目。

密碼重設失敗鎖定計數

此屬性定義在 [密碼重設失敗鎖定間隔時間] 中定義的時間間隔內，使用者在被鎖定之前可以嘗試重設密碼的次數。

例如，如果 [密碼重設失敗鎖定計數] 設定爲 5，[登入失敗鎖定間隔時間] 設定爲 5 分鐘，則在被鎖定之前，使用者可以在 5 分鐘內重設 5 次密碼。

密碼重設失敗鎖定間隔時間 (分鐘)

此屬性定義使用者被鎖定之前，可以完成嘗試密碼重設次數 (在 [密碼重設失敗鎖定計數] 中定義) 的時間量 (以分鐘計算)。

接受鎖定通知的電子郵件位址

此屬性指定使用者被鎖定而無法使用密碼重設服務時，接收通知的電子郵件位址。用由空格分隔的清單形式指定多個電子郵件位址。

N 次失敗後警告使用者

此屬性指定在 Identity Server 傳送使用者將被鎖定的警告訊息之前，可以發生的密碼重設失敗次數。

密碼重設失敗鎖定持續時間 (分鐘)

此屬性定義已發生鎖定後，使用者無法嘗試密碼重設的持續時間 (以分鐘計算)。

密碼重設失敗鎖定模式

此屬性指定如果使用者最初使用密碼重設應用程式重設密碼失敗，是否允許使用者重設密碼。依預設，不啓用此功能。

密碼重設鎖定屬性名稱

此屬性包含在 [密碼重設鎖定屬性值] 中設定的 inetuserstatus 值。如果使用者被鎖定使用 [密碼重設] ，並且 [密碼重設失敗鎖定持續時間 (分鐘)] 變數設定爲 0，則 inetuserstatus 將被設定爲非作用中，從而禁止使用者嘗試重設密碼。

密碼重設鎖定屬性值

此屬性指定使用者狀態的 inetuserstatus 值 (包含在 [密碼重設鎖定屬性名稱] 中) 爲作用中或非作用中。如果使用者被鎖定使用 [密碼重設] ，並且 [密碼重設失敗鎖定持續時間 (分鐘)] 變數設定爲 0，則 inetuserstatus 將被設定爲非作用中，從而禁止使用者嘗試重設密碼。

第 33 章

平台服務屬性

平台服務屬性爲全域屬性。套用於這些屬性的值也套用於整個 Sun ONE Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。) 平台屬性包括：

- 伺服器清單
- 平台語言環境
- Cookie 網域
- 登入服務 URL
- 登出服務 URL
- 可用的語言環境
- 用戶端字元集

伺服器清單

命名服務在初始化期間讀取此屬性。此清單包含單一 Identity Server 配置中的 Identity Server 階段作業伺服器。例如，如果安裝了兩個 Identity Server，但是應該作爲一個整體使用，則它們必須均包含在此清單中。如果此清單中未列出請求服務 URL 時指定的主機，則命名服務將拒絕此請求。清單中的第一個值指定了安裝時指定的服務器主機名稱與連接埠，清單中的最後一個值是唯一識別此伺服器的兩個位元組值。參與負載平衡的每個伺服器都需要具有唯一的識別碼。也可以將伺服器 URL 對映至伺服器 ID，用以縮短 Cookie 長度。例如：

`protocol://`*server_domain*`:`*port*`|01`

其他伺服器可以使用 `protocol://`*server_domain*`:` *port*`|01|`*instance_name* 格式加入。

平台語言環境

此平台語言環境值是安裝 Identity Server 所使用的預設語言子類型。將在此值的語言環境中管理認證、記錄與管理服務。預設值爲 `en_US`。請參閱第 191 頁的表 19-1，以取得所有支援語言子類型的清單。

Cookie 網域

這是在認證期間將 Cookie 設定爲使用者瀏覽器時，Cookie 標頭中要傳回網域的清單。如果清單爲空，則不會設定 Cookie 網域。換句話說，Identity Server 階段作業 Cookie 將僅轉寄至 Identity Server 本身，而不會轉寄至此網域中的任何其他伺服器。如果此網域中的其他伺服器要求 SSO，則必須將此屬性設定爲具有 Cookie 網域的屬性。如果在一個 Identity Server 的不同網域中有兩個介面，則將需要在此屬性中設定兩個 Cookie 網域。如果使用負載平衡器，Cookie 網域必須屬於負載平衡器網域，而不是負載平衡器後面的伺服器網域。此欄位的預設值是已安裝 Identity Server 的網域。

登入服務 URL

此欄位指定登入頁面的 URL。此屬性的預設值爲 */Service_DEPLOY_URI*`/UI/Login`。

登出服務 URL

此欄位指定登出頁面的 URL。此屬性的預設值爲 */Service_DEPLOY_URI*`/UI/Logout`。

可用的語言環境

此屬性儲存爲此平台配置的所有可用語言環境。請考量讓使用者選擇其語言環境的應用程式。此應用程式會從平台設定檔中取得此屬性，然後將語言環境清單展示給使用者。使用者將選擇某種語言環境，此應用程式會在使用者項目 `preferredLocale` 中設定此語言環境。

用戶端字元集

此屬性指定平台層級的不同用戶端使用的字元集。包含用戶端類型及相應字元集的清單。格式如下所示：

```
clientType|charset

clientType2|charset
```

例如：

```
genericHTML|UTF-8
```

第 34 章

策略配置服務屬性

策略配置服務屬性由全域屬性與組織屬性組成。套用於全域屬性的值也套用於整個 Sun ONE Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。) 在服務管理下套用於組織屬性的值會成爲策略配置的預設值。組織註冊服務後，需要建立服務範本。註冊後組織的管理員可以變更預設值。組織屬性不會由組織中的項目繼承。策略配置屬性可分爲：

- 全域屬性
- 組織屬性

全域屬性

策略配置服務中的全域屬性包括：

- 資源比較程式

資源比較程式

此屬性指定資源比較程式資訊，該資訊用於比對策略規則定義中指定的資源。在建立和評估策略時均會使用資源比較。此屬性包含以下值：

`serviceType`	指定應該使用此比較程式的服務。
`class`	定義實施資源比較演算法的 java 類別。
`wildcard`	指定可以在資源名稱中定義的萬用字元。
`delimiter`	指定在資源名稱中使用的分割元。
`caseSensitivity`	指定在比較兩種資源時，是否應該考量或忽略大小寫。`False` 忽略大小寫，`True` 考量大小寫。

組織屬性

策略配置服務中的組織屬性包括：

- LDAP 伺服器與連接埠
- LDAP 基準 DN
- LDAP 使用者基準 DN
- Identity Server 角色基準 DN
- LDAP 連結 DN
- LDAP 連結密碼
- LDAP 連結密碼 (確認)
- LDAP 組織搜尋過濾
- LDAP 組織搜尋範圍
- LDAP 群組搜尋過濾
- LDAP 群組搜尋範圍
- LDAP 使用者搜尋過濾
- LDAP 使用者搜尋範圍
- LDAP 角色搜尋過濾

- LDAP 角色搜尋範圍
- Identity Server 角色搜尋範圍
- LDAP 組織搜尋屬性
- LDAP 群組搜尋屬性
- LDAP 使用者搜尋屬性
- LDAP 角色搜尋屬性
- 搜尋傳回的最大結果數
- 搜尋逾時 (秒)
- 啓用 LDAP SSL
- LDAP 連線區最小大小
- LDAP 連線區最大大小
- 選取的策略主題
- 選取的策略條件
- 選取的策略參考
- 持續的主題結果時間
- 啓用使用者別名

LDAP 伺服器與連接埠

此欄位指定 Identity Server 安裝期間指定的主 LDAP 伺服器之主機名稱與連接埠號 (用於搜尋策略主題，例如 LDAP 使用者、LDAP 角色、LDAP 群組等)。格式爲 *hostname:port*，例如：

```
machine1.example.com:389
```

對於多重 LDAP 伺服器主機的錯誤修復配置，本值可以爲以空格分隔的主機清單。格式爲 hostname1:port1 hostname2:port2...

例如：

```
machine1.example1.com:389 machine2.example1.com:389
```

多重項目必須以本機伺服器名稱作爲字首。這樣可以將特定的 Identity Server 配置爲與特定的 Directory Server 通訊。

格式爲 `servername|hostname:port`

例如：

`machine1.example1.com|machine1.example1.com:389`

`machine1.example2.com|machine1.example2.com:389`

對於錯誤修復配置：

`machine1.example1.com|machine1.example1.com:389 machine2.example.com1:389`

`machine1.example2.com|machine1.example2.com:389 machine2.example2.com:389`

注意 該屬性已變更爲接受值的清單，以支援多個伺服器。在 6.0 SP1 版次中，該屬性只接受單一值。

如果嘗試讓 6.0SP1 和 6.1 共存於單一部署環境中，尤其是在 Identity Server 6.0 SP1 實例指向 6.1 DIT 的情況下，這樣可能會出現問題。

若要使它們共存，請確保該屬性只有單一 LDAP 伺服器。

LDAP 基準 DN

此欄位指定要開始搜尋的 LDAP 伺服器中的基準 DN。依預設，它是 Identity Server 安裝的頂層組織。

LDAP 使用者基準 DN

此屬性指定 LDAP 伺服器中由 LDAP 使用者主題使用的基準 DN，搜尋將從此基準 DN 開始。依預設，它是 Identity Server 安裝基準的頂層組織。

Identity Server 角色基準 DN

此屬性指定 LDAP 伺服器中由 Identity Server 角色主題使用的基準 DN，搜尋將從此基準 DN 開始。依預設，它是 Identity Server 安裝基準的頂層組織。

LDAP 連結 DN

此欄位指定 LDAP 伺服器中的連結 DN。

LDAP 連結密碼

此屬性定義用於連結至 LDAP 伺服器的密碼。依預設，在安裝期間輸入的 `amldapuser` 密碼會作爲連結使用者。

LDAP 連結密碼 (確認)

對 LDAP 連結密碼的確認。

LDAP 組織搜尋過濾

指定用於尋找組織項目的搜尋過濾。預設值爲 `(objectclass=sunMangagedOrganization)`。

LDAP 組織搜尋範圍

此屬性定義用於尋找組織項目的範圍。此範圍必須爲以下一種範圍：

- `SCOPE_BASE`
- `SCOPE_ONE`
- `SCOPE_SUB` (預設)

LDAP 群組搜尋過濾

指定用於尋找群組項目的搜尋過濾。預設值爲 `(objectclass=groupOfUniqueNames)`。

LDAP 群組搜尋範圍

此屬性定義用於尋找群組項目的範圍。此範圍必須爲以下一種範圍：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (預設)

LDAP 使用者搜尋過濾

指定用於尋找使用者項目的搜尋過濾。預設值爲 (objectclass=inetorgperson)。

LDAP 使用者搜尋範圍

此屬性定義用於尋找使用者項目的範圍。此範圍必須爲以下一種範圍：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (預設)

LDAP 角色搜尋過濾

指定用於尋找角色項目的搜尋過濾。預設值爲 (&(objectclass=ldapsubentry)(objectclass=nsroledefinitions))

LDAP 角色搜尋範圍

此屬性定義用於尋找角色項目的範圍。此範圍必須爲以下一種範圍：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (預設)

Identity Server 角色搜尋範圍

此屬性定義用於尋找 Identity Server 角色主題項目的範圍。此範圍必須爲以下一種範圍：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB（預設）

LDAP 組織搜尋屬性

此欄位定義對組織進行搜尋的屬性類型。預設值爲 o。

LDAP 群組搜尋屬性

此欄位定義對群組進行搜尋的屬性類型。預設值爲 cn。

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。預設值爲 uid。

LDAP 角色搜尋屬性

此欄位定義對角色進行搜尋的屬性類型。預設值爲 cn。

搜尋傳回的最大結果數

此欄位定義搜尋傳回的最大結果數。預設值爲 100。如果搜尋限制超過了指定時間，則會傳回到此指定時間點時已經找到的項目。

搜尋逾時 (秒)

此屬性指定發生搜尋逾時之前的時間。如果搜尋超過了指定時間，則會傳回到此指定時間點時已經找到的項目。

啟用 LDAP SSL

此屬性指定 LDAP 伺服器是否正在執行 SSL。選取此屬性會啓用 SSL，取消選取此屬性 (預設) 會停用 SSL。

LDAP 連線區最小大小

此屬性指定用於連線至 Directory Server 的連線區最小大小，如 LDAP 伺服器屬性中指定的最小大小。預設值爲 1。

LDAP 連線區最大大小

此屬性指定用於連線至 Directory Server 的連線區最大大小，如 LDAP 伺服器屬性中指定的最大大小。預設值爲 10。

選取的策略主題

此屬性允許您選取可用於組織中策略定義的主題類型集。

選取的策略條件

此屬性允許您選取可用於組織中策略定義的條件類型集。

選取的策略參考

此屬性允許您選取可用於組織中策略定義的參考類型集。

持續的主題結果時間

此屬性指定快取主題結果 (基於單一登入記號) 可用於評估同一策略請求的時間 (以分鐘計算)。

在最初評估某策略是否與 SSO 記號相符時，會評估策略中的主題實例，以決定此策略是否適用於給定使用者。使用 SSO 記號 ID 加密的主題結果，在策略中進行快取。如果在 [持續的主題結果時間] 屬性指定的時間內，對同一 SSO 記號 ID 的同一策略進行評估，策略框架會擷取快取的主題結果，而不是評估主題實例。這會大大減少策略評估的時間。

啟用使用者別名

如果建立策略以保護在遠端 Directory Server 中主題成員別名爲本機使用者的資源，則必須啓用此屬性。

例如，如果在遠端 Directory Server 中建立 `uid=rmuser`，然後將 `rmuser` 作爲別名加入到 Identity Server 中的本機使用者 (如 `uid=luser`)，則必須啓用此屬性。當您以 `rmuser` 登入時，系統會經由本機使用者 (`luser`) 建立階段作業，從而使策略執行成功。

第 35 章

SAML 服務屬性

安全宣示標記語言 (SAML) 服務屬性爲全域屬性。套用於這些屬性的值也套用於整個 Sun ONE Identity Server 配置，並且由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。)

如需關於 SAML 服務架構的更多資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」。

SAML 屬性如下所示：

- 網站 ID 與網站發行者名稱
- 簽名請求
- 簽名回應
- 簽名假設
- Artifact 名稱
- 目標限定符號
- Artifact 逾時 (秒)
- notBefore 時間假設偏移因素
- 假設逾時 (秒)
- 可信任的夥伴網站
- POST 至目標 URL

網站 ID 與網站發行者名稱

此屬性包含項目清單，其中每個項目包含一個實例 ID、一個網站 ID 以及一個網站發行者名稱。在安裝期間將指定預設值。格式如下所示：

`instanceid=serverprotocol://servername:portnumber|siteid=`*site_id*`|issuerName=`*site_issuer_name*

爲 SSL (在來源網站與目標網站中) 配置完這一屬性後，請確定 `instanceid` 協定爲 `HTTPS//`。

簽名請求

此屬性指定在發送所有 SAML 請求之前，是否對其進行數位簽名 (`XML DSIG`)。按一下此選項會啓用此功能。

簽名回應

此屬性指定在發送所有 SAML 回應之前，是否對其進行數位簽名 (XML DSIG)。按一下此選項會啓用此功能。

無論是否啓用此選項，均會對 SAML Web POST 設定檔使用的所有 SAML 回應進行數位簽名。

簽名假設

此屬性指定在發送所有 SAML 假設之前，是否對其進行數位簽名 (`XML DSIG`)。按一下此選項會啓用此功能。

Artifact 名稱

此屬性爲 SAML 服務配置中定義的 SAML Artifact 指定變數名稱。SAML Artifact 是大小有限資料，可以識別假設與來源網站。它作爲 URL 查詢字串的一部分，透過重新導向傳遞至目標網站。預設值爲 SAMLart。例如，如果使用預設 SAMLart 服務配置，則重新導向查詢字串可能爲：

http://*host:port*/*deploy_URI*/SamlAwareServlet?TARGET=http://*URL*/&SAMLart=artifact123

目標限定符號

此屬性爲重新導向使用的目標網站 URL 指定變數名稱。預設值爲 Target。

Artifact 逾時 (秒)

此屬性指定爲 Artifact 建立的假設之逾時。預設值爲 400。

notBefore 時間假設偏移因素

此屬性用於計算假設的 notBefore 時間。例如，如果 IssueInstant 是 2002-09024T21:39:49Z，並且假設偏移因素 notBefore 時間值設定爲 300 秒 (預設值爲 180)，則假設條件元素的 notBefore 屬性將爲 2002-09-24T21:34:49Z。

假設逾時 (秒)

此屬性指定假設發生逾時之前的秒數。預設值爲 420。

注意 假設的總有效持續時間由在 [notBefore 時間假設偏移因素] 屬性和 [假設逾時] 屬性中設定的值來定義。

可信任的夥伴網站

此屬性儲存夥伴的資訊，以便某個網站可以建立與另一個夥伴網站進行通訊的可信任關係。

此屬性包含項目清單，其中每個項目均包含鍵值/值對 (由「|」分隔)。每個項目均需要來源 ID。例如：

`SourceID=siteid|SOAPURL=https://servername:portnumber/amserver/SAMLSOAPReceiver|AuthType=SSL|hostlist=ipaddress` （或 *server DNS name*、*cert alias*）

這些參數包括：

表 35-1 可信任夥伴網站的參數

`SourceID`	SiteID 和發行者名稱中定義的序列 (含 20 個位元組)。

`target`	在有連接埠號或無連接埠號的特定網域中定義此參數。如果您要存取特定網域中託管的網頁，則 `target` 指定由 `SAMLUrl` 或 `POSTUrl` 參數定義的重新導向至的 URL 以進行進一步處理。
	如果有兩個項目 (一個包含連接埠號，另一個不包含連接埠號) 均屬於 [可信任的夥伴網站] 屬性中指定的同一網域，則包含連接埠號的項目具有較高的優先級。
	例如，如果您有以下兩個可信任的夥伴網站定義：
	`target=sun.com|SAMLUrl=http://machine1.sun.com:8080/amserver/SAMLAwareServlet`
	和
	`target=sun.com:8080|SAMLUrl=httyp://machine2.sun.com:80/amserver/SAMLAwareServlet`
	並且正在尋找以下網頁：
	`http://somemachine.sun.com:8080/index.html`
	由於相符的網域與連接埠共存於 `target` 參數中，因此將選擇第二個定義作為 SAML 服務供應商。

`SAMLUrl`	定義提供了 SAML 服務的 URL。URL 中指定的 servlet 實施在 OASIS-SAML 連結與設定檔規格中定義的使用 `Artifact` 執行網路瀏覽器 `SSO` 設定檔。

POSTUrl	定義提供了 SAML 服務的 URL。URL 中指定的 servlet 實施在 OASIS-SAML 連結與設定檔規格中定義的使用 POST 執行網路瀏覽器 SSO 設定檔。
issuer	定義 Identity Server 中產生的假設之建立者。語法為 hostname:port。
SOAPUrl	指定 SOAP 收件者服務 URL。
AuthType	定義 SAML 中使用的認證類型。應該為以下一種類型： • NOAUTH • BASICAUTH • SSL • SSLWITHBASICAUTH 此參數是選擇性的，如果未指定此參數，則預設值為 NOAUTH。 如果指定了 BASICAUTH 或 SSLWITHBASICAUTH，則需要 User 參數，並且 SOAPUrl 應該為 HTTP。
User	定義用於保護其 SOAP 收件者之夥伴的使用者 ID。
hostlist	此屬性列出了指定夥伴網站中的所有主機 IP 位址和/ 或 certAlias，可用於向此網站傳送請求。這確保了請求者是真正的 SAML Artifact 目的收件者。 如果請求者的主機證書或用戶端證書位於收件者網站中的此清單中，服務將繼續。如果主機證書或用戶端證書與主機清單中的任一主機或證書均不相符，則 SAML 服務將拒絕請求。
AccountMapper	指定可插接式類別，該類別定義假設主題與目標網站身份關聯的方式。依預設為： com.sun.identity.saml.plugins.DefaultAccountMapper
attributeMapper	指定 attributeMapper 所在路徑的類別。應用程式可以產生 attributeMapper，以取得 SSOToken ID 或包含查詢中 AuthenticationStatement 的假設。此對映程式然後即用於擷取主題的屬性。如果未指定任何 attributeMapper，則會使用 DefaultAttributeMapper。
actionMapper	指定 actionMapper 所在路徑的類別。應用程式可以產生 actionMapper，以取得 SSOToken ID 或包含查詢中 AuthenticationStatement 的假設。然後，對映程式即可用於擷取查詢中定義的動作之授權決定。如果未指定任何 actionMapper，則會使用 DefaultActionMapper。

siteAttributeMapper	指定 `siteAttributeMapper` 所在路徑的類別。應用程式可以產生 `siteAttributeMapper`，以取得進行 SSO 時要包含於假設中的屬性。如果未找到任何 `siteAttributeMapper`，則在 SSO 期間假設中將不會包含任何屬性。
`certAlias=`*aliasName*	當夥伴對假設進行了簽名，並且在已簽名假設的 `KeyInfo` 部分找不到夥伴證書時，指定驗證假設中簽名所使用的 `certAlias` 名稱。

下表列出了可信任夥伴網站的範例配置。不是所有實例均必須使用所有參數，因此選擇性參數會包含在方括號中。

	寄件者	**收件者**
artifact	`sourceid`	`sourceid`
	`target`	`SOAPUrl`
	`SAMLUrl`	[`accountMapper`]
	`hostlist`	[`AuthType`]
	[`siteAttributeMapper`]	[`User`]
		[`certAlias`]
POST 設定檔	`sourceid`	`sourceid`
	`target`	`issuer`
	`POSTUrl`	[`accountMapper`]
	[`siteAttributeMapper`]	[`certAlias`]
SOAP 請求		`sourceid`
		`hostlist`
		[`attributeMapper`]
		[`actionMapper`]

寄件者	收件者
	[certAlias]
	[issuer]

POST 至目標 URL

如果此網站透過 SSO (Artifact 設定檔或 POST 設定檔) 收到的目標 URL 列於此屬性中，則從 SSO 接收的此假設或數個假設會透過 http: FORM POST 傳送至目標 URL。避免在 POST 中使用測試 URL 或任何其他附加 URL。

第 36 章

階段作業服務屬性

階段作業服務屬性爲全域屬性與動態屬性。套用於全域屬性的值也套用於整個 Identity Server 配置，並由每個配置的組織繼承。(由於全域屬性的目標是自訂 Identity Server 應用程式，因此這些值無法直接套用於角色或組織。)

套用於動態屬性的值也套用於角色或組織。如果角色指定給使用者或者使用者指定給組織，依預設，這些屬性將由此使用者繼承。在服務配置中爲所有 Identity Server 已註冊組織設定預設階段作業值。但透過以下方法可以爲個別組織設定不同的值：將階段作業服務註冊到特定組織，然後建立範本並輸入值 (非預設值)。

全域屬性

全域屬性包括：

- 最大搜尋結果數
- 搜尋逾時 (秒)

最大搜尋結果數

此屬性指定階段作業搜尋傳回的最大結果數。預設值爲 120。

搜尋逾時 (秒)

此屬性定義階段作業搜尋終止前的最長時間。預設值爲 5 秒。

動態屬性

動態屬性包括：

- 最大階段作業時間 (分鐘)
- 最大閒置時間 (分鐘)
- 最大快取時間 (分鐘)

最大階段作業時間 (分鐘)

此屬性的值以分鐘計算，表示階段作業過期而使用者必須重新認證以重新取得存取權限之前的最大時間。將接受等於或大於 1 的值。預設值爲 120。(若要兼顧安全性與方便性，請考量將最大階段作業時間間隔設定爲較大值，將最大閒置時間間隔設定爲相對較小的值。) 最大階段作業時間限制階段作業的有效性。它不會超過配置的值。

最大閒置時間 (分鐘)

此屬性接受的值等於階段作業過期、使用者必須重新認證以重新取得存取權限之前閒置的最大時間 (以分鐘計算)。將接受等於或大於 1 的值。預設值爲 30。(若要兼顧安全性與方便性，請考量將最大階段作業時間間隔設定爲較大值，將最大閒置時間間隔設定爲相對較小的值。)

最大快取時間 (分鐘)

此屬性的值以分鐘計算，等於用戶端聯絡 Identity Server 以重新顯示快取階段作業資訊之前的最大時間間隔。將接受等於或大於 0 的值。預設值爲 3。建議最大快取時間始終小於最大閒置時間。

第 37 章

使用者屬性

使用者屬性包含在以下兩個位置：[服務配置] 視窗與 [使用者管理] 視窗。[服務配置] 視窗包含已註冊組織的預設屬性。[使用者管理] 視窗包含使用者項目屬性。

- 使用者服務屬性
- 使用者設定檔屬性
- 唯一使用者 ID

使用者服務屬性

使用者服務屬性爲動態屬性。套用於動態屬性的值會指定給在 Identity Server 中配置的角色或組織。如果角色指定給使用者或者使用者指定給組織，這些動態屬性將成爲該使用者的一個特徵。使用者屬性分爲：

- 使用者喜好的語言
- 使用者喜好的時區
- 繼承的語言環境
- 開始檢視的管理員 DN
- 預設使用者狀態

爲所有 Identity Server 已註冊的組織設定預設使用者值。但透過以下方法可以爲個別組織設定不同的值：將使用者服務註冊到特定組織，然後建立範本並輸入值 (非預設值)。

使用者喜好的語言

此欄位指定在 Identity Server 主控台中顯示的文字語言的使用者選項。預設值爲 en。此值會將本土化按鍵集對映至使用者階段作業，從而螢幕文字會以適於使用者使用的語言顯示。

使用者喜好的時區

此欄位指定使用者存取 Identity Server 主控台所在的時區。此欄位沒有預設值。

繼承的語言環境

此欄位指定使用者的語言環境。預設值爲 en_US。第 191 頁的表 19-1 中的任何值均可使用。

開始檢視的管理員 DN

如果該使用者是 Identity Server 管理員，則此欄位指定該使用者登入時，作爲 Identity Server 主控台中顯示的起點之節點。此欄位沒有預設值。可以使用該使用者至少具有讀取權限的有效 DN。

預設使用者狀態

此選項指示任何新建使用者的預設狀態。此狀態會由「使用者項目」狀態取代。只有作用中的使用者才可以透過 Identity Server 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 – 使用者可以透過 Identity Server 進行認證。
- 非作用中 – 使用者無法透過 Identity Server 進行認證，但使用者設定檔依舊儲存在目錄中。

個別使用者狀態的設定方法如下：註冊使用者服務，選擇此值並將其套用於某種角色，然後將此角色加入到使用者設定檔。

使用者設定檔屬性

[使用者設定檔屬性] 是使用者設定檔的預設屬性。這些值由管理員或使用者在登入時，於 [使用者設定檔] 檢視中設定。管理員可以將自己的使用者屬性加入至使用者設定檔，或者建立新的服務。如需更多資訊，請參閱「*Sun ONE Identity Server Customization and API Guide*」。

注意 Identity Server 不強制使用者項目中的屬性必須唯一。例如，可以在同一組織中建立 `userA` 和 `userB`。兩者的 [電子郵件位址] 屬性均可以設定為 `jimb@madisonparc.com`。管理員可以配置 Sun ONE Directory Server 的屬性唯一性外掛程式，以協助強制使屬性值唯一。如需更多資訊，請參閱本章結尾處的「唯一使用者 ID」或「*Sun One Directory Server 管理員指南*」。

名字

此欄位中爲使用者的名字。([名字] 值和 [姓氏] 值可以識別 Identity Server 主控台右上角 [目前已登入] 欄位中的使用者。)

姓氏

此欄位中爲使用者的姓氏。([名字] 值和 [姓氏] 值可以識別 Identity Server 主控台右上角 [目前已登入] 欄位中的使用者。)

全名

此欄位中爲使用者的全名。

密碼

此欄位中爲 [使用者 ID] 欄位中指定的名稱之密碼。

密碼 (確認)

對此密碼的確認。

電子郵件位址

此欄位中爲使用者的電子郵件位址。

員工號碼

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。

住家地址

此欄位中爲使用者的住家地址。

使用者狀態

此選項指示是否允許使用者透過 Identity Server 進行認證。只有作用中的使用者才可以透過 Identity Server 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 – 使用者可以透過 Identity Server 進行認證。
- 非作用中 – 使用者無法透過 Identity Server 進行認證，但使用者設定檔依舊儲存在目錄中。

注意 將使用者狀態變更為非作用中僅會影響透過 Identity Server 進行的認證。Directory Server 使用 nsAccountLock 屬性來確定使用者帳戶狀態。針對 Identity Server 認證而設為非作用中的使用者帳戶，仍可執行不要求 Identity Server 的工作。若要使目錄中的使用者帳號處於非作用中，而且不只是針對 Identity Server 認證，請將 nsAccountLock 的值設定為 true。如果您網站的委託管理員要定期將使用者設為非作用中，請考量將 nsAccountLock 屬性加入 Identity Server 的 [使用者設定檔] 頁面。請參閱「*Sun ONE Identity Server Customization and API Guide*」，以取得詳細資訊。

帳戶過期日期

如果存在該屬性，則當目前日期和時間超過指定的帳戶過期日期時，認證服務將不允許登入。此屬性的格式如下所示：

```
(mm/dd/yyyy hh:mm)
```

使用者認證配置

此屬性設定使用者的認證方法。預設認證方法爲 LDAP。透過按一下 [編輯] 連結可以選取一個或多個認證方法。如果選取多個方法，則使用者可能需要透過所有選取方法成功進行認證。

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。爲使用在此屬性中配置的任何別名，必須透過將 iplanet-am-user-alias-list 屬性加入 LDAP 服務的 [使用者項目搜尋屬性] 欄位中，從而修改 LDAP 服務。

喜好的語言環境

此欄位指定使用者的語言環境。預設值爲 en_US。第 191 頁的表 19-1 中的任何值均可使用。

您可以在下拉式功能表中使用以下某個屬性：

- 忽略
- 自訂
- 繼承

成功 URL

此屬性指定使用者認證成功後將重新導向至的 URL。

失敗 URL

此屬性指定使用者認證失敗後將重新導向至的 URL。

唯一使用者 ID

爲了在 Identity Server 應用程式中強制使 uid 具有唯一性，必須將 Directory Server 中提供的外掛程式配置如下：

```
dn: cn=uid uniqueness,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: uid uniqueness
nsslapd-pluginPath: /ids908/lib/uid-plugin.so
nsslapd-pluginInitfunc: NSUniqueAttr_Init
nsslapd-pluginType: preoperation
```

```
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attribute=uid
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: NSUniqueAttr
nsslapd-pluginVersion: 6.1
nsslapd-pluginVendor: Sun | SunONE
nsslapd-pluginDescription: Enforce unique attribute values
```

建議使用 nsManagedDomain 物件類別標記需要 uid 唯一性的組織。依預設，此外掛程式是停用的。

若要配置每個組織的 uid 唯一性，請在外掛程式項目中加入每個組織的 DN，或者使用記號物件類別選項並將 nsManagedDomain 加入至每個頂層組織項目。

```
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attribute=uid
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
```

錯誤碼

本附錄提供 Sun ONE Identity Server 所產生錯誤訊息的清單。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作爲一個良好起點。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：

- Identity Sever 主控台錯誤
- 認證錯誤碼
- 策略錯誤碼
- amadmin 錯誤碼

如果您需要有關診斷錯誤的進一步援助，請聯絡 Sun ONE 技術支援：

http://www.sun.com/service/sunone/software/index.html

Identity Sever 主控台錯誤

下表描述了 Identity Server 主控台產生和顯示的錯誤碼。

表 A-1 Identity Server 主控台錯誤

錯誤訊息	描述/可能的原因	動作
刪除以下項目時出錯：	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。
您輸入了無效的 URL	不正確地輸入 Identity Server 主控台視窗的 URL 時會出現此訊息。	
沒有與搜尋條件相符的項目。	在搜尋視窗或 [過濾] 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。
沒有可顯示的屬性。	所選物件不包含任何在其綱目中定義的可編輯屬性。	
此服務沒有可顯示的資訊。	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 [搜尋傳回的最大結果數] 屬性修改為較大的值。您還可以修改搜尋參數，使其限制更加嚴格。
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] 屬性修改為較大的值。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。請聯絡您的管理員。	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 的值變更為有效的 DN。
無法建立**身份物件**。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 A-2 認證錯誤碼

錯誤訊息	描述/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 Identity Server 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 Identity Server。	重新啟動伺服器。
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	Identity Server 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 容器的錯誤日誌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。	
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	認證失敗。這是顯示在預設登入失敗範本中的一般錯誤訊息。最常見的原因為憑證無效/不正確。	輸入有效且正確的使用者名稱/密碼 (呼叫的認證模組所需的憑證)。
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/自行註冊認證模組時，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	輸入的密碼缺少字元。登入至成員身份/自行註冊認證模組時，系統會顯示此錯誤。	依預設，登入密碼必須包含至少 8 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/自行註冊認證模組時，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」欄位與「密碼」欄位不能使用相同的值。登入至成員身份/自行註冊認證模組時，系統會顯示此錯誤。	確保使用者名稱與密碼不同。

表 A-2 認證錯誤碼

錯誤訊息	描述/可能的原因	動作
nouser.name	沒有輸入使用者名稱。登入至成員身份/自行註冊認證模組時，系統會顯示此錯誤。	確保輸入使用者名稱。
no.password	沒有輸入密碼。登入至成員身份/自行註冊認證模組時，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/自行註冊認證模組時，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/自行註冊認證模組時，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出錯。	儲存使用者設定檔時出錯。登入至成員身份/自行註冊認證模組時，系統會顯示此錯誤。	確保 `Membership.xml` 檔案中自行註冊的屬性和元素有效且正確。
orginactive	該組織不在作用中。	透過將組織狀態從 `inactive` 變更為 `active`，藉由 Identity Server 啟動組織。
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。	透過將使用者狀態從 `inactive` 變更為 `active`，藉由管理主控台啟動使用者。 如果使用者被 [記憶體鎖定] 鎖定，請重新啟動伺服器。
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為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，已為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	未找到配置。	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 使用者名稱。	

表 A-2 認證錯誤碼

錯誤訊息	描述/可能的原因	動作
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	必填欄位之一未填入。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 Identity Server 主控台中顯示的錯誤碼。

表 A-3 策略錯誤碼

錯誤訊息	描述/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。
rule_name_already_present	具有給定名稱的其他規則已存在	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。	為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。

表 A-3 策略錯誤碼

錯誤訊息	描述/可能的原因	動作
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	屬性值不是整數。	此外掛程式的屬性值應該為整數。
property_value_not_defined	屬性值應該被定義。	為給定屬性提供值。
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

下表描述由 `amadmin` 指令行工具在 Identity Server 除錯檔案中產生的錯誤碼。

表 A-4 amadmin 錯誤碼

錯誤訊息	程式碼	描述/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` 和 `--addAttributes`) 及它們的值。
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，作為 `--runasdn` 的值。
noservicename	4	遺漏 `--deletservice` 值的服務名稱。	提供服務名稱，作為 `--deleteservice` 的值。

表 A-4 amadmin 錯誤碼

錯誤訊息	程式碼	描述/可能的原因	動作
nopwdforadmin	5	遺漏 `--password` 值的密碼。	提供密碼，作為 `--password` 的值。
nolocalename	6	未提供語言環境名稱。語言環境將預設為 en_US。	請參閱預設認證語言環境，以取得語言環境的清單。
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。	檢查以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。	如果 `amadmin` 失敗，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。	如果 `amadmin` 失敗，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。
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 已正確格式化並支援 `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 已正確格式化並支援 `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 檔案為無效檔案而導致無法剖析。	檢查語法並確保輸入 XML 有效。

表 A-4 amadmin 錯誤碼

錯誤訊息	程式碼	描述/可能的原因	動作
nonfatalvalidationerror	21	由於 XML 檔案為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	綱目檔案輸入串流異常。	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。
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	無效的屬性值。	檢查 LDAP 搜尋的層級設定。它應該為 SCOPE_SUB 或 SCOPE_ONE。

表 A-4 amadmin 錯誤碼

錯誤訊息	程式碼	描述/可能的原因	動作
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 有效且為組織物件。
invalidRoleDN	39	無效的角色 DN。	確保 XML 檔案中的 DN 有效且為角色物件。
invalidStaticGroupDN	40	無效的靜態群組 DN。	確保 XML 檔案中的 DN 有效且為靜態群組物件。
invalidPeopleContainerDN	41	無效的個人容器 DN。	確保 XML 檔案中的 DN 有效且為個人容器物件。
invalidOrgUnitDN	42	無效的組織單元 DN。	確保 XML 檔案中的 DN 有效且為容器物件。
invalidServiceHostName	43	無效的服務主機名稱。	確保用於擷取有效階段作業的主機名稱正確。
subschemaexception	44	子綱目錯誤。	僅全域屬性和組織屬性支援子綱目。
serviceschemaexception	45	無法找到服務的服務綱目。	確保 XML 檔案中的子綱目有效。
roletemplateexception	46	僅當綱目類型為動態時，角色範本才可為真。	確保 XML 檔案中的角色範本有效。
cannotAddusersToFileredRole	47	無法將使用者加入已過濾的角色。	確保 XML 檔案中的角色 DN 不是已過濾的角色。
templateDoesNotExist	48	範本不存在。	確保 XML 檔案中的服務範本有效。
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。
cannotCreatePolicyUnderContainer	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。
defaultGroupContainerNotFound	51	未找到群組容器。	為父系組織或容器建立群組容器。
cannotRemoveUserFromFilteredRole	52	無法從已過濾的角色中移除使用者。	確保 XML 檔案中的角色 DN 不是已過濾的角色。
cannotRemoveUsersFromDynamicGroup	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	子綱目字串不存在。	確保子綱目字串存在於 XML 檔案中。

在 SSL 模式中配置 Identity Server

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。

Identity Server 可同時進行 SSL 通訊與非 SSL 通訊。這表示您無需在 SSL 通訊與非 SSL 通訊之間進行選擇，而可以同時使用它們。

以下小節描述使用四個不同的 Web 容器在 SSL 模式中配置 Identity Server 的步驟：

- 使用安全 Sun ONE Web Server 配置 Identity Server
- 使用安全 Sun ONE Application Server 配置 Identity Server

使用安全 Sun ONE Web Server 配置 Identity Server

若要使用 Sun ONE Web Server 在 SSL 模式中配置 Identity Server，請參閱以下步驟：

1. 在 Identity Server 主控台中，按一下頂層組織 (在安裝期間建立) 的 [特性] 箭頭。

   [組織特性] 視窗將顯示在資料框架中。

2. 按一下 [儲存]，以儲存變更。

3. 在 Identity Server 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]。

注意 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 4 至步驟 27 描述 Sun ONE Web Server。

4. 登入 Web Server 主控台。預設連接埠爲 58888。
5. 選取 Identity Server 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]。
6. 按一下畫面右上角的 [套用] 按鈕。
7. 按一下 [套用設定]。

   Web Server 會自動重新啓動。按一下 [確定] 以繼續。
8. 停止選取的 Web Server 實例。
9. 按一下 [安全] 標籤。
10. 按一下 [建立資料庫]。
11. 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。
12. 建立證書資料庫後，按一下 [請求證書]。
13. 在畫面提供的欄位中輸入資料。

    您在 [鍵值對欄位密碼] 欄位中的輸入與您在步驟 11 中的輸入相同。在位置欄位中，需要完整寫出詳細位置。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。

14. 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--
```

15. 複製這些文字並提交，以請求證書。

    請確保您取得了 Root CA 證書。

16. 您將接收到包含證書的證書回應，如：

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

17. 將這些文字複製到剪貼簿，或儲存在檔案中。
18. 移至 Web Server 主控台並按一下 [安裝證書]。
19. 按一下該 Server 的證書。
20. 在 [鍵值對檔案密碼] 欄位中輸入證書資料庫密碼。
21. 在提供的文字欄位中貼上證書，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]。

    瀏覽器將顯示該證書，並提供加入證書的按鈕。

22. 按一下 [安裝證書]。
23. 按一下 [可信任的證書授權單位的證書]。
24. 以步驟 18 至步驟 23 中所述的相同方式安裝 Root CA 證書。
25. 兩個證書安裝完成後，按一下 Web Server 主控台中的 [個人喜好] 標籤。
26. 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]。
27. 將安全狀態從 [停用] 變更爲 [啓用]，然後按一下 [確定] 提交變更。

步驟 28 至步驟 30 描述 Identity Server。

28. 開啓 `AMConfig.properties` 檔案。依預設，該檔案位於 `/opt/SUNWam/lib`。
29. 用 `https://` 取代出現的所有 `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。
30. 儲存 `AMConfig.properties` 檔案。
31. 在 Web Server 主控台中，按一下託管網路伺服器實例之 Identity Server 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。
32. 在文字欄位中輸入證書資料庫密碼並選取 [啓動]。

使用安全 Sun ONE Application Server 配置 Identity Server

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

使用 SSL 設定 Application Server

安全結合 Application Server 實例

1. 透過在您的瀏覽器中輸入以下位址，以管理員身份登入 Sun ONE 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) Identity Server 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. 建立證書資料庫後，按一下 [證書管理] 標籤。
11. 按一下 [請求] 連結 (如果未選取)。
12. 爲證書輸入以下請求資料

    a. 如果該證書爲新證書或更新的證書，則選取它。許多證書會在一段特定時間後過期，某些證書授權單位 (CA) 會自動給您傳送換新通知。

    b. 指定您要提交證書請求的方式。

       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 [可用證書授權單位清單]。

       如果您從使用 Sun ONE Certificate Server 的內部 CA 請求證書，則請按一下 [CA URL] 並輸入 Certificate Server 的 URL。此 URL 應該指向處理證書請求的證書伺服器程式。

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]。將在其上安裝數位證書的 Sun One Application Server 之完整名稱。

[電子郵件位址]。管理員的電子郵件位址。

[組織名稱]。您組織的名稱。證書授權單位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，美國的代碼爲 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 證書。
15. 選取一個 CA，並依循授權單位網站上的說明執行，以取得數位證書。您可以從 CMS、Verisign 或 Entrust.net 取得證書
16. 從證書授權單位接收到數位證書後，您可以將文字複製到剪貼簿，或將其儲存到檔案中。
17. 移至 Sun ONE Application Server 主控台並按一下 [安裝] 連結。
18. 選取 [此伺服器的證書]。
19. 在 [鍵值對檔案密碼] 欄位中輸入證書資料庫密碼。(與在步驟 9 中輸入的密碼相同)。
20. 在提供的文字欄位、[訊息] 文字 (帶有標頭) 中貼上證書，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。瀏覽器會顯示證書，並提供加入證書的按鈕。
22. 按一下 [加入伺服器證書]。
23. 以步驟 10 至步驟 22 中所述的相同方式安裝 Root CA 證書。但是，在步驟 18 中，請選取 [可信任的證書授權單位的證書]。
24. 安裝完兩個證書後，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` 使用的連接埠的值從安裝 Application Server 時輸入的值變更爲更適當的值 (如 443)。
28. 選取 [啓用 SSL/TLS]。
29. 選取 [證書別名]。
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 Sun ONE Identity Server 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。

在 SSL 模式中配置 Identity Server

若要使用 WebLogic 在 SSL 模式中配置 Identity Server，請：

1. 在 Identity Server 主控台中，按一下頂層組織 (在安裝期間建立) 的 [特性] 箭頭。[組織特性] 視窗將顯示在資料框架中。
2. 按一下 [儲存]，以儲存變更。
3. 在 Identity Server 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]。
4. 從以下預設位置開啓 `AMConfig.properties` 檔案：

   `/opt/SUNWam/lib`。
5. 用 `https://` 取代出現的所有 `http://` 協定，並將連接埠號變更爲已啓用 SSL 的連接埠號。
6. 儲存 `AMConfig.properties` 檔案。
7. 重新啓動 Application Server。

索引

符號

英文字母

一畫

四畫

五畫

六畫

七畫

八畫

九畫

十畫

十一畫

十二畫

十三畫

十四畫

十五畫

十六畫

十七畫

十八畫

十九畫

二十畫以上